Billing Code 4810-AK-P
DEPARTMENT OF THE TREASURY

Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector

AGENCY: Departmental Offices, Department of the Treasury.

ACTION: Request for information.

SUMMARY: The U.S. Department of the Treasury (Treasury) is seeking comment through this request for information (RFI) on the uses, opportunities and risks presented by developments and applications of artificial intelligence (AI) within the financial sector. Treasury is interested in gathering information from a broad set of stakeholders in the financial services ecosystem, including those providing, facilitating, and receiving financial products and services, as well as consumer and small business advocates, academics, nonprofits, and others.

DATES: Written comments and information are requested on or before [INSERT DATE THAT IS 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Please submit comments electronically through the Federal eRulemaking Portal at http://www.regulations.gov, in accordance with the instructions on that site. Comments should be captioned with "Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector." In general, Treasury will post all comments to https://www.regulations.gov, including any business or personal information provided such as names, addresses, email addresses, or telephone numbers. All comments, including attachments and other supporting materials, are part of the public record and subject to public disclosure and should not include confidential information, including confidential supervisory information. You should submit only information that you wish to make available publicly. Where appropriate, a comment should include a short Executive Summary (no more than five single-spaced pages).

FOR FURTHER INFORMATION CONTACT: Jeanette Quick, Deputy Assistant Secretary for Financial Institutions Policy, 202-622-6107, jeanette.quick@treasury.gov; Moses Kim, Director, Office of Financial Institutions Policy, 202-622-5824, w.moses.kim@treasury.gov; or Liang Jensen, Senior Policy Advisor, Office of Financial Institutions Policy, 202-622-2685, liang.jensen@treasury.gov. [Persons who have difficulty hearing or speaking may access these numbers via TTY by calling the toll-free Federal Relay Service at (800) 877–8339.]

SUPPLEMENTARY INFORMATION:

I. Background

Treasury supports responsible innovation and competition in the financial sector and seeks to promote a financial system that delivers inclusive and equitable access to financial services that meet the needs of consumers, businesses, and investors, while maintaining stability and market integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats. The use of AI is rapidly evolving, and Treasury is committed to continuing to monitor technological developments and their application and potential impacts in financial services to help inform any potential policy deliberations or actions.

To that end, Treasury is seeking comment on the uses of AI in the financial services sector and the opportunities and risks presented by developments and applications of AI within the sector. Treasury welcomes feedback from all parties that may have a perspective as to implications of AI in the financial sector on any question. "Financial institutions" in this RFI

includes any company that facilitates or provides financial products or services.[1] The RFI also seeks input on the potential opportunities and risks of financial institutions' use of AI and how AI may affect impacted entities. "Impacted entities" in this RFI includes consumers, investors, financial institutions, businesses, regulators, end-users, and any other entity impacted by financial institutions' use of AI.

Prior and ongoing engagement

This RFI effort is one of many ways that Treasury is engaging with stakeholders in improving Treasury's understanding of the developments and application of AI within the financial services sector.

In November 2022, Treasury explored opportunities and risks related to the use of AI in its report assessing the impact of new entrant non-bank firms on competition in consumer finance markets, for which Treasury conducted extensive outreach.[2] Among other findings, that report found that innovations in AI are powering many non-bank firms' capabilities and product and service offerings. The report noted that firms' use of AI may help expand the provision of financial products and services to consumers, particularly in the credit space. The report also found that, in deploying AI models and tools, firms use a greater amount and variety of data than in the past, leading to an unprecedented demand for consumer data, which presents new data privacy and surveillance risks. Additionally, the report identified concerns related to bias and

[1] To the extent applicable, "financial institutions" in this RFI includes banks, credit unions, insurance companies, non-bank financial companies, financial technology companies (also known as fintech companies), asset managers, broker-dealers, investment advisors, other securities and derivatives markets participants or intermediaries, money transmitters, and any other company that facilitates or provides financial products or services under the regulatory authority of the federal financial regulators and state financial or securities regulators.

[2] TREASURY, ASSESSING THE IMPACT OF NEW ENTRANT NON-BANK FIRMS ON COMPETITION IN CONSUMER FINANCE MARKETS (2022), https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf. (Treasury Non-Bank Report).

discrimination in the use of AI in financial services, including challenges with explainability – that is, the ability to understand a model's output and decisions, or how the model establishes relationships based on the model input – and ensuring compliance with fair lending requirements; the potential for models to perpetuate discrimination by using and learning from data that reflect and reinforce historical biases; and the potential for AI tools to expand capabilities for firms to inappropriately target specific individuals or communities (e.g., low- to moderate-income communities, communities of color, women, rural, tribal, or disadvantaged communities). The report found that new entrant non-bank firms and innovations they are utilizing–including developments of AI in financial services—may be able to help improve financial services, but that further steps should be considered to monitor and address risks to consumers, foster market integrity, and help ensure the safety and soundness of the financial system.

In December 2023, Treasury issued an RFI soliciting input to inform its development of a national financial inclusion strategy; that RFI included questions related to the use of technologies such as AI in the provision of consumer financial services, in addition to other topics related to financial inclusion.[3]

In March 2024, Treasury published a report on AI and cybersecurity. In developing that report, Treasury conducted extensive industry outreach on AI-related cybersecurity risks in the financial services sector.[4] In the report, Treasury identifies opportunities and challenges that AI presents to the security and resiliency of the financial services sector. The report outlines a series

[3] TREASURY, REQUEST FOR INFORMATION ON FINANCIAL INCLUSION, 88 Fed. Reg. 88702 (Dec. 22, 2023), https://www.federalregister.gov/documents/2023/12/22/2023-28263/request-for-information-on-financial-inclusion.
[4] TREASURY, MANAGING ARTIFICIAL INTELLIGENCE-SPECIFIC CYBERSECURITY RISKS IN THE FINANCIAL SERVICES SECTOR (Mar. 27, 2024), https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf. (Treasury AI Cybersecurity Report).

of next steps to address AI-related operational risk, cybersecurity, and fraud challenges, as a response to Executive Order 14110.[5] Treasury's efforts to identify and mitigate cybersecurity, fraud, and other risks align with Office of Management and Budget (OMB) Memorandum M-24-10 to federal agencies.[6]

Further, in May 2024, Treasury issued its 2024 National Strategy for Combatting Terrorist and Other Illicit Financing (National Illicit Finance Strategy),[7] noting that innovations in AI, including machine learning and large language models such as generative AI, have significant potential to strengthen anti-money laundering/countering the financing of terrorism (AML/CFT) compliance by helping financial institutions analyze large amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies. One of the objectives identified in the National Illicit Finance Strategy is industry outreach to improve Treasury's understanding of how financial institutions are using AI to comply with applicable AML/CFT requirements.

Treasury also recognizes the important work underway across agencies related to the evolving use of AI in financial services. This includes the Commodity Futures Trading Commission's (CFTC) request for comment issued in January 2024 on current and potential uses and risks of AI in CFTC-regulated derivatives markets, and the report issued by the Technology Advisory Committee of the CFTC in May 2024 on Responsible Artificial Intelligence in

---

[5] WHITE HOUSE, E.O. 14110, SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence. The E.O. calls for a whole-of-government approach to meeting the challenges and opportunities posed by AI.

[6] OMB, MEMORANDUM M-24-10 ADVANCING GOVERNANCE, INNOVATION, AND RISK MANAGEMENT FOR AGENCY USE OF ARTIFICIAL INTELLIGENCE (Mar. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf. The OMB memorandum establishes new agency requirements and guidance for AI governance, innovation, and risk management practices that impact the rights and safety of the American public.

[7] TREASURY, 2024 NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILLICIT FINANCING (2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

Financial Markets.[8] The Securities and Exchange Commission (SEC) also issued a proposed rule in July 2023 on addressing conflicts of interest associated with broker-dealers' and investment advisers' use of predictive data analytics and similar technologies, including AI.[9] Additionally, the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Consumer Financial Protection Bureau (CFPB), and National Credit Union Administration (NCUA) issued an interagency RFI in 2021 on financial institutions' use of AI.[10]

In addition, the Financial Stability Oversight Council (FSOC) identified the use of AI in financial services as a vulnerability for the first time in its 2023 annual report.[11] FSOC noted in its 2023 annual report that the use of AI can introduce certain risks, including safety and soundness risks like cyber and model risks, and recommended monitoring the rapid developments in AI to ensure that oversight structures account for emerging risks to the financial system while also facilitating efficiency and innovation.

In 2018, Treasury's Financial Crimes Enforcement Network (FinCEN) and the federal banking agencies issued a Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing,[12] which encouraged banks to use existing tools or adopt new

---

[8] CFTC, *CFTC Staff Releases Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets*, (Jan. 25, 2024), https://www.cftc.gov/PressRoom/PressReleases/8853-24.
CFTC, RESPONSIBLE ARTIFICIAL INTELLIGENCE IN FINANCIAL MARKETS (May 2, 2024), https://www.cftc.gov/PressRoom/PressReleases/8905-24.

[9] SEC, CONFLICTS OF INTEREST ASSOCIATED WITH THE USE OF PREDICTIVE DATA ANALYTICS BY BROKER-DEALERS AND INVESTMENT ADVISERS (Jul. 26, 2023), https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf.

[10] OCC, FRB, FDIC, CFPB, & NCUA, REQUEST FOR INFORMATION AND COMMENT ON FINANCIAL INSTITUTIONS' USE OF ARTIFICIAL INTELLIGENCE, INCLUDING MACHINE LEARNING, 86 Fed. Reg. 16837 (Mar. 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[11] *See* FSOC, ANNUAL REPORT (2023), https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf. FSOC's 2022 report also discussed AI. *See* FSOC, ANNUAL REPORT (2022), https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.

[12] FinCEN, FRB, FDIC, NCUA, & OCC, JOINT STATEMENT ON INNOVATIVE EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING (Dec. 3, 2018), https://www.fincen.gov/news/news-releases/joint-statement-innovative-efforts-combat-money-laundering.

technologies, including AI, to identify and report money laundering, terrorist financing, and other illicit financial activity. Pursuant to requirements and authorities outlined in the Anti-Money Laundering Act of 2020 (the AML Act), FinCEN is also taking several steps to create the necessary regulatory and examination environment to support AML/CFT-related innovation that can enhance the effectiveness and efficiency of the Bank Secrecy Act (BSA) regime. Section 6209 of the AML Act requires the Secretary of the Treasury to issue a rule specifying standards for testing technology and related technology internal processes designed to facilitate effective compliance with the BSA by financial institutions, and these standards may include an emphasis on innovative approaches to compliance, such as the use of machine learning.[13] The rulemaking would follow the issuance of the April 2021 Statement and separate Request for Information on Model Risk Management issued by FinCEN and the OCC, Federal Reserve, FDIC, and NCUA.[14] As part of the regulatory process, FinCEN may consider how financial institutions are currently using innovative approaches to compliance, like machine learning and AI, and the potential benefits and risks of specifying standards for those technologies. In February 2023, FinCEN hosted a FinCEN Exchange that brought together law enforcement, financial institutions, and other private sector and government entities to discuss how AI is used for monitoring and detecting illicit financial activity. FinCEN also regularly engages financial institutions on the

[13] Treasury's 2024 Illicit Finance Strategy outlined measures to encourage private sector use of technology to improve AML/CFT programs and compliance, including the rulemaking required under AML Act section 6209. https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

[14] OCC, FRB, FDIC, NCUA, & FinCEN, *Joint Statement on Bank Secrecy Act / Anti-Money Laundering Compliance* (Apr. 09, 2021), https://www.fincen.gov/news/news-releases/agencies-issue-statement-and-request-information-bank-secrecy-actanti-money.
OCC, FRB, FDIC, NCUA, & FinCEN, 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, 86 FR 18978 (Apr. 12, 2021), https://www.federalregister.gov/documents/2021/04/12/2021-07428/request-for-information-and-comment-extent-to-which-model-risk-management-principles-support.

topic through the BSA Advisory Group Subcommittee on Innovation and Technology, and BSAAG Subcommittee on Information Security and Confidentiality.[15]

Given the rapidly evolving nature of AI, this RFI builds on the work that Treasury has done to date and seeks to gather additional perspectives.

Current RFI

Treasury understands that financial institutions are exploring the use of AI, and is interested in gaining insights into those current and potential uses. The RFI also seeks input on the potential benefits and challenges of financial institutions' use of AI for impacted entities.

This RFI adopts the definition of AI utilized in President Biden's Executive Order on Safe, Secure, and Trustworthy Development and Use of AI:

> The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human—based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.[16]

Treasury interprets this definition to describe a wide range of models and tools that utilize data, patterns, and other informational inputs to generate outputs – including statistical relationships, forecasts, content, and recommendations – for a given set of objectives. For the purposes of this RFI, Treasury is seeking comment on the latest developments in AI technologies

[15] The OCC, FDIC, FRB and NCUA also participate actively in BSAAG and the subcommittees.
[16] WHITE HOUSE, *supra* note 5.

and applications, including but not limited to advancements in existing AI (e.g., machine learning models that learn from data and automatically adapt and improve with minimal human interference, rather than relying on explicit programming) and emerging AI technologies including deep learning neutral network such as generative AI and large language models (LLMs).[17]

Use of AI

Through this RFI, Treasury seeks to increase its understanding of how AI is being used within the financial services sector and the opportunities and risks presented by developments and applications of AI within the sector, including potential obstacles for facilitating responsible use of AI within financial institutions, the effect on impacted entities through use of AI by financial institutions, and recommendations for enhancements to legislative, regulatory, and supervisory frameworks applicable to AI in financial services.[18] Treasury is interested in gaining insights into the uses of AI by financial institutions, including but not limited to those outlined below:

- *Provision of products and services*: Financial institutions' use of AI to assist in decisions related to offering financial products or services, such as whether to offer transaction

[17] As used here, generative AI is defined as a kind of AI capable of generating new content such as code, images, music, text, simulations, 3D objects, and videos. It is often used to describe algorithms (such as ChatGPT) that can be used to create new content. LLM is defined as a class of language models that use deep-learning algorithms and are trained on extremely large textual datasets that can be multiple terabytes in size. LLMs can be classified as two types: generative or discriminatory. Generative LLMs are models that output text, such as the answer to a question or an essay on a specific topic. They are typically unsupervised or semi-supervised learning models that predict what the response is for a given task. Discriminatory LLMs are supervised learning models that usually focus on classifying text, such as determining whether a text was made by a human or AI. *See* U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE LANGUAGE OF TRUSTWORTHY AI: AN IN-DEPTH GLOSSARY OF TERMS (Mar. 22, 2023), https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary.

[18] *See also* PAUL TIERNO, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN FINANCIAL SERVICES (CONGRESSIONAL RESEARCH SERVICE, 2024), https://crsreports.congress.gov/product/pdf/R/R47997.

accounts, credit, or insurance, and the terms and conditions of such offerings, as well as financial forecasting products and pattern recognition tools;

- *Risk management*: Financial institutions' use and potential use of AI for managing various types of risk, including credit risk, market risk, operational risk, cyber risk, fraud and illicit finance risk, compliance risk (including fraud risk), reputation risk, interest rate risk, liquidity risk, model risk, counterparty risk, and legal risk, as well as the extent to which financial institutions may be exploring the use of AI for treasury management or asset-liability management;
- *Capital markets*: Financial institutions' use of AI to assist in capital markets activities, including identifying investment opportunities, allocating capital, executing trades, and providing financial advisory services;
- *Internal operations*: Financial institutions' use of AI to manage internal operations, such as payroll, HR functions, training, performance management, communications, cybersecurity, software development, and other internal operational functions;
- *Customer service*: Financial institutions' use of AI in customer management, including complaint handling, investor relations, website management, claims management, or other external-facing functions;
- *Regulatory compliance*: Financial institutions' use of AI to manage regulatory requirements, including capital and liquidity requirements, regulatory reporting or disclosure requirements, BSA/AML requirements, consumer and investor protection requirements, and license management; and
- *Marketing*: Financial institutions' use of AI to market to individuals, groups of individuals, or institutional counterparties.

Potential Opportunities and Risks

AI has the potential to offer improved efficiency and enhanced capabilities across the use cases outlined above and others, to the benefit of impacted entities. For example, AI can process certain forms of, and large amounts of, information that may otherwise be impractical or impossible to use, thus unlocking new insights and capabilities. This could translate to tangible benefits, including cost savings for financial institutions and expanded access to products and services that may be more individually tailored to impacted entities.

Nevertheless, the use of AI, particularly the use of emerging AI technologies, can present a variety of challenges to existing risk mitigation strategies, particularly as more complex models and tools evolve. Potential types of risk associated with AI use by financial institutions include model risks, operational risks, compliance risks, and third-party risks, among others. Potential risks associated with AI use for impacted entities may include bias, discrimination, monoculture, concentration, fraud, herding, hallucinations, explainability, conflicts, reputational risk, and data privacy risks, among others.[19] More generally, concerns have been expressed about AI being used in connection with cyber threats or contributing to job displacement.

Financial institutions typically manage AI-related risks through existing risk management frameworks, the most common of which include model risk, operational risk, compliance risk (including compliance with laws and regulations related to consumer protection and AML/CFT), and third-party risk management).[20] However, as noted in the Treasury AI Cybersecurity Report,

[19] For a discussion of such potential risks, see Gary Gensler, *"AI, Finance, Movies, and the Law" Prepared Remarks before the Yale Law School* (Feb. 13, 2024), https://www.sec.gov/news/speech/gensler-ai-021324.
[20] FSOC, *supra* note 11.

some financial institutions have reported that existing risk management frameworks may not be adequate to address emerging AI technologies.[21]

Oversight of AI - Explainability and Bias

The rapid development of emerging AI technologies has created challenges for financial institutions in the oversight of AI. Financial institutions may have an incomplete understanding of where the data used to train certain AI models and tools was acquired and what the data contains, as well as how the algorithms or structures are developed for those AI models and tools. For instance, machine-learning algorithms that internalize data based on relationships that are not easily mapped and understood by financial institution users create questions and concerns regarding explainability, which could lead to difficulty in assessing the conceptual soundness of such AI models and tools.[22]

Financial regulators have issued guidance on model risk management principles, encouraging financial institutions to effectively identify and mitigate risks associated with model development, model use, model validation (including validation of vendor and third-party models), ongoing monitoring, outcome analysis, and model governance and controls.[23] These principles are technology-agnostic but may not be applicable to certain AI models and tools.

---

[21] TREASURY, *supra* note 4.
[22] FSOC, *supra* note 11.
[23] *See, e.g.*, FEDERAL HOUSING FINANCE AGENCY, ARTIFICIAL INTELLIGENCE / MACHINE LEARNING RISK MANAGEMENT (Feb. 10, 2022), https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/AdvisoryBulletinDocuments/Advisory-Bulletin-2022-02.pdf; OCC, SOUND PRACTICES FOR MODEL RISK MANAGEMENT: SUPERVISORY GUIDANCE ON MODEL RISK MANAGEMENT, (Apr. 4, 2011), https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html; FDIC, SUPERVISORY GUIDANCE ON MODEL RISK MANAGEMENT (Jun. 17, 2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.html; and FRB, GUIDANCE ON MODEL RISK MANAGEMENT (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

Due to their inherent complexity, however, AI models and tools may exacerbate certain risks that may warrant further scrutiny and risk mitigation measures. This is particularly true in relation to the use of emerging AI technologies.

Furthermore, the rapid development of emerging AI technologies may create a human capital shortage in financial institutions, where sufficient knowledge about a potential risk or bias of those AI technologies may be lacking such that staff may not be able to effectively manage the development, validation, and application of those AI technologies. Some financial institutions may rely on third-party providers to develop and validate AI models and tools, which may also create challenges in ensuring alignment with relevant risk management guidance.

Challenges in explaining AI-assisted or AI-generated decisions also create questions about transparency generally, and raise concerns about the potential obfuscation of model bias that can negatively affect impacted entities. In the Non-Bank Report, Treasury noted the potential for AI models to perpetuate discrimination by utilizing and learning from data that reflect and reinforce historical biases.[24] These challenges of managing explainability and bias may impede the adoption and use of AI by financial institutions.

Consumer Protection and Data Privacy

Use of AI in financial services – particularly use of emerging AI technologies – may negatively impact consumers and complicate efforts for financial institutions to ensure compliance with fair lending and anti-discrimination laws, or laws prohibiting unfair, deceptive or abusive acts or practices, potentially leading to legal violations.[25] Some stakeholders have

[24] TREASURY, *supra* note 2.

[25] Fair lending and anti-discrimination laws include the Fair Housing Act, Equal Credit Opportunity Act, and Fair Credit Reporting Act. In September 2023, the CFPB issued guidance about certain legal requirements that lenders

expressed concerns that AI-powered capabilities that enable financial institutions to offer more personalized products and services can also be used to inappropriately target consumers in ways that might be unfair, abusive, and discriminatory.[26] In response to these challenges, methods for testing and addressing potential biases – including adversarial testing[27] and less discriminatory alternatives (LDA) testing[28]– continue to evolve, and some research has indicated that carefully designed and monitored AI models and tools can help reduce bias in the provision of financial services.[29]

Additionally, use of AI may present new or increased data privacy risks for impacted entities and compliance risks for financial institutions. Existing approaches to comply with

---

must adhere to when using AI and other complex models. The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers. CFPB, *CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence,* (Sept. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence.
The CFPB published guidance on adverse action notification requirements that are technology-agnostic and stated that creditors subject to the CFPB's Regulation B are not permitted to use AI, complex algorithms, or "black-box" models which the creditors may not understand sufficiently; when the creditor is not able to accurately identify the specific reasons for denying credit or taking other adverse actions against consumers, the creditor may not be meeting its legal obligations under federal consumer financial laws.
CFPB, ADVERSE ACTION NOTIFICATION REQUIREMENTS AND THE PROPER USE OF THE CFPB'S SAMPLE FORMS PROVIDED IN REGULATION B, Consumer Financial Protection Circular 2023-03 (Sept. 19, 2023), https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.
CFPB, ADVERSE ACTION NOTIFICATION REQUIREMENTS IN CONNECTION WITH CREDIT DECISIONS BASED ON COMPLEX ALGORITHMS, Consumer Financial Protection Circular 2022-03 (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.
[26] TREASURY, *supra* note 2.
[27] Adversarial machine learning is defined as a practice concerned with the design of machine learning algorithms that can resist security challenges and a field to study vulnerabilities of machine learning approaches in adversarial settings to develop techniques to make learning robust to adversarial manipulation. *See* U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE LANGUAGE OF TRUSTWORTHY AI: AN IN-DEPTH GLOSSARY OF TERMS (Mar. 22, 2023), https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary.
[28] LDA testing used here refers to the practice of searching for less discriminatory alternatives as part of the model testing. *See* CFPB, *Interactive Bureau Regulations*, 12 CFR Part 1002 (Regulation B), Comment for 1002.6– Rules Concerning Evaluation of Applications, 6(a)-2 Effects test, https://www.consumerfinance.gov/rules-policy/regulations/1002/interp-6/#6-a-Interp-2.
[29] *See, e.g.*, ROBERT BARTLETT ET AL., CONSUMER-LENDING DISCRIMINATION IN THE FINTECH ERA (UNIVERSITY OF CALIFORNIA BERKELEY, 2019), https://doi.org/10.1016/j.jfineco.2021.05.047. While the research found reduced disparities in interest rates charged to borrowers that identified as racial or ethnic minorities, disparities were still found to exist. The research found that fintech lenders still charged borrowers that identified as Black or Latino interest rates 7.9 basis points higher than those charged to otherwise-equivalent borrowers.

privacy laws that involve anonymizing or de-identifying data before selling data may be, or may become, ineffective as models develop and become capable of more readily and accurately identifying owners of previously anonymized data. AI models and tools require great amounts of data to train and operate, creating a demand for more or new sources of data. In addition, AI may create or exacerbate issues related to data accuracy, and the use of inaccurate data or providing inaccurate information may also lead to a violation of law. Some financial institutions are using certain types of "alternative data"[30] for credit or insurance underwriting, or to inform other types of financial decision-making affecting impacted entities. Federal agencies have encouraged the responsible use of alternative data and described risk mitigation measures for institutions using such data.[31]

The Treasury Non-Bank Report noted concerns that the use of alternative data could subject growing amounts of behavior to commercial surveillance.[32] In particular, Treasury noted concerns that the use of data regarding individual behavior – even behavior that is not explicitly related to financial products -- in AI models that are used to inform decisions to offer financial products and services, such as credit products, could have unintended spillover effects. Additionally, AI-powered predictive analytics are enabling firms to conjecture about the attributes or behavior of an individual based on analysis of data gathered on other individuals. Such capabilities have the potential to undermine privacy (including the privacy of others) and

[30] As used here, "alternative data" refers to information not typically found in credit files of credit reporting agencies. Generally, alternative data used in financial services is financial data, such as account balance and cash-flow data, or rent and utility payments. However, other fields, such as education data, have been known to be used in credit underwriting.

[31] FRB, CFPB, FDIC, NCUA, & OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (Dec. 3, 2019), https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement_alternative-data.pdf. The interagency statement explained risk mitigation measures such as (1) conducting a thorough analysis of relevant consumer protection laws and regulations to ensure firms understand the opportunities, risks, and compliance requirements before using alternative data, and (2) using data that has a "direct relation to consumers' finances."

[32] TREASURY, *supra* note 2.

dilute the power of existing "opt-out" privacy protections, especially when a consumer may not be aware of the information being used about them or the way it may be used.

Third-Party Risks

Many financial institutions rely on third-party providers for business operations, including the use of AI. This reliance, as well as the increasing complexity of the AI technologies provided, may exacerbate third-party and related risks.[33]

In 2023, federal banking agencies issued interagency guidance on third-party risk management, which replaced prior guidance on third-party risk management and provided a standardized, principles-based approach for assessing and managing risks associated with third-party relationships.[34] The principles—including those related to due diligence, contract management, and ongoing monitoring— may be applicable to financial institutions' use of AI developed by third-party vendors. The guidance specifies that covered financial institutions are responsible for ensuring compliance for all activities performed, including those conducted by third-parties.

Further, the SEC has taken steps to update its expectations for third-party risk management for investment advisers. In 2022, the SEC proposed a rule under the Investment Advisers Act of 1940 that would require registered investment advisers to perform due diligence prior to outsourcing certain services or functions to service providers and to periodically monitor the performance of models developed by third-parties.[35]

---

[33] *Id.*
[34] FRB, FDIC, & OCC, INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT (Jun. 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.
[35] SEC, OUTSOURCING BY INVESTMENT ADVISERS, 87 Fed. Reg. 68816 (Oct. 26, 2022), https://www.federalregister.gov/documents/2022/11/16/2022-23694/outsourcing-by-investment-advisers#:~:text=SUMMARY%3A,without%20first%20meeting%20minimum%20requirements.

In addition, the National Association of Insurance Commissioners (NAIC) adopted the *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers* in December 2023.[36] The model bulletin provides principles-based guidance reminding insurers that decisions or actions impacting consumers that are made or supported by advanced analytical and computational technologies, including AI, must comply with all applicable insurance laws and regulations. The bulletin states that insurers are expected to develop and maintain a written program for the responsible use of AI and encourages insurers to use verification and testing methods "to identify errors and bias" and the potential for unfair discrimination in predictive models and other AI systems.

II. Overview of Questions

The questions in this RFI are organized into parts A through C in section III below. Part A solicits comment on the uses of AI, including use cases, types of models being employed, and variability in use and access to AI across financial institutions. Part B focuses on opportunities and risks associated with financial institutions' use of AI, and how financial institutions are exploring or pursuing potential benefits and managing risks. In addition, Part B presents questions on impacted entities—both opportunities and risks, particularly those related to bias and discrimination, as well as privacy. Part C seeks input on potential further actions to advance responsible innovation and competition within the financial sector with respect to the use of AI.

III. Request for Information

[36] NAIC, NAIC MODEL BULLETIN ON THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS BY INSURERS (Dec. 4, 2023), https://content.naic.org/sites/default/files/inline-files/2023-12-4%20Model%20Bulletin_Adopted_0.pdf.

Treasury welcomes input on any matter that commenters believe is relevant to Treasury's efforts to understand the uses, opportunities, and risks of AI in financial services. Treasury is interested in gathering information from a broad set of stakeholders in the financial services ecosystem, including those providing, facilitating, and receiving financial products and services, as well as consumer and small business advocates, academics, nonprofits, and others interested in providing information to Treasury on potential opportunities and risks related to the use of AI in financial services.

Treasury is further interested in comments on the extent to which stakeholders can undertake additional actions to manage the risks posed by AI and comply with existing legal and regulatory requirements, as well as the extent to which existing legal and regulatory requirements may need to be enhanced to manage the risks posed by AI, and whether commenters have recommendations for legislative, regulatory, or supervisory enhancements that may be appropriate to both foster innovation and ensure responsible use of AI in the financial services sector.

Treasury is also interested in understanding how the use of AI may differ across financial institutions of different sizes and complexity, and the extent to which such variance may impact competition. In particular, Treasury is interested in comments about the extent to which small financial institutions may face unique challenges in accessing and using AI.

Commenters are encouraged to address any of the questions relevant to them and may respond to all or a subset of the questions. When responding to one or more of the questions below, please note in your response the number(s) of the questions to which you are responding. To the extent possible, please cite data or provide specific examples that support your responses.

A. General Use of AI in Financial Services

Treasury is interested in understanding the evolving use of AI in financial services. In particular, Treasury is interested in how financial institutions are using or exploring the use of AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing, as outlined in the background section above. Treasury is also seeking to understand the types of AI being used, in particular new developments made to existing AI and emerging AI technologies, and how they are developed and deployed by financial institutions. Finally, Treasury is interested in gaining insights into the general accessibility of AI—in terms of economic viability of developing or purchasing AI technologies, as well as the human resources and infrastructure to support their use—across financial institutions, and whether asymmetries with respect to accessibility could impact competition.

Question 1:

Is the definition of AI used in this RFI appropriate for financial institutions? Should the definition be broader or narrower, given the uses of AI by financial institutions in different contexts? To the extent possible, please provide specific suggestions on the definitions of AI used in this RFI.

Question 2:

What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?

Question 3:

To what extent does the type of AI, the development of AI, or AI applied use cases differ within a financial institution? Please describe the various types of AI and their applied use cases within a financial institution.

Are there additional use cases for which financial institutions are applying AI or for which financial institutions are exploring the use of AI? Are there any related reputation risk concerns about using AI? If so, please provide specific examples.

Question 4:

Are there challenges or barriers to access for small financial institutions seeking to use AI? If so, why are these barriers present? Do these barriers introduce risks for small financial institutions? If so, how do financial institutions expect to mitigate those risks?

B. Actual and Potential Opportunities and Risks Related to Use of AI in Financial Services

AI provides opportunities for financial institutions to improve efficiency, reduce costs, strengthen risk controls, and expand impacted entities' access to financial products and services. At the same time, the use of AI in financial services can pose a variety of risks for impacted entities, depending on its application. Treasury is interested in perspectives on actual and potential benefits and opportunities to financial institutions and impacted entities of the use of AI in financial services, as well as views on the optimal methods to mitigate risks. In particular,

Treasury is interested in perspectives on bias and potential discrimination as well as privacy risks, the extent to which impacted entities are protected from and informed about the potential harms from financial institutions' use of AI in financial services.

Actual and Potential Opportunities and Benefits

Question 5:

What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? Please describe specific benefits with supporting data and examples. How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)?

How has AI been used in financial services to improve fair lending and consumer protection, including substantiating information? To what extent does AI improve the ability of financial institutions to comply with fair lending or other consumer protection laws and regulations? Please be as specific as possible, including details about cost savings, increased customer reach, expanded access to financial services, time horizon of savings, or other benefits after deploying AI.

Actual and Potential Risks and Risk Management

Oversight of AI – Explainability and Bias

Question 6:

To what extent are the AI models and tools used by financial institutions developed in-house, by third-parties, or based on open-source code? What are the benefits and risks of using AI models and tools developed in-house, by third-parties, or based on open-source code?

To what extent are a particular financial institution's AI models and tools connected to other financial institutions' models and tools? What are the benefits and risks to financial institutions and consumers when the AI models and tools are interconnected among financial institutions?

Question 7:

How do financial institutions expect to apply risk management or other frameworks and guidance to the use of AI, and in particular, emerging AI technologies? Please describe the governance structure and risk management frameworks financial institutions expect to apply in connection with the development and deployment of AI. Please provide examples of policies and/or practices, to the extent applicable.

What types of testing methods are financial institutions utilizing in connection with the development and deployment of AI models and tools? Please describe the testing purpose and the specific testing methods utilized, to the extent applicable.

To what extent are financial institutions evaluating and addressing potential gaps in human capital to ensure that staff can effectively manage the development and validation practices of AI models and tools?

What challenges exist for addressing risks related to AI explainability? What methodologies are being deployed to enhance explainability and protect against potential bias risk?

Question 8:

What types of input data are financial institutions using for development of AI models and tools, particularly models and tools relying on emerging AI technologies? Please describe the data governance structure financial institutions expect to apply in confirming the quality and integrity of data. Are financial institutions using "non-traditional" forms of data? If so, what forms of "non-traditional" data are being used? Are financial institutions using alternative forms of data? If so, what forms of alternative data are being used?

Fair Lending, Data Privacy, Fraud, Illicit Finance, and Insurance

Question 9:

How are financial institutions evaluating and addressing any increase in risks and harms to impacted entities in using emerging AI technologies? What are the specific risks to consumers and other stakeholder groups, including low- to moderate-income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)? How are financial institutions protecting against issues such as dark patterns – user interface designs that can potentially manipulate impacted entities in decision-making – and predatory targeting emerging in

the design of AI? Please describe specific risks and provide examples with supporting data.

Question 10:

How are financial institutions addressing any increase in fair lending and other consumer-related risks, including identifying and addressing possible discrimination, related to the use of AI, particularly emerging AI technologies? What governance approaches throughout the development, validation, implementation, and deployment phases do financial institutions expect to establish to ensure compliance with fair lending and other consumer-related laws for AI models and tools prior to deployment and application?

In what ways could existing fair lending requirements be strengthened or expanded to include fair access to other financial services outside of lending, such as access to bank accounts, given the rapid development of emerging AI technologies? How are consumer protection requirements outside of fair lending, such as prohibitions on unfair, deceptive and abusive acts and practices, considered during the development and use of AI? How are related risks expected to be mitigated by financial institutions using AI?

Question 11:

How are financial institutions addressing any increase in data privacy risk related to the use of AI models, particularly emerging AI technologies? Please provide examples of how financial institutions have assessed data privacy risk in their use of AI.

In what ways could existing data privacy protections (such as those in the Gramm-Leach-Bliley Act (Pub. L. No. 106-102)) be strengthened for impacted entities, given the rapid development of emerging AI technologies, and what examples can you provide of the impact of AI usage on data privacy protections?

How have technology companies or third-party providers of AI assessed the categories of data used in AI models and tools within the context of data privacy protections?

Question 12:

How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?

Question 13:

How do financial institutions, technology companies, or third-party service providers expect to use AI to address and mitigate illicit finance risks? What challenges do organizations face in adopting AI to counter illicit finance risks? How do financial institutions use AI to comply with applicable AML/CFT requirements? What risks may such uses create?

Question 14:

As states adopt the NAIC's *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers* and other states develop their own regulations or guidance, what changes have insurers implemented and what changes might they implement to comply or be consistent with these laws and regulatory guidance?

How do insurers using AI make certain that their underwriting, rating, and pricing practices and outcomes are consistent with applicable laws addressing unfair discrimination?

How are insurers currently covering AI-related risks in existing policies? Are the coverage, rates, or availability of insurance for financial institutions changing due to AI risks? Are insurers including exclusions for AI-related risks or adjusting policy wording for AI risks?

Third-party Risks

Question 15:

To the extent financial institutions are relying on third-parties to develop, deploy, or test the use of AI, and in particular, emerging AI technologies, how do financial institutions expect to manage third-party risks? How are financial institutions applying third-party risk management frameworks to the use of AI?

What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions? How have these challenges varied or affected the use of AI across financial institutions of various sizes and complexity?

Question 16:

What specific concerns over data confidentiality does the use of third-party AI providers create? What additional enhancements to existing processes do financial institutions expect to make in conducting due diligence prior to using a third-party provider of AI technologies?

What additional enhancements to existing processes do financial institutions expect to make in monitoring an ongoing third-party relationship, given the advances in AI technologies? How do financial institutions manage supply chain risks related to AI?

Question 17:

How are financial institutions applying operational risk management frameworks to the use of AI? What, if any, emerging risks have not been addressed in financial institutions' existing operational risk management frameworks?

How are financial institutions ensuring their operations are resilient to disruptions in the integrity, availability, and use of AI? Are financial institutions using AI to preserve continuity of other core functions? If so, please provide examples.

C. Further actions

As noted, Treasury supports responsible innovation and competition in the financial sector and seeks to promote a financial system that delivers inclusive and equitable access to

financial services that meet the needs of consumers and businesses, while maintaining stability and market integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats.

Question 18:

What actions are necessary to promote responsible innovation and competition with respect to the use of AI in financial services? What actions do you recommend Treasury take, and what actions do you recommend others take? What, if any, further actions are needed to protect impacted entities, including consumers, from potential risks and harms?

Please provide specific feedback on legislative, regulatory, or supervisory enhancements related to the use of AI that would promote a financial system that delivers inclusive and equitable access to financial services that meet the needs of consumers and businesses, while maintaining stability and integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats. What enhancements, if any, do you recommend be made to existing governance structures, oversight requirements, or risk management practices as they relate to the use of AI, and in particular, emerging AI technologies?

Question 19:

To what extent do differences in jurisdictional approaches inside and outside the United States pose concerns for the management of AI-related risks on an enterprise-wide basis? To what extent do such differences have an impact on the development of products,

competition, or other commercial matters? To what extent do such differences have an impact on consumer protection or availability of services?

Moses Kim,
Director, Office of Financial Institutions Policy