DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency
Docket ID OCC-2020-0049

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Docket No. OP- 1743

FEDERAL DEPOSIT INSURANCE CORPORATION
RIN 3064-ZA24

BUREAU OF CONSUMER FINANCIAL PROTECTION
Docket No. CFPB-2021-0004

NATIONAL CREDIT UNION ADMINISTRATION
Docket No. NCUA-2021-0023

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

AGENCY: Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency (agencies).

ACTION: Request for information and comment.

SUMMARY: The agencies are gathering information and comments on financial institutions' use of artificial intelligence (AI), including machine learning (ML). The purpose of this request for information (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 and regulations, including those related to consumer protection.

DATES: Comments must be received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Interested parties are encouraged to submit written comments jointly to all of the agencies. Commenters are encouraged to use the title "*Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning*" to facilitate the organization and distribution of comments among the agencies. Commenters are also encouraged to identify the number of the specific question for comment to which they are responding. Please send comments by one method only and should be directed to:

OCC: Commenters are encouraged to submit comments through the Federal eRulemaking Portal. Please use the title "Request for Information on Financial Institutions' Use of Artificial Intelligence, including Machine Learning; Request for Comment" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- *Federal eRulemaking Portal – Regulations.gov:*

Go to *https://regulations.gov/*. Enter "Docket ID OCC-2020-0049" in the Search Box and click "Search." Public comments can be submitted via the "Comment" box below the displayed document information or by clicking on the document title and then clicking the "Comment" box on the top-left side of the screen. For help with submitting effective comments please click on "Commenter's Checklist." For assistance with the *Regulations.gov* site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*.

- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street, SW., suite 3E-218, Washington, DC 20219.
- *Hand Delivery/Courier:* 400 7th Street, SW., suite 3E-218, Washington, DC 20219.

Instructions: You must include "OCC" as the agency name and "Docket ID OCC-2020-0049" in your comment. In general, the OCC will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information provided such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this action by the following method:

- *Viewing Comments Electronically – Regulations.gov:* Go to *https://regulations.gov/*. Enter "Docket ID OCC-2020-0049" in the Search Box and click "Search." Click on the "Documents" tab and then the document's title. After clicking the document's title, click the "Browse Comments" tab. Comments can be viewed and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Results" options on the left side of the screen. Supporting materials can be viewed by clicking on the "Documents" tab and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Documents Results" options on the left side of the screen." For assistance with the *Regulations.gov* site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*. The docket may be viewed after the close of the comment period in the same manner as during the comment period.

***Board*:** You may submit comments, identified by Docket No. OP-1743, by any of the following methods:

- *Agency Web Site*: http://www.federalreserve.gov. Follow the instructions for submitting comments at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.
- *E-mail*: regs.comments@federalreserve.gov. Include docket number in the subject line of the message.
- *FAX*: (202) 452-3819 or (202) 452-3102.

Mail: Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551. All public comments will be made available on the Board's website at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, unless modified for technical reasons or to remove personally identifiable information or other confidential information at the commenter's request. Accordingly, your comments will not be edited to remove any identifying or contact information. Public comments may also be viewed in paper in Room 146, 1709 New York Avenue NW, Washington, DC 20006, between 9:00 a.m. and 5:00 p.m. on weekdays.

FDIC:

- *Agency Website: https://www.fdic.gov/regulations/laws/federal/*. Follow the instructions for submitting comments on the agency's website.
- *Email: Comments@fdic.gov*. Include RIN 3064-ZA24 in the subject line of the message.
- *Mail:* James P. Sheesley, Assistant Executive Secretary, Attention: Comments-RIN 3064-ZA24, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.
- *Hand Delivery/Courier:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

Public Inspection: All comments received will be posted without change to

https://www.fdic.gov/regulations/laws/federal/—including any personal information provided—for public inspection. Paper copies of public comments may be ordered from the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226 or by telephone at (877) 275-3342 or (703) 562-2200.

Bureau of Consumer Financial Protection (Bureau):

You may submit responsive information and other comments, identified by Docket No. CFPB-2021-0004, by any of the following methods:

- *Federal eRulemaking Portal*: Go to http://www.regulations.gov. Follow the instructions for submitting comments.
- *Email*: *2021-RFI-AI@cfpb.gov*. Include Docket No. CFPB-2021-0004 in the subject line of the message.
- *Mail/Hand Delivery/Courier*: Comment Intake, Bureau of Consumer Financial Protection, 1700 G Street, NW, Washington, DC 20552. Please note that due to circumstances associated with the COVID-19 pandemic, the CFPB discourages the submission of comments by mail, hand delivery, or courier.
- *Instructions*: The Bureau encourages the early submission of comments. All submissions must include the document title and docket number. Because paper mail in the Washington, DC area and at the Bureau is subject to delay, and in light of difficulties associated with mail and hand deliveries during the COVID-19 pandemic, commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to http://www.regulations.gov. In addition, once the Bureau's headquarters reopens, comments will be available for public inspection and copying at 1700 G Street, NW, Washington, DC 20552, on

official business days between the hours of 10 a.m. and 5 p.m. Eastern Time. At that time, you can make an appointment to inspect the documents by calling 202-435-7275.

All submissions in response to this RFI, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Please do not include in your submissions sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, or other information that you would not ordinarily make public, such as trade secrets or confidential commercial information. Submissions will not be edited to remove any identifying or contact information, or other information that you would not ordinarily make public. If you wish to submit trade secret or confidential commercial information, please contact the individuals listed in the FOR FURTHER INFORMATION CONTACT section below. Information submitted to the Bureau will be treated in accordance with the Bureau's Rule on the Disclosure of Records and Information, 12 CFR part 1070 *et seq*.

NCUA: You may submit comments to the NCUA, Docket No. NCUA –2021-0023, by any of the methods set forth below. Commenters are encouraged to submit comments through the Federal eRulemaking Portal, if possible. Please use the title ''Request for Information and Comment: Financial Institutions' Use of Artificial Intelligence, including Machine Learning'' to facilitate the organization and distribution of the comments. *(Please send comments by one method only)*:

- *Federal eRulemaking Portal: www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* (703) 518–6319.

- *Mail:* Address to Melane Conyers-Ausbrooks, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, VA. 22314-3428.

In general, the NCUA will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information that you provide such as name and address information, email addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this Request for Information by any of the following methods:

- *Viewing Comments Electronically:* You may view all public comments on the Federal eRulemaking Portal at http://www.regulations.gov as submitted, except for those NCUA cannot post for technical reasons.
- Due to social distancing measures in effect, the usual opportunity to inspect paper copies of comments in the NCUA's law library is not currently available. After social distancing measures are relaxed, visitors may make an appointment to review paper copies by calling (703) 518–6540 or emailing OGCMail@ncua.gov.

FOR FURTHER INFORMATION CONTACT:

OCC: Kevin Greenfield, Deputy Comptroller for Operational Risk, Norine Richards, Director for Bank Technology Operations, Paul Reymann, Director for Consumer Compliance Policy, or Siobhan Williams, Bank Information Technology Analyst, Bank Supervision Policy Department, (202) 649-6550; Beth Knickerbocker, Chief Innovation Officer, or Maggie Colvin, Innovation

Officer, Office of Innovation, (202) 649-5200; Alireza Ebrahim, Senior Financial Economist, Risk Analytics Division, (202) 649-5515; or Jorge D. Aguilar, Counsel, Chief Counsel's Office, (202) 649-7187.

Board: David Palmer, Lead Financial Institution Policy Analyst, (202) 452-2904, Jeff Ernst, Lead Financial Institution Policy Analyst, (202) 452-2814, or Kavita Jain, Deputy Associate Director, (202) 452-2062, Division of Supervision and Regulation; Dana Miller, Senior Counsel, (202) 452-2751, or Carol Evans, Associate Director, (202) 452-2051, Division of Consumer and Community Affairs, or Patricia Yeh, Senior Counsel, (202) 452-3089, or Gavin Smith, Senior Counsel, (202) 452-3474, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551. For the hearing impaired only, Telecommunication Device for the Deaf (TDD), (202) 263-4869.

FDIC: Sumaya Muraywid, Senior Examination Specialist, Division of Risk Management Supervision, (202) 898–3904, smuraywid@fdic.gov, David Friedman, Senior Policy Analyst, Division of Depositor and Consumer Protection, 202-898-7168, dfriedman@fdic.gov; or Chris Ledoux, Corporate Expert, Legal Division, 202-898-3535, cledoux@fdic.gov.

Bureau: Albert D. Chang, Senior Counsel, Office of Innovation, (202) 450-7299*;* Patrice Alexander Ficklin, Fair Lending Director, Office of Fair Lending & Equal Opportunity, (202) 435-7205; and Kathryn Lazarev, Senior Counsel, Office of Regulations, (202) 435-7700. If you require this document in an alternative electronic format, please contact *CFPB_Accessibility@cfpb.gov*

NCUA: Timothy Segerson, Deputy Director, Office of Examination & Insurance, 703-518-6300; Chrisanthy Loizos, Senior Trial Attorney, Office of General Counsel, 703-518-6540; Joe Goldberg, Director, Division of Consumer Compliance Policy and Outreach, 703-518-1142.

SUPPLEMENTARY INFORMATION

Background Information

The agencies support responsible innovation by financial institutions that includes 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 and 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.[1]

Financial institutions are exploring AI-based applications in a variety of fields. Uses of AI by financial institutions include (but are not limited to):

- *Flagging unusual transactions*. This involves employing AI to identify potentially suspicious, anomalous, or outlier transactions (e.g., fraud detection and financial crime monitoring). It involves using different forms of data (e.g., email text, audio data – both structured[2] and unstructured), with the aim of identifying fraud or anomalous transactions with greater accuracy and timeliness. It also includes identifying transactions for Bank

[1] In this RFI, the term "AI approach" refers to a tool, model, process, or application that employs AI technology in some form.

[2] The term "structured data" generally refers to a set of data that has been systematically organized or arranged.

Secrecy Act/anti-money laundering investigations, monitoring employees for improper practices, and detecting data anomalies.

- *Personalization of customer services*. AI technologies, such as voice recognition and natural language processing (NLP)[3], are used to improve customer experience and to gain efficiencies in the allocation of financial institution resources. One example is the use of chatbots[4] to automate routine customer interactions, such as account opening activities and general customer inquiries. AI is leveraged at call centers to process and triage customer calls to provide customized service. These technologies are also used to better target marketing and customize trade recommendations.
- *Credit decisions.* This involves the use of AI to inform credit decisions in order to enhance or supplement existing techniques. This application of AI may use traditional data or employ alternative data[5] (such as cash flow transactional information from a bank account).
- *Risk management.* AI may be used to augment risk management and control practices. For example, an AI approach might be used to complement and provide a check on another, more traditional credit model. Financial institutions may also use AI to enhance credit monitoring (including through early warning alerts), payment collections, loan restructuring and recovery, and loss forecasting. AI can assist internal audit and independent risk management to increase sample size (such as for testing), evaluate risk,

[3] "Natural language processing" generally refers to the use of computers to understand or analyze natural language text or speech.

[4] The term "chatbot" generally refers to a software application used to conduct an on-line chat conversation via text or text-to-speech, in lieu of providing direct contact with a live human agent.

[5] For the purposes of this RFI, alternative data means information not typically found in the consumer's credit files of the nationwide consumer reporting agencies or customarily provided by consumers as part of applications for credit.

and refer higher-risk issues to human analysts. AI may also be used in liquidity risk management, for example, to enhance monitoring of market conditions or collateral management.

- *Textual analysis*. Textual analysis refers to the use of NLP for handling unstructured data (generally text) and obtaining insights from that data or improving efficiency of existing processes. Applications include analysis of regulations, news flow, earnings reports, consumer complaints, analyst ratings changes, and legal documents.
- *Cybersecurity.* AI may be used to detect threats and malicious activity, reveal attackers, identify compromised systems, and support threat mitigation. 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.

Potential Benefits of AI

AI has the potential to offer improved efficiency, enhanced performance, and cost reduction for financial institutions, as well as benefits to consumers and businesses. AI can identify relationships among variables that are not intuitive or not revealed by more traditional techniques. AI can better process certain forms of information, such as text, that may be impractical or difficult to process using traditional techniques. AI also facilitates processing significantly large and detailed datasets, both structured and unstructured, by identifying patterns or correlations that would be impracticable to ascertain otherwise.

Other potential AI benefits include more accurate, lower-cost, and faster underwriting, as well as expanded credit access for consumers and small businesses that may not have obtained credit

under traditional credit underwriting approaches. AI applications may also enhance an institution's ability to provide products and services with greater customization.

Potential Risks of AI

It is important for financial institutions to have processes in place for identifying and managing potential risks associated with AI, as they do for any process, tool, or model employed. Many of the potential risks associated with using AI are not unique to AI. For instance, the use of AI could result in operational vulnerabilities, such as internal process or control breakdowns, cyber threats, information technology lapses, risks associated with the use of third parties, and model risk, all of which could affect a financial institution's safety and soundness. The use of AI can also create or heighten consumer protection risks, such as risks of unlawful discrimination, unfair, deceptive, or abusive acts or practices (UDAAP) under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), unfair or deceptive acts or practices (UDAP) under the Federal Trade Commission Act (FTC Act), or privacy concerns.

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

- *Explainability*. For the purposes of this RFI, explainability refers to how an AI approach uses inputs to produce outputs. 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). Lack of explainability can pose different challenges in different contexts. Lack of explainability can also inhibit

financial institution management's understanding of the conceptual soundness[6] of an AI approach, which can increase uncertainty around the AI approach's reliability, and increase risk when used in new contexts. 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 Us*age. Data plays a particularly important role in AI. In many cases, AI algorithms identify patterns and correlations in training data without human context or intervention, and then use that information to generate predictions or categorizations.[7] Because the AI algorithm is dependent upon the training data, an AI system generally reflects any limitations of that dataset. As a result, as with other systems, AI may perpetuate or even amplify bias or inaccuracies inherent in the training data, or make incorrect predictions if that 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, particularly when a change in external circumstances (e.g., economic downturns and financial crises) may cause inputs to vary materially from the original training data. Dynamic updating techniques can produce changes that range from minor adjustments to existing elements of a model to the introduction of entirely new elements.

[6] For this RFI, the term "conceptual soundness" generally refers to the quality of the theory, design, methodology, data, developmental testing, and confirmation that an approach is appropriate for the intended use.

[7] In this context, training data are the data used to develop and calibrate an AI approach; for example, a financial institution might use a large dataset of past fraudulent transactions to train the approach to detect and prevent future fraud.

Request for Comment

As discussed, the agencies recognize that AI has the potential to offer improved efficiency, enhanced performance, and cost reduction for financial institutions, as well as benefits to consumers and businesses. In this RFI, the agencies are seeking information on financial institutions' risk management practices related to the use of 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.

Explainability

Understanding the conceptual soundness of any model, tool, application, or system aids in managing its risks including those related to lack of explainability. The importance of conceptual soundness is described in existing agency guidance and is well established in industry practice. For traditional approaches, conceptual soundness is foundational both to development and validation/independent review. In the case of certain less transparent AI approaches, however, evaluations of conceptual soundness can be complicated. The underlying theory and logic may be less accessible to users than that of traditional approaches or more transparent AI approaches. Without insight into an approach's general operating principles, financial institution management may not be able to evaluate with confidence how the system will function in unforeseen circumstances. To address 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.

> *Question 1*: 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?
>
> *Question 2:* 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.
>
> *Question 3*: 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.

AI may use alternative datasets in certain applications (such as credit underwriting, fraud detection, and trading) in ways that can assist in identifying related trends or predictions that may be difficult to identify with traditional methods. 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. Finally, in many cases, AI developers process or optimize raw data so that the data can be better used for training. Various data processing techniques exist, some of which may affect performance.

Question 4: 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.

Question 5: 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.

Question 6: 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.

Question 7: 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. Over time, this could result in drift (i.e., the AI approach could change) as it learns from the new data. This can present challenges for validating, monitoring, tracking, and documenting the AI approach, including for persons conducting an independent review. It may be important to understand whether an AI approach that was independently reviewed initially has significantly evolved over time (e.g., using an influx of new data). Dynamic updating can also affect how results are tracked over time. For example, initial performance thresholds chosen to monitor the approach could become less meaningful if the AI approach has significantly changed to focus on different target outcomes. Similar risks can arise with AI approaches that are not updated as their context evolves, since they are more closely tuned to their training data. For example, AI approaches that are validated in one circumstance may not perform well in another, and an independent review conducted in a previous context may no longer be accurate in new circumstances.

Question 8: 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 (e.g., level of expertise of AI or insight into the third-party AI approach) in a financial institution's adoption of AI.

> *Question 9*: 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 develop the approach internally. Existing agency guidance (as noted in the Appendix) describes information and risks that may be relevant to financial institutions when selecting third-party approaches (including ones using AI) and sets out principles for the validation of such third-party approaches.

> *Question 10*: 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. For example, it may be challenging to verify that a less transparent and explainable approach comports with fair lending laws.

Question 11: What techniques are available to facilitate or evaluate the compliance of AI-based credit determination approaches with fair lending laws or mitigate risks of non-compliance? Please explain these techniques and their objectives, limitations of those techniques, and how those techniques relate to fair lending legal requirements.

Question 12: 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?

Question 13: To what extent do model risk management principles and practices aid or inhibit evaluations of AI-based credit determination approaches for compliance with fair lending laws?

Question 14: As part of their compliance management systems, financial institutions may conduct fair lending risk assessments by using models designed to evaluate fair lending risks ("fair lending risk assessment models"). What challenges, if any, do financial institutions face when applying internal model risk management principles and practices to the development, validation, or use of fair lending risk assessment models based on AI?

Question 15: 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 identify 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

Question 16: To the extent not already discussed, please identify any additional uses of AI by financial institutions and any risk management challenges or other factors that may impede adoption and use of AI.

Question 17: 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.

Appendix: Laws, Regulations, Supervisory Guidance, and other Agency Statements Relevant to AI

This Appendix contains a list of laws, regulations, supervisory guidance, and other statements issued by the agencies that may be relevant to AI. This includes existing laws and regulations relating to safety and soundness and consumer protection. The items below do not constitute an exhaustive list; other laws, regulations, guidance, and statements may be relevant based on the particular facts and circumstances. Some laws and regulations are applicable to any process or tool a financial institution employs, regardless of whether a financial institution utilizes AI or how.

Laws and Regulations

- Section 39 of the Federal Deposit Insurance Act as implemented through the agencies' safety and soundness regulations[8]

[8] Refer to the Interagency Guidelines Establishing Standards for Safety and Soundness, 12 CFR 364, Appendix A (FDIC); 12 CFR 263 (FRB); 12 CFR 30, appendix A (OCC).

- Sections 501 and 505(b) of Gramm-Leach-Bliley Act as implemented through the agencies' regulations and standards, including Interagency Guidelines Establishing Information Security Standards[9]
- Fair Credit Reporting Act (FCRA) / Reg. V
- Equal Credit Opportunity Act (ECOA) / Reg. B
- Fair Housing Act (FHA)
- Section 5 of the Federal Trade Commission Act (prohibiting UDAP) and sections 1031 and 1036 of the Dodd-Frank Act (prohibiting unfair, deceptive, or abusive acts or practices (UDAAP))

Supervisory Guidance and Statements

- Interagency Statement on the Use of Alternative Data in Credit Underwriting[10]
- Supervisory Guidance on Model Risk Management[11]
- Third-Party/Outsourcing Risk Management[12]

---

[9] Refer to the Interagency Guidelines Establishing Information Security Standards, 12 CFR 364, Appendix B (FDIC); 12 CFR 208, Appendix D-2 and 12 CFR 225, Appendix F (FRB); 12 CFR 30, appendix B (OCC); Guidelines for Safeguarding Member Information, 12 CFR 748, Appendix A (NCUA).

[10] Refer to FDIC FIL-82-2019, https://www.fdic.gov/news/financial-institution-letters/2019/fil19082.html; Federal Reserve CA Letter 19-11, https://www.federalreserve.gov/supervisionreg/caletters/caletters.htm; and OCC Bulletin 2019-62, https://www.occ.gov/news-issuances/bulletins/2019/bulletin-2019-62.html.

[11] Refer to the "Supervisory Guidance on Model Risk Management," Federal Reserve SR Letter 11-7, https://www.federalreserve.gov/supervisionreg/srletters/srletters.htm; OCC Bulletin 2011-12, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html; and FDIC Financial Institution Letter (FIL)-22-2017, https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.html.

[12] FDIC: Guidance for Managing Third-Party Risk (FIL)-44-2008, https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html; OCC Bulletin 2013-29, OCC Bulletin 2020-10; NCUA: Evaluating Third Party Relationships, Supervisory Letter (SL) 07-01 (Oct. 2007); and FRB: Guidance on Outsourcing Risk (SR 13-19), https://www.federalreserve.gov/supervisionreg/srletters/srletters.htm.

- New, Modified, or Expanded Bank Products and Services[13]
- CFPB Innovation Spotlight on Providing Adverse Action Notices When Using AI/ML Models [14]

Examination Manuals/Procedures/Other Resources

- Federal Financial Institutions Examination Council Information Technology Examination Handbook[15]
- Consumer Compliance Manuals and Booklets[16]
- Interagency Fair Lending Examination Procedures[17]
- CFPB Examination Procedures, ECOA Baseline Review Module 5: Fair Lending Risks Related to Models[18]

Blake J. Paulson
Acting Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System.

Ann Misback,
Secretary of the Board.

---

[13] OCC Bulletin 2017-43, https://www.occ.treas.gov/news-issuances/bulletins/2017/bulletin-2017-43.html; and NCUA 19-CU-04 (Dec. 2019), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/use-alternative-data-credit-underwriting.

[14] Patrice Alexander Ficklin, Tom Pahl, and Paul Watkins, CFPB Blog, Innovation spotlight: Providing adverse action notices when using AI/ML models (July 7, 2020), *available at* https://www.consumerfinance.gov/about-us/blog/innovation-spotlight-providing-adverse-action-notices-when-using-ai-ml-models/.

[15] FFIEC IT Handbook, https://ithandbook.ffiec.gov/.

[16] OCC *Consumer Compliance* series of *Comptroller's Handbook* booklets, https://www.occ.treas.gov/topics/supervision-and-examination/consumer-compliance/index-consumer-compliance.html; NCUA: Evaluating Compliance Risk – Updated Compliance Indicators, SL-17-01 (March 2017), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/use-alternative-data-credit-underwriting.

[17] Interagency Fair Lending Examination Procedures, https://www.ffiec.gov/PDF/fairlend.pdf.

[18] See, CFPB ECOA Baseline Review, p. 24, https://files.consumerfinance.gov/f/documents/cfpb_supervision-and-examination-manual_ecoa-baseline-exam-procedures_2019-04.pdf.

Federal Deposit Insurance Corporation.
Dated at Washington, DC, on or about February 25, 2021.
James P. Sheesley,
Assistant Executive Secretary.

David Uejio,
Acting Director, Bureau of Consumer Financial Protection.

Melane Conyers-Ausbrooks,
Secretary of the Board,
National Credit Union Administration.