**CFPB Summary re: Request for Information/Comment on Financial Institutions' Use of Artificial Intelligence/Machine Learning**

**Docket No. CFPB-2021-0004**

*Prepared by the Legislative & Regulatory Affairs Division*

*April 2021*

The OCC, Federal Reserve Board, FDIC, NCUA and CFPB (collectively, "the agencies") issued a Request for Information (RFI)/Comments on financial institutions' use of artificial intelligence (AI), including machine learning (ML). The purpose of the RFI is to understand respondents' views on the use of AI by financial institutions in their provision of services to customers and for other business or operational purposes; appropriate governance; risk management and controls over AI; and any challenges in developing, adopting, and managing AI. The RFI also solicits respondents' views on the use of AI in financial services to assist in determining whether any clarifications from the agencies would be helpful for financial institutions' use of AI in a safe and sound manner and in compliance with applicable laws/regulations, including those related to consumer protection.

Comments are due by June 1, 2021. The proposed rule can be access here.

**Summary:**

The agencies support responsible innovation by financial institutions that include the identification and management of risks associated with the use of new technologies and techniques. With appropriate governance, risk management, and compliance management, financial institutions' use of innovative technologies/techniques such as those involving AI, has the potential to augment business decision-making, and enhance services available to consumers and businesses. The appendix of this RFI includes a non-comprehensive list of laws, regulations, and other agency issuances that may be relevant to the use of AI approaches by agency-supervised institutions. Uses of AI by financial institutions include (but are not limited to):

- Flagging unusual transactions – this involves employing AI to identify potential suspicious, anomalous or outlier transactions (fraud detection and financial crime monitoring)

- Personalization of customer services – AI technologies, such as voice recognition and natural language processing (NLP), are used to improve customer experience and to gain efficiencies in the allocation of financial institution resources.

- Credit decisions – this involves the use of AI to inform credit decisions in order to enhance or supplement existing techniques.

- Risk Management – AI may be used to augment risk management and control practices. For example, the AI approach might be used as a check on a more traditional credit

model. Financial institutions may use AI to enhance credit monitoring, payment collections, loan restructuring and recovery, etc.

- Textual Analysis - this refers to the use of NLP for handling unstructured data (generally text) and obtaining insights from that data or improving efficiency of existing processes.

- Cybersecurity - AI may be used to detect threats and malicious activity, reveal attackers, identify compromised systems and support threat mitigation.

**Potential Benefits of AI**

The Bureau recognizes the potential benefits of AI such as:

- Improved efficiency
- Enhanced performance and cost reduction
- Identification of relationships among variables that are not intuitive
- Facilitates processing of large/detailed data sets
- More accurate, lower-cost and faster underwriting
- Expanded credit access for consumers/small businesses

**Potential Risks of AI**

The Bureau notes the importance of financial institutions having processes in place to identify and manage potential risks associated with AI such as:

- Operational vulnerabilities such as internal process/control breakdowns, cyber threats, information technology lapses, risks associated with the use of third parties, and model risks
- Heightened consumer protection risks such as possible UDAAP/UDAP violations or privacy concerns.

- AI may present particular risk management challenges to financial institutions in the areas of explainability, data usage and dynamic updating.

<u>Explainability</u>

- This refers to how an AI approach uses inputs to produce outputs. Lack of explainability can prohibit financial institution management's understanding of the conceptual soundness of an AI approach. Lack of explainability can also inhibit independent review and audit and make compliance with laws and regulations, including consumer protection requirements, more challenging.

Broader or More Intensive Data Usage

- Data plays an important role in AI. Due to the fact that an AI algorithm is dependent upon the training data, an AI system generally reflects any limitations of that dataset. As a result, AI may perpetuate or even amplify bias or inaccuracies inherent in the training data or make incorrect predictions if the data set is incomplete or non-representative.

Dynamic Updating

- Some AI approaches have the capacity to update on their own, sometimes without human interaction, often known as "dynamic updating." Monitoring and tracking an AI approach that evolves on its own can present challenges in review and validation.

**Request for Comments:**

In this RFI, the agencies are seeking information on financial institutions' risk management practices related to AI; barriers or challenges facing financial institutions when developing, adopting and managing AI and its risks; and benefits to financial institutions and their customers from the use of AI. The RFI also solicits respondents' views on the use of AI in financial services which will help the agencies determine whether any clarification would be helpful for financial institutions' use of AI in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection.

The agencies are also asking particular questions regarding the following:

Explainability:

To address the lack of explainability of certain AI approaches, researchers have developed techniques to help explain predictions or categorizations. These techniques are often referred to as "post-hoc" methods, because they are used to interpret the outputs rather than the design.

Related Questions

- How do financial institutions identify and manage risks relating to AI explainability? What barriers or challenges for explainability exist for developing, adopting, and managing AI?

- How do financial institutions use post-hoc methods to assist in evaluating conceptual soundness? How common are these methods? Are there limitations of these methods (whether to explain an AI approach's overall operation or to explain a specific prediction or categorization)? If so, please provide details on such limitations.

- For which uses of AI is lack of explainability more of a challenge? Please describe those challenges in detail. How do financial institutions account for and manage the varied challenges and risks posed by different uses?

Risks from Broader or More Intensive Data Processing and Usage:

Like other systems, AI is designed to interact directly with training data to identify correlations and patterns and use that information for prediction or categorization. This means that data quality is important for AI. If the training data are biased or incomplete, AI may incorporate those shortcomings into its predictions or categorizations. The importance of practices such as data quality assessments to determine relevance and suitability of data used in a model, may be heightened in the use of AI.

Related Questions:

- How do financial institutions using AI manage risks related to data quality and data processing? How, if at all, have control processes or automated data quality routines changed to address the data quality needs of AI? How does risk management for alternative data compare to that of traditional data? Are there any barriers or challenges that data quality and data processing pose for developing, adopting, and managing AI? If so, please provide details on those barriers or challenges.

- Are there specific uses of AI for which alternative data are particularly effective?

Overfitting:

Overfitting can occur when an algorithm "learns" from idiosyncratic patterns in the training data that are not representative of the population as a whole. Overfitting is not unique to AI, but it can be more pronounced in AI than with traditional models. Undetected overfitting could result in incorrect predictions or categorizations.

Related Questions:

- How do financial institutions manage AI risks relating to overfitting? What barriers or challenges, if any, does overfitting pose for developing, adopting, and managing AI? How do financial institutions develop their AI so that it will adapt to new and potentially different populations (outside of the test and training data)?

Cybersecurity Risk:

Like other data-intensive technologies, AI may be exposed to risk, from a variety of criminal cybersecurity threats. For example, AI can be vulnerable to "data poisoning attacks," which attempt to corrupt and contaminate training data to compromise the system's performance.

Related Questions:

- Have financial institutions identified particular cybersecurity risks or experienced such incidents with respect to AI? If so, what practices are financial institutions using to manage cybersecurity risks related to AI? Please describe any barriers or challenges to

the use of AI associated with cybersecurity risks. Are there specific information security or cybersecurity controls that can be applied to AI?

Dynamic Updating:

A particular characteristic of some AI is the ability for it to learn or evolve over time, especially as it captures new training data. This can present challenges for validating, monitoring, tracking and documenting the AI approach.

Related Questions:

- How do financial institutions manage AI risks relating to dynamic updating? Describe any barriers or challenges that may impede the use of AI that involve dynamic updating. How do financial institutions gain an understanding of whether AI approaches producing different outputs over time based on the same inputs are operating as intended?

AI Use by Community Institutions:

A financial institution's AI strategy, use of AI, and associated risk management practices could vary substantially based on the financial institution's size, complexity of operations, business model, staffing and risk profile, and this could affect the corresponding risks that arise. Community institutions may be more likely to use third-party AI approaches or rely on third party services that use AI. This may pose different challenges in a financial institution's adoption of AI.

Related Questions:

- Do community institutions face particular challenges in developing, adopting, and using AI? If so, please provide detail about such challenges. What practices are employed to address those impediments or challenges?

Oversight of Third Parties:

Financial institutions may opt to use AI developed by third parties, rather than developed internally. Existing agency guidance describes information/risks that may be relevant to financial institutions when selecting third party approaches and sets out principles for the validation of such third-party approaches.

Related Questions:

- Please describe any particular challenges or impediments financial institutions face in using AI developed or provided by third parties and a description of how financial institutions manage the associated risks. Please provide detail on any challenges or impediments. How do those challenges or impediments vary by financial institution size and complexity?

Fair Lending:

Depending on the specific use, 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.

Related Questions:

- What techniques are available to facilitate or evaluate the compliance of AI-based credit determination approaches with fair lending laws or mitigate risks of noncompliance? Please explain these techniques and their objectives, limitations of those techniques, and how those techniques relate to fair lending legal requirements?

- What are the risks that AI can be biased and/or result in discrimination on prohibited bases? Are there effective ways to reduce risk of discrimination, whether during development, validation, revision and/or use? What are some of the barriers to or limitations of those methods?

- As part of their compliance management systems, financial institutions may conduct fair lending risk assessments by using models designed to evaluate fair lending risks. What challenges, if any, do financial institutions face when applying internal model risk management principles and practices to development, validation, or use of fair lending risk assessment models based on AI?

- The Equal Credit Opportunity Act (ECOA), which is implemented by Regulation B, requires creditors to notify an applicant of the principal reasons for taking adverse action for credit or to provide an applicant a disclosure of the right to request those reasons. What approaches can be used to identity the reasons for taking adverse action on a credit application, when AI is employed? Does Regulation B provide sufficient clarity for the statement of reasons for adverse action when AI is used? If not, please describe in detail any opportunities for clarity.

Additional Considerations:

- To the extent not already discussed, please identity any additional uses of AI by financial institutions and any risk management challenges or other factors that may impede adoption and use of AI.

- To the extent not already discussed, please identify any benefits or risks to financial institutions' customers or prospective customers from the use of AI by those financial institutions. Please provide any suggestions on how to maximize benefits or address any identified risks.