Center for American Progress
1333 H Street NW, Suite 100E
Washington, DC 20005
202.682.1611
americanprogress.org

August 12, 2024

Jeanette Quick
Deputy Assistant Secretary for Financial Institutions Policy
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Submitted electronically via regulations.gov

RE: Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector (89 FR 50048)

The Center for American Progress (CAP) and Governing for Impact (GFI) submit this response to the "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector" (89 FR 50048).[1]

In June 2024, CAP and GFI released a report, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence,"[2] focusing on the existing statutory authorities that federal agencies can use to regulate the risks and opportunities from Artificial Intelligence (AI). The report examines numerous existing statutory authorities and makes more than 80 recommendations for agency action. While each authority and recommendation in the report has been extensively researched, each potential recommendation will require further vetting before agencies act. These recommendations demonstrate, though, that agencies cannot and should not wait to utilize existing authorities to address AI.

Chapter 5 of our report, "Financial Regulatory Agencies,"[3] identifies 11 existing statutory authorities that allow financial services regulators to address the risks of AI and is the primary source referenced throughout this RFI response. In addition to our answers to specific questions from the RFI we have attached Chapter 5 of our report in full along with the accompanying fact sheet.

[1] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," *Federal Register* 89 (114) (2024): 50048-50055, available at https://www.govinfo.gov/content/pkg/FR-2024-06-12/pdf/2024-12336.pdf.
[2] Will Dobbs-Allsopp and others, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authority To Regulate Artificial Intelligence" (Washington D.C.: Governing for Impact and Center for American Progress, 2024), available at https://www.americanprogress.org/article/taking-further-agency-action-on-ai/.
[3] Todd Phillips and Adam Conner, "Financial Regulatory Agencies," in Dobbs-Allsop and others, "*Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authority to Regulate Artificial Intelligence*," available at https://www.americanprogress.org/article/taking-further-agency-action-on-ai/financial-regulatory-agencies-chapter/.

We write to highlight the ways in which our report is responsive to the RFI, as well as to share the full report and associated materials with you. Some sections of our report respond to questions 1,6, and 11, but the bulk of our recommendations are responsive to Question 18. Below, we have briefly summarized our report recommendations, which can be read in full in our attached report chapter and fact sheet. As modeled by Question 18, we have differentiated between recommendations directly relevant to the Treasury Department and those that apply to other financial services regulators.

Further questions can be directed to Adam Conner (aconner@americanprogress.org) at CAP or Will Dobbs-Allsopp (wdobbsallsopp@governingforimpact.org) at GFI. Please do not hesitate to reach out with any questions or for further discussion.

Thank You,

Adam Conner
Vice President, Technology Policy
Center for American Progress

Will Dobbs-Allsopp
Policy Director
Governing for Impact

****

Introduction

This RFI notes that "'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."[4] Throughout our report and in our responses to this RFI, we include three main categories of impacted entities: Customers, Banks, and Securities brokers and futures commission merchants, securities and derivatives exchanges, and other market intermediaries. As noted in our report:[5]

> **Customers**: Banks and other financial services providers may illegally discriminate against customers when making lending decisions with unknowingly biased AI systems. Banks' and lenders' retail and institutional customers are also at risk of faulty AI systems that fail to accurately respond to their inquiries, accurately assess their credit worthiness, or execute transactions. Similarly, brokers' customers face losses from transactions that AI systems fail to execute. Financial institutions also serve as a wealth of information about customers, which is necessary for AI systems to operate, and may be liable for customer losses stemming from AI-enabled fraud.

[4] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50049.
[5] Phillips and Conner, "Financial Regulatory Agencies."

Banks: The core purpose of bank regulation is to ensure banks' safety and soundness, and AI could put this at risk. Banks face potential operational failures from AI-enabled cyberattacks that can evade their information technology (IT) defenses, runs from depositors' use of AI for treasury management, and losses from banks' own opaque and faulty AI-based risk management systems.

Securities brokers and futures commission merchants, securities and derivatives exchanges, and other market intermediaries: In addition to banks, the nonbank financial institutions that comprise the capital markets are also poised to use AI systems that may pose risks to firms' financial health and that of markets overall. Brokers may be liable for trades that AI systems failed to execute or misexecuted, and investment advisers and brokers may be liable for AI systems that fail to offer conflict-free advice or advice in the clients' best interests. Exchanges may face operational failures from their AI-based matching software or experience flash crashes stemming from erroneous high-frequency trading. Additionally, clearinghouses relying on AI systems that fail may be unable to novate trades, putting the markets at risk of requiring bailouts.

The RFI asks for stakeholders to provide information on "potential opportunities and risks related to the use of AI in financial services."[6] Throughout our report and in response to this RFI, we highlight potential risks associated with the use of AI in the financial sector, including but not limited to:[7]

Prevention of access to financial services: AI-powered systems may prevent consumers from accessing critical financial services by illegally discriminating against customers, generating incorrect information for their credit reports, or using faulty AI systems to execute transactions. The OMB M-24-10 AI guidance lists AI used by federal agencies for "[a]llocating loans; determining financial-system access; credit scoring; determining who is subject to a financial audit; making insurance determinations and risk assessments; determining interest rates; or determining financial penalties" as potentially rights-impacting.

Algorithmic discrimination that may exacerbate historical inequalities: Massive amounts of data are required to train and run AI-powered systems. In the financial services world, such historical data may dangerously reflect long-embedded systemic inequalities, such as redlining, unfair credit denials, and other discriminatory practices. AI systems trained on these historic data run the substantial risk of incorporating these inequities if not addressed proactively.

AI-enabled fraud: AI is already embraced as a tool to enable advanced fraud against consumers and financial institutions. The use of AI voice cloning and AI-generated fake accounts are just the tip of the iceberg when it comes to future AI-enabled financial fraud.

Failure to comply with anti-money laundering requirements: The Bank Secrecy Act and Treasury Department regulations require institutions to submit suspicious activity reports (SARs) whenever customers engage in activity that may involve money laundering. Black-box AI

[6] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50053.
[7] Phillips and Conner, "Financial Regulatory Agencies."

systems may fail to report otherwise suspicious activities, leaving banks in violation of the Bank Secrecy Act.

Threats to safe, secure, and stable financial systems: Integrating AI systems into financial services may pose a risk to the operation of these critical systems, as their sophistication grows along with the lack of transparency into proprietary black-box AI systems and algorithms that provide essential services and upkeep. The 2008 financial crisis proved how important the stability of the broader financial system is for a growing economy; yet AI and the commercial cloud computing that provides advanced AI pose risks that could negatively affect financial stability. Indeed, the Financial Stability Oversight Council has identified AI as a "vulnerability" within the U.S. financial system. For example, a bank's use of the same or similar data for AI-based risk management models, AI-enabled network effects, or unregulated AI service providers may pose systemic risks.

Finally, while this RFI is issued by the Department of Treasury, Question 18 asks, "What actions do you recommend Treasury take, and what actions do you recommend others take?"[8] We interpret this to include actions that the Department of Treasury and other Financial Regulatory Agencies could take to address AI risks. For ease of reference, in our response to Question 18, our recommendations are broken into two sections: one set of recommendations for the Department of Treasury and one for other Financial Regulatory Agencies. In our report, we define Financial Regulatory Agencies to include:

> "the federal banking and credit union agencies, financial markets regulators, and executive branch agencies. Specifically, in this report, these agencies include the Treasury Department, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Commodity Futures Trading Commission, the National Credit Union Administration, the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau, the Financial Stability Oversight Council, which is chaired by the secretary of the treasury."

Question 1

Question 1: Is the definition of AI used in this RFI appropriate for financial institutions?[9]

The RFI adopts the definition of Artificial Intelligence (AI) from the 2023 executive order on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,"[10] which is the definition in law from 15 U.S.C. 9401(3).[11] In addition to that definition of AI, the Department of Treasury should also

[8] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50055.
[9] Ibid., p. 50053.
[10] Executive Office of the President, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Press release, October 30, 2023, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[11] Title 15 Commerce and Trade, Chapter 119 National Artificial Intelligence Initiative, § 9401 Definitions, available at https://uscode.house.gov/view.xhtml?req=(title:15%20section:9401%20edition:prelim).

consider the definition of "automated systems" from the 2022 White House Blueprint for an AI Bill of Rights (AI Bill of Rights):[12]

> AUTOMATED SYSTEM: An "automated system" is any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities. Automated systems include, but are not limited to, systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure. "Passive computing infrastructure" is any intermediary technology that does not influence or determine the outcome of decision, make or aid in decisions, inform policy implementation, or collect data or observations, including web hosting, domain registration, networking, caching, data storage, or cybersecurity. Throughout this framework, automated systems that are considered in scope are only those that have the potential to meaningfully impact individuals' or communi-ties' rights, opportunities, or access.

The definition of "automated systems" is used in the AI Bill of Rights in conjunction with a two-part test to help determine the appropriate scope, including the critical impact of the use of the AI or automated system. The AI Bill of Rights notes, "Thus, this framework uses a two-part test to determine what systems are in scope. This framework applies to (1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services."[13] This broader definition of automated systems ensures the scope of the impact of these systems in critical areas of the financial sector is fully taken into account.

Question 6

> Question 6: 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?"[14]

The concentration of advanced foundation models and commercial cloud computing in a handful of companies, especially the high-powered computing needed to train and run advanced foundation models,[15] means there is a high risk that AI foundation models and commercial cloud computing are concentrated in a few providers.[16]

---

[12] The White House Office of Science and Technology Policy, "The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People" (Washington D.C.: 2022), p. 10, available at https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
[13] Ibid., p. 8.
[14] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50054.
[15] Andrew Kersley, "Big tech's cloud oligopoly risks AI market concentration," *ComputerWeekly.com*, April 15, 2024, available at https://www.computerweekly.com/feature/Big-techs-cloud-oligopoly-risks-AI-market-concentration.
[16] Amba Kak, Sarah Myers West, Meredith Whittaker, "Make no mistake—AI is owned by Big Tech," *MIT Technology Review*, December 5, 2023, available at https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/.

In our report, we propose that under the **Dodd-Frank Act**, the Financial Stability Oversight Council should:[17]

- Designate major providers of AI services to financial institutions as systemically important if they reach an adoption level that creates vulnerability; and
- Designate the cloud service providers to those firms as systemically important.

In addition, we note the risk of firms being locked into one AI system and recommend that regulators, using various statutory authorities to mitigate this risk:

> **Ensure firms may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not develop their own systems in-house; instead, they will license software from a few competing nonfinancial institutions. Financial firms must be able to move between different and competing AI systems to avoid lock-in. Accordingly, regulators should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. Regulators must ensure that there are many—for example, at least five—providers of AI software for banks that provide for base interoperability, so that not all institutions are using the same one or two pieces of software.

Question 11

> Question 11: In what ways could existing data privacy protections (such as those in the Gramm-Leach-Bliley Act (Pub. L. 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?[18]

The Gramm-Leach-Bliley Act (GLBA) "requires the banking and financial regulators to "establish appropriate … administrative, technical, and physical safeguards" for institutions that 1) "insure the security and confidentiality of customer records and information"; 2) "protect against any anticipated threats or hazards to the security or integrity of such records"; and 3) "protect against unauthorized access to or use of [customer information]." Under this authority, the federal banking regulators have implemented interagency guidelines for establishing information security standards and issued IT and cybersecurity risk management guidance."[19] In this vein, we recommend that regulators, including the Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission, Consumer Financial Protection Bureau, consider using GLBA authority to ensure resilience against AI-designed cyber threats specifically by requiring:[20]

- Third-party AI audits for all institutions;
- Red-teaming of AI for the largest institutions; and

[17] Phillips and Conner, "Financial Regulatory Agencies."
[18] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50054.
[19] Phillips and Conner, "Financial Regulatory Agencies"
[20] Phillips and Conner, "Financial Regulatory Agencies," p. 11.

- Disclosure of annual resources on AI cybersecurity and AI risk management and compliance.

Question 18

> 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?[21]

Our previous work mapping agency regulatory authority in the artificial intelligence and automated technology space is most directly responsive to Question 18 of the RFI. Below, we offer a summary of the proposals contained in the financial regulation chapter of our report. More details are available in the full chapter, attached to this comment and available online.[22]

As a general matter, most of our recommendations attempt to establish the same core set of regulatory mechanisms wherever possible across the financial sector, including:

- **Minimum risk management practices**: The OMB M-24-10 AI guidance requires minimum risk management practices for federal agencies that utilize AI for certain purposes presumed to be safety-impacting or rights-impacting. These steps, including AI impact assessments and other requirements, could be repurposed for use beyond federal agencies, such as at banks or financial services institutions.

- **AI audits**: The development of an independent third-party AI auditing ecosystem is being explored to ensure effective risk management and compliance with AI systems. AI audits in this context can include both the data used to train AI systems and the AI systems themselves, including their source code. The audits would also include third parties utilizing AI for banks or other financial institutions as vendors or contractors. In all cases, regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Ensuring explainability and legibility**: The 2022 AI Bill of Rights made "notice and explanation" a key principle for the safe use of AI, noting that people "should know that an

[21] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50055.
[22] Phillips and Conner, "Financial Regulatory Agencies."

automated system is being used and understand how and why it contributes to outcomes that impact you" and that automated systems should "provide clear, timely, understandable, and accessible notice of use and explanations." The 2023 AI executive order noted that "requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models" should be a priority for independent agencies, including independent financial regulators. This expectation for explainability and legibility is also reflected in the OMB M-24-10 AI guidance for federal agencies using or procuring AI, which notes: "Explanations might include, for example, how and why the AI-driven decision or action was taken. This does not mean that agencies must provide a perfect breakdown of how a machine learning system came to a conclusion, as exact explanations of AI decisions may not be technically feasible. However, agencies should still characterize the general nature of such AI decisions through context such as the data that the decision relied upon, the design of the AI, and the broader decision-making context in which the system operates. Such explanations should be technologically valid, meaningful, useful, and as simply stated as possible, and higher-risk decisions should be accompanied by more comprehensive explanations."
Financial regulators should collaborate with others in the public and private sector as they develop best practices for explanation and legibility.

- **AI red-teaming**: The 2023 AI executive order defined AI "red-teaming" as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI." Red-teaming has emerged as a method to test AI that is embraced by leading generative AI companies and has been a focus of the White House in voluntary commitments, the executive order, and the OMB M-24-10 AI guidance. This can also include red team/blue team exercises, whereby the blue team defends the systems against the simulated penetrations, or "violet-teaming," which attempts to address broader systemic societal issues in adversarial testing.

- **Disclosure of annual resources spent on AI cybersecurity and AI risk management and compliance:** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in banking operations, the potential vulnerabilities and risks associated with cyber threats amplify significantly. By mandating such disclosures, regulators can ensure customers, policymakers and investors gain valuable insights into a bank's commitment to mitigating cyber risks through AI.

- **Where relevant, providing for human review of AI-influenced determinations:** Since AI-based systems may use black-box algorithms to make various financial determinations (e.g. determining credit scores or determining the inputs that will influence a credit score), individually traceable data are required for adequate human review.

- **Where possible, ensuring firms can move between different AI systems:** The sheer amount of computing power involved in generative AI means that most financial institutions will not be developing their systems in-house; instead, they will license software from a few competing nonfinancial institutions. It is imperative that financial firms are able to move between different

and competing AI systems to avoid lock-in. Accordingly, regulators should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for an easy transition to a competing system upon the contract's expiration. Regulators must require that all registrants and registered entities ensure that there are many—for example, at least five—providers of AI software that provide for base interoperability before entering contracts, so that not all institutions use the same one or two pieces of software.

Summarizing report proposals

What follows is a brief summary of our report's proposals regarding the financial services sector. The full chapter and fact sheet with a full list of recommendations is attached for those interested in more detail.

Some of our proposals derive from statutory authorities jointly administered by Treasury and other agencies:

- Under the **Bank Secrecy Act**, we propose that Treasury and the other relevant agencies:
    - Regulate how institutions' customer identification and suspicious activity reporting programs use AI; and
    - Require banks to periodically review their BSA systems to ensure accuracy and explainability.

- Under the **Gramm-Leach-Bliley Act,** we propose that the Office of the Comptroller of the Currency and the other relevant agencies:
    - Require third-party AI audits for all institutions;
    - Require red-teaming of AI for the largest institutions; and
    - Require disclosure of annual resources on AI cybersecurity and AI risk management and compliance.

- Under the **Community Reinvestment Act**, we propose that the banking regulators:
    - Require banks to indicate whether they use AI to comply with Community Reinvestment Act (CRA) regulations and, if so, require those systems to be explainable.

- Under the **Federal Deposit Insurance Act, Federal Credit Union Act, and the Bank Holding Company Act,** we propose that regulators at Treasury and elsewhere:
    - Require financial institutions' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict standards, and require those institutions to periodically review their customer-facing AI systems to ensure accuracy and explainability;
    - Ensure banks' capital structures can withstand sudden and deep withdrawals of customer deposits or losses from banks' risk management processes;
    - Require that AI systems that are parts of banks' capital, investment, and other risk management models be explainable;
    - Ensure firms may move between different AI systems before they contract for one system; and

    - Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.

- Under the **Dodd-Frank Act**, we propose that the Financial Stability Oversight Council:
    - Designate major providers of AI services to financial institutions as systemically important if they reach an adoption level that creates vulnerability; and
    - Designate the cloud service providers to those firms designated as systemically important.

Other proposals stem from statutes that don't implicate Treasury directly but are included given Question 18's request concerning "what actions do you recommend others take?"[23] These include:

- Under the **Equal Credit Opportunity Act**, we propose that the Consumer Financial Protection Bureau ("CFPB"):
    - Require lenders to periodically review their lending systems to ensure explainability and that no new discriminatory activity applies;
    - Prohibit lenders from using third-party credit scores and models developed with unexplainable AI; and
    - Require lenders to employ staff with AI expertise.

- Under the **Fair Credit Reporting Act** ("FCRA"), we propose that the CFPB:
    - Require credit reporting agencies to describe whether and to what extent AI was involved in formulating reports and scores;
    - Require credit reporting agencies to periodically review their AI systems to ensure explainability and that no new discriminatory activity applies;
    - Require credit reporting agencies to provide for human review of information that consumers contest as inaccurate;
    - Update model forms and disclosures to incorporate disclosure of AI usage;
    - Require purveyors of workplace surveillance technologies to comply with the FCRA; and
    - Ensure that electronic surveillance and management technologies used by employers comply with the FCRA.

- Under the **Consumer Financial Protection Act,** we propose that the CFPB:
    - Require financial institutions' consumer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict consumer protection standards, periodically reviewing consumer-facing AI systems to ensure accuracy and explainability;
    - Require AI red-teaming and red team/blue team exercises for the largest institutions;
    - Require third-party AI audits for all institutions; and
    - Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.

[23] Department of the Treasury, "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector," p. 50055.

- Under the **Securities Exchange Act of 1934**, we propose that the Securities and Exchange Commission ("SEC"):
    - Require that AI systems that are parts of brokers' capital, investment, and other risk management models be explainable;
    - Require brokers' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with those brokers periodically reviewing their customer-facing AI systems to ensure accuracy and explainability;
    - Require brokers using AI systems to make investment recommendations to ensure those systems are explainable and operate in clients' best interests;
    - Require red-teaming of AI for exchanges, alternative trading systems, and clearinghouses;
    - Ensure firms may move between different AI systems before they contract for one system; and
    - Require disclosure of annual resources dedicated to cybersecurity spending and AI risk management and compliance.

- Under the **Investment Advisers Act of 1940**, we propose that the SEC:
    - Require that registered investment advisers' (RIAs) AI systems used to make investment recommendations are explainable and operate in clients' best interests;
    - Require RIAs' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with RIAs periodically reviewing their customer-facing AI systems to ensure accuracy and explainability; and
    - Ensure RIAs may move between different AI systems before they contract for one system.

- Under the **Commodity Exchange Act**, we propose that the Commodity Futures Trading Commission:
    - Require AI systems that are parts of futures commission merchants', swap dealers', or major swap participants' capital, investment, or other risk management models to be explainable;
    - Require futures commission merchants' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards;
    - Require that FCMs' AI systems used to make investment recommendations be explainable and operate in clients' best interests;
    - Require red-teaming of AI for swap dealers, exchanges, and clearinghouses;
    - Require third-party AI audits for all institutions;
    - Ensure firms can move between different AI systems before they contract for one system; and
    - Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.

Conclusion

We applaud the Treasury's attention to this important set of issues and are grateful for the opportunity to comment. We have attached Chapter 5, “Financial Regulatory Agencies,” in full, along with the accompanying factsheet that includes the recommendations. Further questions can be directed to Adam Conner (aconner@americanprogress.org) at CAP or Will Dobbs-Allsopp (wdobbsallsopp@governingforimpact.org) at GFI. We are always happy to answer any further questions.