American Bankers Association
Building Success. Together.

Matthew A. Daigler
Vice President & Senior Counsel
P 202-663-5253
mdaigler@aba.com

June 28, 2021

OFFICE OF THE COMPTROLLER OF THE CURRENCY
Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E—218
Washington, DC 20219
[Docket ID OCC—2020-0049]

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Ann E. Misback
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
[Docket No. OP-1743]

FEDERAL DEPOSIT INSURANCE CORPORATION
James P. Sheesley
Assistant Executive Secretary
Attention: Comments-RIN 3064-ZA24
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
[RIN 3064-ZA24]

BUREAU OF CONSUMER FINANCIAL PROTECTION
Comment Intake, Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552.
[Docket No. CFPB-2021-0004]

NATIONAL CREDIT UNION ADMINISTRATION
Melane Conyers Ausbrooks
Secretary of the Board, National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
[Docket No. NCUA-2021-0023]

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

To the Above-Listed Agencies:

The American Bankers Association ("**ABA**")[1] welcomes the opportunity to comment on the request for information and comment ("**RFI**") on financial institutions' use of artificial intelligence ("**AI**"), including machine learning ("**ML**"), by the Board of Governors of the Federal Reserve System ("**FRB**"), Bureau of Consumer Financial Protection ("**CFPB**"), Federal

[1] The American Bankers Association is the voice of the nation's $21.5 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard $18 trillion in deposits and extend nearly $11 trillion in loans.

Deposit Insurance Corporation ("**FDIC**"), National Credit Union Administration ("**NCUA**"), and Office of the Comptroller of the Currency ("**OCC**," collectively the "**Agencies**").[2]

This RFI is a timely look at an important issue. Banks are actively evaluating ways to safely and responsibly integrate AI solutions to better serve customers and communities across the country. ABA believes AI holds tremendous opportunity to make financial services safer, more convenient, and more inclusive. This opportunity can only be realized when AI is implemented responsibly and the risks associated with AI are well managed. Fortunately, banks are moving carefully to avoid any unintended consequences and banking regulations today already capture the risks associated with AI. Regulators should focus on areas where they can provide clarity to allow banks to adopt AI and ensure that all financial services providers are held to this same high standard.

Our main points with respect to the RFI, which are discussed at greater length below, are as follows:

- Banks are highly regulated and supervised and existing regulation and examination procedures well capture the risks of using AI and ML. As a result, new banking regulations are not necessary or warranted to address AI.

- The Agencies should consider areas where they can clarify existing regulations and supervisory guidance to address the risks and opportunities associated with AI and related technologies to help ensure that banks can continue to bring innovative services to consumers and communities in a safe and responsible manner.

- Because innovation is happening at banks and non-banks alike, the Agencies should ensure that rules are applied consistently to ensure that consumers remain protected wherever they choose to receive their financial services.

- Since banks often have more than one regulator, it is important for the Agencies to take a coordinated approach that fosters innovation and gives banks clarity about how to safely and responsibly implement technologies and move forward with confidence.

- Expectations regarding the use of AI and ML, particularly with respect to explainability, should be framed in the context of the relative risk and importance of the specific use case in question.

- While banks currently manage fair lending risk in the use of AI, in order to support adoption of AI additional clarifying guidance is needed on how to manage disparate impact risks effectively.

[2] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, National Credit Union Administration, Office of the Comptroller of the Currency, Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 FR 1687 (Mar. 31, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf.

- The Agencies should create and encourage participation in pilot or innovation programs in connection with banks' use of AI and ML approaches, as appropriate, although the utilization of such programs should be voluntary.

I. Introduction

ABA believes responsible innovation in financial services will continue to benefit bank customers as it has throughout the history of banking. AI is already adding efficiencies in banking that are providing more Americans with access to safer and more affordable financial products. AI is helping banks extend credit to more borrowers, enhance the customer experience, improve fraud detection, lower the cost of offering services, and much more.

ABA supports the Agencies' efforts to seek more information regarding the developing field of AI and outreach to interested parties regarding the uses and risks of AI. This is particularly important given the significant benefits associated with AI and the extensive effort that banks are devoting to managing the risks associated with these technologies.

We also applaud the Agencies' collaboration on these issues in releasing a joint RFI. As banks innovate, they do so within an established regulatory framework, backed by strong supervision and oversight that ensures robust customer and data protection. Since banks often have multiple regulators, it is important for regulators to take a coordinated approach that fosters innovation and gives banks clarity regarding their expectations for safe and responsible implementation of these technologies. Furthermore, because innovation is happening at banks and non-banks alike, regulators should ensure that rules are applied consistently to ensure consumers remain protected wherever they choose to receive financial services.

II. AI in Banking

Banks of all sizes use AI today to provide real benefits to consumers and will do so increasingly in the future. Ultimately, AI can be beneficial to any business line that seeks to harness the power of data. Banks are adopting AI cautiously to ensure that they do not introduce new risks or unintended consequences to consumers. The current state of adoption of AI by banks varies by application and institution. Some applications, like fraud controls, have already seen widespread AI adoption, while, in lending and other areas, banks have been slower to adopt AI due to uncertainty regarding regulatory and supervisory expectations.

It is important to recognize that AI is fundamentally a technology or modelling technique, not an activity or service. AI has been used as a catch-all term[3] that encompasses a broad array of interrelated technologies and techniques capable of analyzing data and identifying patterns to make decisions and affect outcomes. As such, AI facilitates or enables certain activities but does not change their underlying nature or the services offered.

As with any technology, the use of AI presents certain risks that must be managed. However, the potential risks associated with using AI are not unique to AI, such as creating operational vulnerabilities or consumer protection risks. Banks are already subject to a strong regulatory

[3] The RFI defines "AI approach" very broadly to include "a tool, model, process, or application that employs AI technology in some form." 86 FR at 16839, n.1.

framework and proactive supervision that ensures that banks implement AI and any other technology in a careful and responsible way to best protect consumers.

As explained below, ABA believes a principles-based regulatory approach will help provide a flexible framework for the use of AI that promotes innovation while ensuring that emerging risks are captured. With respect to banking, we do not believe that new regulations are necessary or warranted. Instead, we support the Agencies' efforts to consider areas where they can clarify existing regulations and supervisory expectations to address the risks and opportunities associated with AI and related technologies and to help ensure that banks can continue to bring innovative services to consumers in a safe and responsible manner.

The following are examples of areas where AI is improving, or holds promise to improve, banking.

A. Customer Experience

Banks are using voice recognition and natural language processing ("**NLP**") to automate routine customer interactions (*e.g.*, chatbots), triage customer calls, provide tailored marketing, and customize trade recommendations. As customer interactions move outside of branches and onto online and mobile platforms, banks are using AI to better connect with customers. They can help customers manage budgets and make digital tools more accessible. Chatbots, for example, allow people who are unfamiliar with technology interact digitally.

In addition, customers receiving marketing material are often selected using predictive models created with ML techniques. These models benefit consumers by curtailing the influx of marketing messages to those that they are likely to need or want. Financial institutions that employ these techniques can benefit from greatly increased efficiency and reduce costs for customized solutions. Cybersecurity, Data Privacy, and Fraud

Today, banks maintain high standards of cybersecurity and are adopting AI to help maintain that edge. For instance, AI algorithms can be used to protect consumer accounts by learning how the customer normally acts and flagging unusual behavior in real-time. This can have a major impact by quickly identifying potentially fraudulent transactions and reducing "false positives" that may degrade customers' experience with the bank. NLP tools can be trained to flag suspicious text in emails that indicate phishing attacks, and anomaly detection can be used to warn of deviations in network traffic that are similar to known cyber threats. AI is almost certain to play an increasing role in the future of data protection, fraud prevention, and cybersecurity.

Bank systems are under attack from hackers, cybercriminals, and fraudsters of all types, using various tools to break into networks to gain access to financial and other personal information. Banks need to upgrade their systems continuously to detect, prevent, and mitigate cyber threats and the possible breaches that affect the data security and privacy of our customers.

B. Risk Management and Compliance

As banks seek to keep pace with regulatory compliance requirements, they are turning to new and innovative regulatory technology ("**RegTech**") tools to assist in meeting obligations in an effective and efficient manner. These RegTech tools help banks strengthen their compliance programs, which in turn has the potential to benefit consumers. Banks also use AI in electronic

communications surveillance for insider trading. Using AI and ML, banks can proactively detect behavioral patterns, in both structured data (trading data, personal information, etc.) and unstructured data (voice, SMS, email, etc.), that otherwise would be hidden within a vast amount of data.

C. Lending

AI promises to help banks better evaluate creditworthiness and more quickly provide credit to customers at lower cost. This has the potential to lead to credit being available to more creditworthy borrowers on more affordable terms, particularly applicants with minimal or no credit records and low-income applicants. Despite this promise, banks are moving slowly to implement AI in lending to ensure that they do not introduce unfair and prohibited biases into the lending process.

The most immediate application of AI in lending is for the purpose of automating the underwriting process. These automated processes can apply traditional underwriting decisions in an automated way, reducing underwriting times and lowering costs. This allows banks to extend financing to more applicants and allows borrowers to receive loan approvals and, in turn, funds more quickly. Although ML can allow banks to incorporate nontraditional data like cashflow or a company's daily sales into their credit decisioning engines, it has seen slower adoption by banks in lending. This process is sometimes referred to as advanced credit analytics. Advanced credit analytics can reduce delinquency rates and allow banks to extend credit to more qualified borrowers with thin or nonexistent credit files.

D. Bank Secrecy Act/Anti-Money Laundering

The use of AI has made the process of combating money laundering and terrorist financing more efficient. For many years, financial institutions have used increasingly sophisticated software programs to detect anomalies in customer transaction patterns to root out possible fraud. Today banks are applying new tools and approaches based on AI and ML that are purpose-built to address anti-money laundering ("**AML**") and countering the financing of terrorism ("**CFT**") concerns.

III. Current Regulatory Oversight

Today, extensive banking regulation applies to the activities that AI supports or promises to support in the future. The risks that AI may pose are already well-considered and managed by existing banking regulations and supervisory guidance. We believe the following guidance and regulations are particularly relevant to promoting the benefits of AI while addressing any risks.

A. Model Risk Management

The "model" definition set out in the prudential regulators' model risk management framework (Supervisory Letter SR 11-7) covers machine learning models (the "**Guidance**").[4] We appreciate

[4] *See* Federal Reserve Board, Supervisory Letter SR 11-7, Guidance on Model Risk Management (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm ("For the purposes of this document, the term model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into

that the Guidance is principles-based and, accordingly, offers an intrinsic flexibility vis-a-vis the risk to an institution and consumers by specific use cases. As recently described by Federal Reserve Governor Lael Brainard, the Guidance "highlights the importance of embedding critical analysis throughout the development, implementation, and use of models, which include complex algorithms like AI."[5]

The Guidance also underscores the "effective challenge" of models by unbiased, qualified individuals independent from model development, implementation, and use (*i.e.*, a "second set of eyes"). The Guidance, paired with prudential regulators' guidance on third-party risk management, clarifies expectations for firms when they turn to outside vendors to assist with AI-based tools or services. ***The Guidance emphasizes that regulators' expectations have to be framed in the context of the relative risk and importance of the specific use-case in question.*** The Guidance further explains how AI tools that may be unexplainable or opaque may, with particular use cases, be used in practice with the appropriate controls.[6]

A related issue is the challenge of "overfitting," that is, when an algorithm "learns" from idiosyncratic patterns in the training data that are not representative of the population as a whole. As noted in the RFI, "overfitting" and forms of model drift are not unique to AI.[7] However, as contemplated within the Guidance, the primary defense against overfitting is the technical training of those implementing ML models. It should be clarified that this includes not only those that develop the models, but also those that review and provide "effective challenge." Model developers/owners must be experienced, produce documentation of their model-fitting procedure, and get adequate review by model risk personnel. Adherence to the Guidance helps ensure that models are managed appropriately and safely throughout their lifecycle, regardless of methodology.

Another related issue is dynamic updating (*i.e.*, when an AI approach can update itself on its own sometimes without human intervention). As noted in the RFI, if an AI approach has the capacity for dynamic updating, there may be increased difficulty in review and validation.[8] However, although relatively uncommon at this time, dynamic updating is conceptually no different than calibrating a traditional ML or statistical model. The Guidance once again deals effectively with the management of the increased risks by encouraging frequent and/or granular monitoring of model outcomes, where human oversight is engaged if and when dynamically updating models breach allowed parameters. Here we note that a distinction should be drawn between models that are trained online (*i.e.*, in live use in real-time) and models that are retrained offline (*i.e.,* not in

---

quantitative estimates"). *See also* OCC Bulletin 2011-12 (Apr. 4, 2011), and FDIC FIL 22-2017 (June 7, 2017).

[5] *See* Lael Brainard, Federal Reserve Board Governor, "What Are We Learning about Artificial Intelligence in Financial Services?" Remarks at Fintech and the New Financial Landscape, Hosted by the Federal Reserve Bank of Philadelphia, the Federal Deposit Insurance Corporation, University of Pennsylvania Wharton School of Business, Bank Policy Institute, and Brookings Institution, Philadelphia, Pennsylvania (Nov. 13, 2018), https://www.federalreserve.gov/newsevents/speech/files/brainard20181113a.pdf.

[6] *See, e.g.,* Brainard, *supra* note 5.

[7] 86 FR at 16840.

[8] 86 FR at 16840.

live use) often with guardrails. The former would require a higher degree of monitoring as compared to models that are re-calibrated "offline," and the ABA does not consider such offline updating to be "dynamic updating."

B. Fair Lending

As banks consider adopting technologies that promise to make financial services and products more broadly available, they also must consider the fair lending[9] implications of such technologies. Many commenters tout AI's capacity to increase access to credit; however, it is clear that AI may also pose risks of arbitrarily excluding some consumers from credit. For these reasons, banks know they must understand and manage the fair lending risks resulting from AI use in credit, including in marketing, underwriting, and pricing.

Fair lending risks take the form of disparate treatment, which could result from a model's inclusion or prohibited bases or proxies, and disparate impact, which results from neutral factors that disproportionately impact protected classes or other underserved groups. The OCC has made clear its expectations that banks will manage the fair lending risks that arise from use of AI, noting that banks must "identify potential disparate impact and other fair lending issues. . . . Bank management should be able to explain and defend underwriting and modeling decisions."[10] Relatedly, we welcomed the CFPB's statement regarding the existing regulatory flexibility in explaining reasons for credit denials under Regulation B.[11]

For many banks, however, assessing and addressing disparate impact risk stemming from AI can be a complicated, lengthy, and expensive process, particularly for community banks, given the complexity of new models and the sheer amount of data that can be manipulated. These tasks may be challenging for banks when massive amounts of data are used and because attributes may be bundled and cannot be readily separated, or a vendor refuses to test or validate predictability if certain attributes are removed (which may force the bank to cease doing business with the vendor). Moreover, such testing is beyond smaller banks' in-house expertise and reliance on outside consultants is costly. The Agencies should consider these challenges to managing fair lending risks as they consider additional guidance.

C. Cybersecurity

Banks believe strongly in protecting consumers' sensitive personal and financial information and privacy. Because banks are at the center of people's financial lives, our industry has long been subject to federal and state data protection and privacy laws. For example, Title V of the Gramm-Leach-Bliley Act ("**GLBA**")[12] not only requires banks to protect the security and confidentiality

[9] The primary fair lending laws are the Equal Credit Opportunity Act (ECOA), 15 USC §§ 1601, *et seq.*, and the Fair Housing Act (FHA), 12 USC § 2601.

[10] OCC, Semiannual Risk Perspective (Spring 2019), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2019.pdf, at 23.

[11] Innovation Spotlight: Providing Adverse Action Notices When Using A!/ML Models, https://www.consumerfinance.gov/about-us/blog/innovation-spotlight-providing-adverse-action-notices-when-using-ai-ml-models/.

[12] 15 U.S.C. §§ 6801 *et seq*.

of customer records and information, it also requires banks to provide consumers with notice of their privacy practices and limits the disclosure of financial and other consumer information with nonaffiliated third parties.

The GLBA also required the Agencies to establish standards for safeguarding customer information. These standards require financial institutions to ensure the security and confidentiality of customer information, protect against any anticipated threats to such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. And, since April 1, 2005, the Agencies have required banks to have incident-response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Banks maintain rigorous cybersecurity programs designed to protect the institution and its clients, support secure delivery of services, and meet regulatory requirements, while remaining technology-agnostic and principles-based. These programs encompass the governance, policies, processes, assessments, controls, testing, and training efforts required by industry standards and the regulators.[13] They also provide sufficient security measures to address the risks associated with the introduction and development of AI systems.

As noted above, AI is already a very promising and useful tool for purposes of protecting consumer data while also reducing the risk of cyberattacks and fraud. In the future, it is likely to be even more helpful to strengthen banks' efforts in these areas, consistent with regulatory requirements.

D. UDAAP

The Dodd–Frank Wall Street Reform and Consumer Protection Act ("**Dodd-Frank Act**")[14] prohibits banks and other covered entities from engaging in any unfair, deceptive, or abusive act or practices ("**UDAAP**") in connection with providing consumer financial services.[15] In labeling conduct as UDAAP, bank supervisors examine whether an act or practice harms the consumer (or consumers more generally) and determine whether the conduct is unfair, deceptive, or abusive from the perspective of the consumer.

Thus, banks' existing adherence to UDAAP principles ensures that consumer well-being is put at the forefront of how banks use AI and other ML techniques. Banks, in compliance with UDAAP, already engage in a variety of prophylactic measures to prevent consumer harm, including tracking and analyzing complaint data, managing conduct risk within the institution, and paying close attention to the needs of vulnerable consumers, such as students, the elderly, service

[13] *See, e.g.,* Financial Services Sector Cybersecurity Profile, https://www.aba.com/banking-topics/technology/cybersecurity/cybersecurity-profile.

[14] Public Law 111-203, 124 Stat. 1376 (2010).

[15] Dodd-Frank Act, Title X, Subtitle C, Section 1036.

members, and those with limited English proficiencies. For more examples of how banks manage UDAAP risks, please see ABA's UDAAP Risk Assessment Matrix.[16]

E. Bank Secrecy Act/Anti-Money Laundering[17]

As noted above, banks are applying new tools and approaches based on AI and ML that are purpose-built to address AML/CFT concerns. In fact, the Agencies and Financial Crimes Enforcement Network ("**FinCEN**") confirmed that step in their Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, issued December 3, 2018, where they stated:

> Innovation has the potential to augment aspects of banks' BSA/AML compliance programs, such as risk identification, transaction monitoring, and suspicious activity reporting. Some banks are becoming increasingly sophisticated in their approaches to identifying suspicious activity, commensurate with their risk profiles, for example, by building or enhancing innovative internal financial intelligence units devoted to identifying complex and strategic illicit finance, vulnerabilities and threats. 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.[18]

In addition, on January 1, 2021, the "Anti-Money Laundering Act of 2020" became law. This legislation is designed to update and make AML/CFT reflect the increasing expectations for applying technological solutions for AML/CFT. Among other things, the Act requires FinCEN to examine technological solutions to streamline the filing of Suspicious Activity Reports ("**SARs**"), create an Innovation Lab at FinCEN, and requires each of the federal financial regulators to explore new technologies for AML/CFT compliance. It also requires FinCEN to study technology, specifically AI, to determine whether it can be further leveraged to make FinCEN's data analysis more efficient and effective and whether technology can help FinCEN better disseminate information.

---

[16] ABA, UDAAP Risk Assessment Matrix (May 29, 2018), https://www.aba.com/news-research/references-guides/udaap-risk-assessment-matrix#:~:text=The%20ABA%20UDAAP%20Risk%20Assessment,your%20overall%20risk%20assessment%20framework.

[17] *See* ABA Response to the Agencies "Request for Information and Comment: Extent to Which Model Risk Management Principles Support Compliance with Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements" (June 11, 2021), https://www.aba.com/-/media/documents/comment-letter/clmodelrisk20210611.pdf?rev=c0b7f6ae4dda4a12b92d5bd986d97121.

[18] Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.

IV. General Considerations

Against the backdrop of the substantial benefits that AI is already providing banks and their customers and the extensive regulation that banks are already subject to, including with respect to AI, we respectfully raise the following general considerations in connection with the RFI.

A. Existing Regulations are Flexible Enough to Cover AI Risks

There do not appear to be significant regulatory gaps that would result in risks to the safety and soundness of individual firms or of the financial system, or to consumers with respect to the use of AI by banks. The introduction of new AI-specific regulations for banks would likely stifle innovation and put banks at a greater competitive disadvantage with respect to non-banks offering similar financial services and products that are lightly regulated today.

Because multiple legal requirements and regulatory regimes applicable to banks already exist to address the risks posed by AI (as discussed above), ABA believes the Agencies should refrain from adding additional regulatory requirements. The absence of any compelling need for regulatory intervention or guidance is especially clear in light of banks' incentives and capabilities to identify and address risks. Banks understand that AI will become integral to their core functions and are devoting considerable resources to using AI to evolve compliance and risk-management functions accordingly.

Instead, the Agencies should consider areas where they can clarify existing regulation and guidance to facilitate the use of AI and related technologies. We discuss some of these opportunities below. In this regard, it is important that supervision by the Agencies, and within each agency, be consistent with the requirements. Existing regulations, as written, do not pose an unnecessary barrier to new innovation; instead, there is often a disconnect between the intention behind the requirements and the application or interpretation of rules and guidance by supervisors. For example, bank examiners should be trained to review for AI-related issues, without being overly academic or prescriptive. Organizing interagency "horizontal reviews" in groups of banks may be helpful to address this concern.

Should the Agencies nonetheless consider further guidance or regulation on AI, we recommend that they provide a flexible, principles-based framework for the use of AI that promotes innovation while ensuring that emerging risks are captured.

B. Regulations and Guidance Should be Appropriately Interpreted and Applied to Address Risk and Use Cases

The variability of use cases raises challenges for any comprehensive AI regulation. Some applications of AI are relatively low-risk and, therefore, can be impaired by overregulation. For example, significant differences exist between algorithms that can autonomously assist a customer with trading, on the one hand, and algorithms used in a website navigation function or chatbots, on the other. Simply put, the degree of risk oversight must depend on a model's use. As Governor Brainard noted:

> Not all contexts require the same level of understanding of how machine learning models work. Users may, for example, have a much greater tolerance for opacity in a model that is used as a "challenger" to existing models and simply prompts additional questions for a

bank employee to consider relative to a model that automatically triggers bank decisions. For instance, in liquidity or credit risk management, where AI may be used to test the outcomes of a traditional model, banks may appropriately opt to use less transparent machine learning systems.[19]

Accordingly, regulation and guidance should be appropriately interpreted and applied to address both the risks and uses of AI.

C. Consumers Should Receive Consistent Protections

As noted above, banks are already subject to a comprehensive regulatory framework and proactive supervision that ensures that AI and any other new technologies are implemented carefully and do not lead to unintended consequences. When banks innovate and implement new technologies, they do so within a strong regulatory environment. This is backed by a culture of compliance and proactive supervision and examination that ensures that any risks are identified and remediated before there is consumer harm.

This level of oversight and supervision should be applied to banks and non-banks alike to ensure all consumers are protected equally, regardless of where they engage with the financial marketplace.[20] To this end, the Agencies should coordinate their approaches to AI to create consistent expectations regarding AI. As non-banks begin offering banking products and services through digital channels, the Agencies and other regulators should coordinate to ensure that these activities are appropriately monitored, emerging risks adequately captured, and all applicable legal requirements met.

The CFPB plays an important role in ensuring that customer protection requirements apply on a consistent basis with a unique opportunity to oversee and regulate non-bank financial institutions. While generally subject to the same consumer protection rules, non-banks typically lack the proactive supervision and oversight that characterizes the banking community and which ensures that regulations are applied consistently. A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for non-banks to ensure that federal consumer financial law is "enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition."[21] Experience demonstrates that consumer protection laws and regulations must be enforced in a fair and comparable way to ensure that the legal and regulatory obligations are observed. ABA believes that establishing accountability across all providers of comparable financial products and services is a fundamental mission of the CFPB.

---

[19] *See* Lael Brainard, Federal Reserve Governor, "Supporting Responsible Use of AI and Equitable Outcomes in Financial Services," Remarks at the AI Academic Symposium hosted by the Board of Governors of the Federal Reserve System, Washington, D.C. (Virtual Event) (Jan. 12, 2021), https://www.federalreserve.gov/newsevents/speech/brainard20210112a.htm.

[20] *See, e.g.*, Financial Stability Institute, Occasional Paper #17, Fintech Regulation: How to Achieve a Level Playing Field (Feb. 2021), https://www.bis.org/fsi/fsipapers17.pdf (suggesting that consumer protection requirements should be applied to any entity engaging in a particular activity regardless of entity status).

[21] Dodd-Frank Act, Section 1021(b)(4).

D. The Term AI Should Not Be Defined at This Time

The definition of the term AI in the RFI includes a very expansive (and circular) definition of the term "AI approach" as "a tool, model, process, or application that employs AI technology in some form."[22] As noted above, AI is a technology or technique, not an activity. Because ABA does not believe that AI-specific regulations are necessary at this time, we encourage the Agencies to take a principles-based approach that focuses less on AI and more on the activities that AI applies to—that is, more about risk and activities than the technology or technique. For this reason, we do not think that it is necessary for the Agencies to adopt a common or more precise definition of AI or ML at this time.

Furthermore, the broad description of "AI approach" in the RFI risks picking up practically everything that is related to AI, no matter how customary and well understood the activity actually is. In their efforts to address the risks of AI, the Agencies should guard against "scope creep," where activity is picked up that is not intended or warranted. Furthermore, the Agencies should remain cognizant of the fact that any definition of AI could become outdated as technology develops—what was novel 10 years ago is frequently commonplace today.

V. Specific Comments on the RFI

The following are comments on specific questions raised by the RFI and should be read in connection with the discussion above.

A. Explainability

ABA recognizes that some AI approaches appear to be less explainable than other approaches as to their overall functioning or how they arrive at an individual outcome in a given situation. We further recognize that an increased burden of explainability may pose different challenges in different contexts.[23] A more technical explanation may be necessary in most cases for internal purposes of aiding model development and validation and ensuring legal compliance. However, external facing explanations (for customers, system users, supervisors) are likely to take a very different form (*e.g.*, they may be more limited and simpler) and may only be required in certain higher risk/impact cases.

Consistent with the risk-based approach of the Guidance, a granular approach to explainability may not always be appropriate. The degree of explainability required should depend on materiality of risk associated with the process or activity. Consistent with the discussion in Section IV.B above, we believe the Agencies should avoid requiring higher explainability and transparency requirements than the risk or use requires. A stricter degree of explainability and model transparency may be required in certain applications, such as credit, where an explanation of the reason for credit denial is required, whereas a lesser degree of explainability may be required for a chatbot that directs a user to different places on a bank's website.

[22] *See* 86 FR at 16839, n.1.

[23] *See* 86 FR at 16839-40. *See also* Brainard, *supra* note 19.

Whether ML fits within the "model" definition set out in the prudential regulators' model risk management frameworks,[24] the Guidance provides a comprehensive framework for the supervision of models. This Guidance is appropriately principles-based and, accordingly, offers intrinsic flexibility vis-a-vis the risk to an institution and consumers posed by specific use cases.

The Agencies are already applying the Guidance in a flexible matter and addressing the unique challenges of AI and ML. They should continue this flexible approach and avoid applying existing regulation with too heavy a hand, which could make AI and ML unviable. For example, banks are demonstrating "conceptual soundness" under the Guidance by using post-hoc methods, including guardrails and/or ongoing monitoring, as appropriate. In addition, banks may use such methods to manage the risks of using third-party models when third parties may not disclose proprietary software or algorithms. For example, banks may validate the inputs to and outputs from the algorithms, and test those results against all documentation provided by the third-party vendor.

B. Fair lending

As noted, banks manage fair lending risk in the use of AI, but to increase adoption of AI more guidance is needed to support effective management of disparate impact risks in banks. The RFI asks about the need for more regulatory clarity as to providing the principal reasons for adverse action in adverse action notices. However, the areas for which more clarity in the regulatory framework is needed to facilitate the use of AI in credit underwriting are not limited to adverse action notices, but also include the appropriate manner in which ML models should be tested for fair lending risk and how ML model development processes can search for less discriminatory alternatives.

Clarifying guidance that provides illustrative examples and clarifies supervisory expectations regarding disparate impact testing and analysis would be particularly helpful. The Agencies should also aim to provide consistent and clear guidance on how to test and demonstrate that models comply not only with the ECOA, but also with the Fair Housing Act's disparate impact liability standard, consistent with the Supreme Court's *Inclusive Communities* framework.[25] These guidelines would be useful to more adequately allocate compliance resources, particularly for smaller banks.

Any fair lending clarifying guidance for AI should be jointly communicated by the CFPB, OCC, FDIC, FRB, and NCUA. In addition, we urge the Agencies to consider including the Federal Trade Commission ("**FTC**") and Conference of State Bank Supervisors. Including these regulators would help ensure that customers are treated fairly regardless of the financial institutions with which they choose to do business.

C. AI Use by Community Institutions

Community Institutions face particular challenges in implementing AI processes. Community institutions may not be able to afford AI professionals with adequate training to perform these

[24] *See supra* note 4.

[25] *Texas Department of Housing and Community Affairs et al. v. Inclusive Communities Project, Inc., et al.*, 576 U.S. 519 (2015).

functions in house. Many smaller institutions are forced to use third-party solutions to compete with the efficiency and accuracy of the AI processes at larger institutions.

However, third-party software may have embedded AI processes or predictions. Because third parties typically do not disclose proprietary software or algorithms, this raises the "black box" challenge. One way banks manage these risks is by validating the inputs to and outputs from the algorithms, and by testing those results against all documentation provided by the third-party vendor.

ABA appreciates the Agencies' willingness to address some of the hurdles, duplication, and costs associated with managing third-party risk. Increasingly, a bank's ability to compete in the marketplace will depend on its ability to leverage the expertise of third-party service providers.[26] Banks that are unable to adopt new technologies or partner with third parties may not be able to provide the products and services that customers expect.[27]

In addition, community banks rely on technology infrastructure from companies that provide software systems known as core banking platforms (core providers). Core technology supports everything from accepting deposits to originating loans, all of which tie into operating the core ledger that keeps track of customers' accounts. For many banks, their core provider is the heart of their technology infrastructure. Without the support of core providers, it is nearly impossible for community banks to adopt new technologies.

ABA has engaged with core providers through its banker-driven Core Platforms Committee, made up of community and mid-sized banks, in an effort to strengthen relationships between banks and core providers.[28] One of the key priorities that this committee has identified is data access. Community banks often struggle to access the data held in their core platforms quickly and easily, severely limiting their ability to apply AI. For community banks to remain competitive, it is critical that the core providers give them the ability to analyze their data efficiently and apply new technologies to gain insights.

D. Pilot and Innovation Programs

Pilot and Innovation programs should be leveraged in connection with AI and ML approaches, as appropriate. In this regard, we note that, in conjunction with existing BSA/AML processes, the Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing recognized that pilot programs undertaken by banks are an important means of testing and validating the effectiveness of innovative approaches.[29] The Joint Statement made clear that regulators may provide feedback, but that pilot programs in and of themselves should not subject

[26] *See* discussion *supra* in Section V.A.

[27] *See* ABA, Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services (Sep. 22, 2020), https://www.aba.com/-/media/documents/comment-letter/cl-thirdparty-20200922.pdf?rev=b29d5ba67fde4e24bbb143bcf2069604.

[28] *See* ABA, Core Platforms Committee, https://www.aba.com/member-tools/committees-councils/core-platforms-committee.

[29] *See supra* note 18.

banks to supervisory criticism even if the programs ultimately prove unsuccessful. Specific to our purposes, the Joint Statement noted:

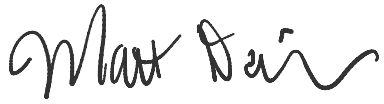
> For example, when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, the Agencies will not automatically assume that the banks' existing processes are deficient. In these instances, the Agencies will assess the adequacy of banks' existing suspicious activity monitoring processes independent of the results of the pilot program. Further, the implementation of innovative approaches in banks' BSA/AML compliance programs will not result in additional regulatory expectations.

While we support the creation of pilot and innovation programs, use of such programs should be completely voluntary. Accordingly, banks should be free to implement AI solutions in the normal course of business without utilizing pilot or innovation programs if they so choose.

VI. Conclusion

ABA believes the Agencies' work to better understand the risks and opportunities with the application of AI in financial services is important. This technology is critical to our global competitiveness. AI makes banking services better, cheaper, and more widely available, and will continue to do so. While these benefits do not come without risks, we believe that the robust bank regulatory structure already captures these risks today. Accordingly, the Agencies should avoid additional regulation of AI use by banks and provide a flexible framework that can encourage innovation while mitigating risks. We urge the Agencies to make appropriate clarifications, such as those outlined in this letter, to enable adoption of this important technology and to ensure that these principles are applied consistently for all financial services providers.

Sincerely,



Matthew A. Daigler

Vice President & Senior Counsel
Innovation Policy and Regulation