U.S. DEPARTMENT OF THE TREASURY

Artificial Intelligence in Financial Services

Report on the Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector

December 2024

*Staff Acknowledgements**

The Office of Financial Institutions, including Acting Assistant Secretary Laurie Schaffer, Deputy Assistant Secretary Jeanette Quick, Director Moses Kim, lead authors Senior Policy Advisor Liang Jensen and Senior Policy Advisor Casey Laxton, and contributors Senior Policy Advisor Josh Nimmo, Senior Policy Advisor Ben Hobbs, and Fellow Jack Ginsberg, led the preparation of this report, in collaboration with Treasury staff from the Office of Financial Institutions Policy, Federal Insurance Office, Office of Capital Markets, Office of Consumer Policy, Office of Cyber Security and Critical Infrastructure Protection, Office of General Counsel, Office of International Financial Markets, and Office of Terrorism and Financial Intelligence.

** The cover design of this report was assisted by artificial intelligence.*

Contents

I. Executive Summary

On June 12, 2024, the United States Department of the Treasury (Treasury) published a request for information on the Uses, Opportunities, and Risks of Artificial Intelligence (AI) in the Financial Services Sector (AI RFI).[1] Through the AI RFI, Treasury sought input on key issues relating to AI deployment within the financial services sector, including the opportunities and risks presented to financial firms, including banks and nonbanks, by their own use of AI, and the opportunities and risks facing consumers, investors, businesses, regulators, end-users, and any other entity impacted by deployment of AI.[2]

The AI RFI closed for public comment on August 12, 2024. In response to the AI RFI, Treasury received 103 comment letters from a variety of stakeholders, including financial firms, consumer advocacy groups, technology providers, financial technology companies, trade associations, and consulting firms. Considered in their entirety, these comment letters demonstrated that AI is used increasingly throughout the financial sector to support a broad range of functions and firms. The respondents[3] commented on existing use cases, expansive opportunities, and associated risks[4], underscoring the potential for AI to broaden opportunities while amplifying certain risks. In particular, many respondents noted that emerging AI technologies such as Generative AI are driving expanded use cases but also introducing new risk, leading firms to be cautious about deploying them broadly in customer-facing applications. Additionally, respondents highlighted differences in supervision for banks and nonbanks developing and deploying AI, as well as the resource gap and dependency on third-party providers for smaller financial firms. This feedback carries important implications for future work by Treasury and financial regulators, as

---

1 Treasury, Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector, 89 Fed. Reg. 50048 (Jun. 12, 2024), https://www.federalregister.gov/documents/2024/06/12/2024-12336/request-for-information-on-uses-opportunities-and-risks-of-artificial-intelligence-in-the-financial (Treasury AI RFI, or the AI RFI).

2 *Id.* "*Financial institutions*" in the AI RFI includes banks, credit unions, insurance companies, nonbank 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. This report uses the term "financial firms" instead to reflect the broad scope of institutions included in financial services. "*Impacted entities*" in the AI RFI includes consumers, investors, financial institutions, businesses, regulators, end-users, and any other entity impacted by financial institutions' use of AI.

3 Throughout this report, "respondent" is used to reference individuals and entities that provided public feedback through public comment letters about the AI RFI, as well as those who provided feedback directly to Treasury staff.

4 In addition to the risks highlighted here, respondents also raised concerns about risks related to cybersecurity and financial stability. As Treasury authored or contributed to analysis and recommendations related to these areas in separate materials, they are not the focus of the discussion in this report. *See, e.g.,* Treasury, Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector (Mar. 2024), https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf (Treasury AI Cybersecurity Report); Financial Stability Oversight Council, Annual Report (Dec. 6, 2024), https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.pdf (FSOC 2024 Annual Report); Financial Stability Oversight Council, Annual Report (2023), https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf (FSOC 2023 Annual Report); and Financial Stability Board, The Financial Stability Implications of Artificial Intelligence (Nov. 14, 2024), https://www.fsb.org/uploads/P14112024.pdf.

existing laws, regulations, and guidance, while applicable and largely supported by respondents, may require enhancement to address the growing complexities posed by accelerated AI development. To that end, many respondents expressed support for a number of government actions, including:

1. Aligning definitions of AI models and systems applicable to the financial services sector to facilitate interagency collaboration and coordination with stakeholders;
2. Considering providing additional clarification on standards for data privacy, security, and quality for financial firms developing and deploying AI;
3. Considering expanding consumer protections to mitigate consumer harm;
4. Considering clarifying how to ensure uniform compliance with current consumer protection laws that apply to existing and emerging technologies and providing additional guidance to assist firms as they assess AI models and systems for compliance;
5. Enhancing existing regulatory frameworks and develop consistent federal-level standards to mitigate risks associated with potential regulatory arbitrage and conflicting state laws while clarifying supervisory expectations for financial firms developing and deploying AI; and
6. Facilitating domestic and international collaboration among governments, regulators, and the financial services sector and pursue public-private partnerships to share information and best practices, promote consistency for standards, and monitor concentration risk.

This report provides background on the use of AI in financial services based on respondents' comments and building on observations from previous Treasury reports and stakeholder engagement,[5] highlights Treasury's ongoing efforts to evaluate recent developments in AI, and summarizes key recommendations from respondent feedback. Next, the report details the respondents' comments on current and potential AI use cases, along with the associated risks, opportunities, and proposed risk mitigation strategies. Finally, the report identifies policy considerations based on Treasury's analysis of the AI RFI responses and lays out potential next steps to be considered by Treasury, government agencies, and the financial services sector, including:

1. Treasury recommends continuing international and domestic collaboration among governments, regulators, and the financial services sector to promote consistent and robust standards for uses of AI in the financial services sector.
2. Treasury recommends further analysis and stakeholder engagement to explore solutions for any identified gaps in the existing regulatory frameworks,[6] and to

[5] Treasury, Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets (Nov. 2022), https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf (Treasury Non-bank Report); Treasury AI Cybersecurity Report, *supra* note 4.

[6] FSOC 2024 Annual Report, *supra* note 4. The report noted that the authority to supervise third-party service providers varies among financial regulators and recommended that Congress pass legislation to ensure that relevant agencies have adequate examination and enforcement powers to oversee third-party service providers that interact with their regulated entities.

address the potential risk of AI causing consumer harm, as identified by the respondents.

3. Treasury recommends financial regulators continue coordinating to identify potential enhancements to existing risk management frameworks and working with other government agencies to clarify supervisory expectations on the application of frameworks and standards, where appropriate.
4. Treasury recommends the financial services sector and government agencies further facilitate financial services-specific AI information sharing, alongside the AI cybersecurity forum recommended in the Treasury AI Cybersecurity Report, to develop data standards, share risk management best practices, and enhance understanding of emerging AI technologies in financial services.
5. Treasury recommends that financial firms prioritize their review of AI use cases for compliance with existing laws and regulations before deployment and that they periodically reevaluate compliance as needed.

II. BACKGROUND

AI has long been deployed in the financial services sector in a variety of ways, including credit underwriting, insurance underwriting, trading, investment advice, customer service, compliance, forecasting, and process automation.[7] The use of AI in general – such as traditional machine learning algorithms – can be traced back to the 1940s.[8] Many AI uses in the financial services sector can be categorized under the traditional machine learning method – or "traditional AI" – in which statistical models are trained on a dataset with input and output parameters.[9] The last two years, however, marked a major shift from traditional AI with an acceleration in the development of emerging AI technologies – such as deep learning models utilizing neural networks and "Generative AI." Generative AI differs from traditional AI in its ability to create new content based on what is learned from the training data. Generally, Generative AI relies on more sophisticated models that are trained on vast amounts of data.[10] The President's Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence from October 30, 2023 (AI EO)[11] defined Generative AI as "the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content" and noted that Generative AI can produce "images, videos, audio, text, and other digital content."[12]

Financial firms are in the early stages of understanding and deploying emerging AI technology, including Generative AI, as noted in the AI RFI feedback. Emerging AI, including Generative AI models, are generally trained on more extensive datasets than traditional AI models and require distinct model development processes and model training techniques compared to traditional AI models. Many financial firms rely on third-parties to develop and deploy these more advanced AI models, and the rapid rise of open-source tools is also changing the way models are developed and deployed. Additionally, developing and overseeing Generative AI models require significantly more advanced expertise, higher computational power, and more substantial financial investment than traditional AI models. Furthermore, Generative AI models exhibit a greater level of

---

7 *See* THE ALAN TURING INSTITUTE, ARTIFICIAL INTELLIGENCE IN FINANCE (Apr. 2019), https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_0.pdf; Treasury AI RFI, *supra* note 1.

8 *See* ALAN TURNING INSTITUTE, *supra* note 7; Treasury AI RFI, *supra* note 1.

9 SARAH HAMMER, NAVIGATING THE NEURAL NETWORK: ARTIFICIAL INTELLIGENCE IN FINANCE AND RECALIBRATION OF THE REGULATORY FRAMEWORK (Oct. 2024), https://pennreg.org/wp-content/uploads/2024/10/Hammer-Navigating-the-Neural-Network.pdf.

10 IBM, What Are Foundation Models? (Oct. 11, 2024), https://www.ibm.com/think/topics/foundation-models?utm_source=chatgpt.com. Generative AI systems are built on "foundation models" – a term that describes a type of large-scale AI model trained on vast amounts of data, providing foundational capabilities to be fine-tuned for applications across various sectors.

11 WHITE HOUSE, EXECUTIVE ORDER 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 (AI EO). The AI EO calls for society-wide effort that includes government, the private sector, academia, and civil society to meet the challenges and opportunities posed by AI.

12 *Id*.

complexity and can be susceptible to "AI hallucinations,"[13] producing confidently stated but incorrect output, presenting new challenges for AI governance and management.[14]

As the use of AI has evolved, Treasury has continued to monitor technological developments and their applications and potential impacts in financial services to help inform any potential policy deliberations or actions. The AI RFI is one of many efforts in which Treasury has been engaging with stakeholders to improve Treasury's understanding of the applications of AI within the financial services sector. Treasury's Nonbank Report published in 2022 explored opportunities and risks related to the use of AI in assessing the impact of nonbank firms (including fintechs) on competition in the consumer finance market.[15] As directed by the AI EO, Treasury published a report in March 2024 on AI and cybersecurity and fraud risks through extensive outreach on AI-related cybersecurity risks in the financial services sector.[16]

In June 2024, the Financial Stability Oversight Council (FSOC) Secretariat hosted a conference on AI and financial stability to explore potential systemic risks posed by AI in financial services.[17] FSOC identified the use of AI in financial services as a systemic vulnerability in its 2023 Annual Report. In its 2024 Annual Report, FSOC recommended continued monitoring of the rapid development of the usage of AI technologies in financial services to ensure policies are updated to address emerging risks to the financial system while facilitating efficiency.[18] In September 2024, Treasury hosted a roundtable discussion with representatives from the insurance industry, consumer groups, state insurance regulators, academics, and other stakeholders to gather more feedback about AI in the insurance sector.[19]

Additionally, in May 2024, Treasury issued its National Strategy for Combating Terrorist and other Illicit Financing, noting that AI has significant potential to strengthen anti-money laundering/countering the financing of terrorism (AML/CFT) compliance in the financial sector.[20] In October 2024, Treasury released its inaugural U.S. National Strategy for Financial Inclusion, which acknowledges the potential risks and opportunities for AI to expand consumers' access to financial products and services.[21]

---

13 IBM, *What are AI Hallucinations?* (Jun. 2024), https://www.ibm.com/topics/ai-hallucinations.

14 Florence G'Sell, Regulating Under Uncertainty: Governance Options for Generative AI (Sep. 2024), https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai.

15 Treasury Non-bank Report, *supra* note 5.

16 Treasury AI Cybersecurity Report, *supra* note 4.

17 Financial Stability Oversight Council, 2024 Conference on Artificial Intelligence and Financial Stability (Jun. 6-7, 2024), https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/financial-stability-oversight-council/2024-conference-on-artificial-intelligence-financial-stability.

18 *See* FSOC 2024 Annual Report, *supra* note 4; FSOC 2023 Annual Report, *supra* note 4.

19 Treasury, *Readout: U.S. Department of the Treasury Hosts Roundtable on Artificial Intelligence in the Insurance Sector* (Sept. 24, 2024), https://home.treasury.gov/news/press-releases/jy2607.

20 Treasury, 2024 National Strategy for Combating Terrorist and Other Illicit Financing (May 2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

21 *See* Treasury, National Strategy for Financial Inclusion in the United States: Fostering Financial Access, Resilience, and Well-Being for All (Oct. 2024), https://home.treasury.gov/system/files/136/NSFI.pdf.

Notably, Treasury's Office of Payment Integrity within the Bureau of the Fiscal Service announced its latest efforts in enhancing fraud detection processes in October, including the use of machine learning AI to expedite the identification of Treasury check fraud, which resulted in $1 billion in recovery of fraud and improper payments.[22] In November 2024, the Office of Financial Research released its annual report which noted that AI may pose new risks and vulnerabilities given sudden changes in adoption.[23]

Treasury also continues to engage with its foreign counterparts, including through the Financial Stability Board,[24] G7, and G20, on the implications of AI for the global economy and financial stability and to promote interoperability and alignment in regulatory approaches.

Lastly, Treasury has continued to coordinate with the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC) to establish an AI Executive Steering Group and address issues identified in the Treasury AI Cybersecurity Report.

---

22 *See* TREASURY, *Press Release: Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal Year 2024* (Oct. 17, 2024), https://home.treasury.gov/news/press-releases/jy2650.

23 *See* OFFICE OF FINANCIAL RESEARCH, ANNUAL REPORT (2024), https://www.financialresearch.gov/annual-reports/files/OFR-AR-2024_web.pdf.

24 NELLIE LIANG, U.S. TREASURY UNDERSECRETARY FOR DOMESTIC FINANCE, REMARKS ON ARTIFICIAL INTELLIGENCE IN FINANCE (Jun. 4, 2024), https://www.fsb.org/2024/06/remarks-by-nellie-liang-on-artificial-intelligence-in-finance/.

III. Key Recommendations Based on Summary of Responses

Public feedback from respondents including a broad array of stakeholders, as outlined in Section IV below, recommended several potential actions to be taken by government agencies and the financial sector, including:

- *Align definitions of AI models and systems applicable to the financial services sector to facilitate interagency collaboration and coordination with stakeholders*

Respondents provided divergent views but broadly agreed on the need for alignment on definitions of key terms and on the scope of AI definitions. Many respondents supported the definition in the AI RFI but suggested Treasury consider alternative definitions—such as those used by the Organization for Economic Co-operation and Development (OECD)[25] and the European Union (EU).[26] Some respondents expressed concerns that the definition used in the AI RFI was too broad and would therefore hinder innovations by including traditional statistical models and technologies that should not be regulated by an AI governance framework. Others recommended adopting a widely accepted definition of AI developed by a standard-setting body to ensure clarity. Overall, respondents generally agreed that consistent AI definitions would enhance collaboration among government agencies, reduce regulatory uncertainty, and minimize friction for financial firms operating across jurisdictions.

- *Consider providing additional clarification on standards for data privacy, security, and quality for financial firms developing and deploying AI*

Respondents emphasized the need of high-quality data – clean, complete, standardized, and comprehensive – for training AI models, testing efficacy, and reducing bias. To ensure high-quality data for developing and deploying AI, respondents recommended various strategies to fine tune datasets and data curation. Ensuring data security – protecting stakeholders (including firms, consumers, and end users) from data

[25] OECD defines an "AI System" as a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. OECD, OECD AI Principles Overview, https://oecd.ai/en/ai-principles.

[26] The EU AI Act defines an "AI system" as a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. EU AI Act, https://artificialintelligenceact.eu/article/3/.

breaches and data manipulation – and data privacy is critical to respondents. Respondents also raised concerns about intellectual property, data authorization, and unauthorized data use. Some respondents called for a robust, industry-wide data protection framework to comprehensively address current risks, noting that the existing data protection framework is fragmented. Other respondents suggested adopting existing or voluntary AI governance and risk management frameworks to address these risks. Some respondents also suggested legislation that encourages prioritizing data quality and protection while avoiding cost-cutting measures that undermine critical data-related safeguards.

- *Consider expanding consumer protections to mitigate consumer harm*

Respondents emphasized the need for policymakers and regulators to address the potential risk of AI models and systems causing consumer harm through opaque data collection, privacy violations, and exacerbation of biases resulting in discrimination. Respondents' views varied on whether existing laws – such as the Gramm-Leach-Bliley Act (GLBA) – are sufficient or need enhancements. Many respondents supported an opt-in model for data collection withdrawal options, and regulatory limits to reduce data breach risks. To mitigate bias-related risks, respondents suggested incorporating fair lending principles, using alternative data for "credit invisible" consumers, and strengthening compliance monitoring, while urging regulators to enhance fair lending oversight, mandate explainable AI models, and promote transparency.

- *Consider clarifying how to ensure uniform compliance with current consumer protection laws that apply to existing and emerging technologies and providing additional guidance to assist firms as they assess AI models and systems for compliance*

While financial firms may be subject to existing consumer protection laws such as the Fair Housing Act, Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA), respondents suggested regulators take additional steps to clarify ways to ensure uniform compliance with consumer protection laws that apply to existing and emerging technologies between banks and nonbanks and bolstering stronger compliance processes. Some respondents noted that additional regulatory guidance can encourage firms to develop and deploy AI in ways that lead to more competition in the market. Respondents stressed the need to address AI systems' potential to exacerbate discrimination. Suggestions included regulators monitoring financial product pricing, requiring explainable AI models, and identifying "less discriminatory alternatives" – methods that achieve the same objectives while reducing bias and the possibility of unfair outcomes – for compliance with fair lending laws.

- *Enhance existing regulatory frameworks and develop consistent federal-level standards to mitigate risks associated with potential regulatory arbitrage and conflicting state laws while clarifying supervisory expectations for financial firms developing and deploying AI*

Respondents highlighted the risk of regulatory arbitrage due to varying levels of oversight across financial firms and jurisdictions and suggested enhancing existing frameworks to mitigate associated risks, particularly for risks associated with emerging AI technologies like Generative AI. Respondents reflected on whether voluntary adoption of the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (NIST AI RMF)[27] would satisfy regulatory expectations and supported collaboration between NIST and Treasury to develop a financial sector-specific AI risk profile. Respondents noted lack of clarity as to how financial regulators' standards and expectations use the NIST AI RMF, if at all, and whether the NIST AI RMF is aligned with prudential or other regulatory expectations related to AI. Separately, many respondents advocated for consistent federal-level standards to mitigate risks associated with fragmented state laws,[28] which can impose uneven requirements on financial firms. A consistent regulatory approach was viewed as essential to protecting consumers, competition, and national security while fostering responsible innovation. Respondents stressed the need for regulations that ensure fairness and safety without creating barriers, especially for smaller firms operating across multiple jurisdictions.

- *Facilitate domestic and international collaboration among governments, regulators, and the financial services sector and pursue public-private partnerships to share information and best practices, promote consistency, and monitor concentration risk*

Respondents widely supported public-private partnerships and encouraged Treasury and the federal government to continue facilitating collaboration across industries. Some respondents recommended creating an interagency group led by Treasury to share information on trends, risks, and regulatory expectations. Respondents emphasized the importance of including diverse stakeholders, such as industry representatives, academics, consumer advocates, civil rights groups, and regulators, alongside representatives from outside the financial services sector such as technology companies. Treasury was also suggested as a resource to aggregate and distribute data on suspicious transactions to improve AI models for fraud detection and AML/CFT

---

27 NIST, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK 1.0 (Jan. 26, 2023), https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development.

28 Multiple insurance industry respondents reiterated that the business of insurance in the United States is primarily regulated at the state level. These respondents noted that state insurance regulators oversee AI use, that existing state insurance laws and regulations are sufficient to govern insurers' use of AI, and that federal regulation of AI use in insurance is unwarranted. Respondents specifically emphasized the National Association of Insurance Commissioners' adoption of its *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers* in December 2023, which has been adopted by 18 states and the District of Columbia. *See* NAIC, Implementation of NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers (as of Dec. 1, 2024), https://content.naic.org/sites/default/files/cmte-h-big-data-artificial-intelligence-wg-ai-model-bulletin.pdf.pdf. *See also* Section V.1.

compliance. Some respondents also suggested that Treasury and other federal agencies enhance the monitoring of AI-related concentration risk and consider ways for risk mitigation as necessary. Additionally, respondents urged Treasury to collaborate with international organizations and foreign counterparts to facilitate interoperability efforts and harmonize standards, which could aid financial firms operating across multiple jurisdictions.

IV. Summary of Responses to the AI RFI

A. Responses on the Current Uses and Potential Opportunities of AI in Financial Services

The AI RFI requested feedback from respondents on current and potential AI use cases. One of the most significant learnings from the comment responses is the reported ubiquity of AI usage – in particular traditional AI such as algorithms or machine learning – in virtually every function of financial firms, ranging from compliance management, internal operations, underwriting, customer service, treasury management, and product development and marketing. Respondents also indicated that although many Generative AI use cases are in early stages, a rapid expansion of AI use cases, and in particular, Generative AI use cases in financial services is expected in the coming years. This may have important implications for the existing regulatory frameworks and significant impacts for the financial system as a whole. This section provides a summary of feedback on the current uses and opportunities of AI, and the following section discusses feedback related to the risks associated with AI use cases. The use cases noted by respondents include: (1) external consumer-facing and investor-facing uses; and (2) internal uses. These use cases and opportunities are discussed in more detail below.

1. Traditional AI and Generative AI Uses

Respondents noted a long-standing history of financial firms using AI – such as algorithms or machine learning – for external- and internal-facing operations, including credit underwriting, trading and investment, risk management, regulatory compliance, customer service, and back-office operations. Respondents also noted that some financial firms have been experimenting with Generative AI tools – to explore the capabilities of AI in enhancing existing processes.[29] Respondents cited recent surveys indicating almost eight in ten (78%) financial firms are implementing Generative AI for at least one use case and 86% of financial firms expect a significant or moderate increase in their model inventory due to Generative AI adoption.[30] Many respondents highlighted that the use of

[29] IBM, *2024 Global Outlook for Banking and Financial Markets: Regenerate Banking with AI* (2024), https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2024-banking-financial-markets-outlook. The report notes that, through a survey with 600 bank executives worldwide, almost 78% (8 in 10) institutions are implementing generative AI for at least one use case, with 8% of them taking a more systemic approach by implementing generative AI across the enterprise. The top use cases are focused on enhancing risk and compliance (32%), improving client engagement (26%), and software development (24%). *See also* IIF, *2023 Public Survey Report on AI / ML Use in Financial Services* (2023), https://www.iif.com/About-Us/Press/View/ID/5611/New-IIF-EY-Survey-Finds-Generative-AI-Could-be-Revolutionary-for-Financial-Services. The report notes that 86% of the 65 financial firms participating in the survey expected a significant or moderate increase in their model inventory due to Generative AI adoption, with 37% of respondents indicating significant expansion in uses cases ahead. Respondents noted near-term use cases of Generative AI in risk identification and assessment, code assistance, document querying and extraction, and financial crime/AML.

[30] *See* IBM and IIF, *supra* note 29.

emerging AI technologies is in its early stages, only being gradually integrated in the financial services sector, and mainly beginning with business functions such as risk and compliance, client engagement, code assistance, and content extraction. Many respondents noted the potential of Generative AI to bring transformative impact to the financial services sector, suggesting that the sector could see an expansion of Generative AI use cases ahead.

2. External and Internal Uses by Financial Firms

Respondents highlighted various consumer-facing uses of AI in financial services, such as tailoring service offerings and driving customer engagement. Payment providers were cited as using AI to analyze point-of-sale data to provide personalized recommendations to customers. AI also enables easier customer sentiment analysis and market research by processing unstructured data like emails, pictures, voice notes, and social media posts. In credit underwriting, respondents noted the use of machine learning to analyze alternative data, such as rent payments, utility bills, and geolocation data. Though alternative data can be used to evaluate creditworthiness without relying on machine learning or emerging AI tools, respondents said that the ability of AI to process large amounts of data makes it a more appealing option. Meanwhile, emerging AI technologies such as Generative AI are increasingly used for processing unstructured data like customer communications.

In investor-facing financial services, respondents reported that AI is widely used in investment and trading. For example, robo-advisors offer personalized investment advisory services, while AI-driven insights improve forecasting and trading process automation. AI can also inform trading strategies by identifying patterns, optimizing execution, managing portfolio workflows, and assessing risk-return tradeoffs.

In the insurance industry, respondents highlighted AI's role in underwriting, claims processing, fraud detection, marketing, and risk management. Property and casualty insurers reported using AI to analyze claims data in real time, detect inconsistencies, forecast catastrophic weather losses, and expedite claims payments. Similarly, life insurers use AI for pricing, marketing, and underwriting functions.

Respondents noted that AI has significant potential to improve financial inclusion by enhancing access to services for underserved communities. Respondents cited examples like using alternative data to expand credit access for minorities and small businesses without credit histories, as well as AI-driven microfinance initiatives where AI could enhance the existing process of evaluating and granting small loans. Natural language processing tools can enable personalized customer service, including translation and transcription, supporting minorities and individuals with disabilities. Respondents highlighted AI's potential to reduce bias by screening for discriminatory patterns in processes like mortgage underwriting and by identifying less discriminatory model alternatives.

Respondents noted that financial firms are increasingly using AI – and particularly experimenting with Generative AI – for internal business operations, including but not limited to risk management, regulatory compliance, treasury management, fraud detection, and back-office functions. AI is widely used for cybersecurity risk management, as highlighted in the Treasury AI Cybersecurity Report, and for AML/CFT and sanctions compliance, including analyzing large sets of data, detecting anomalies, flagging suspicious activities, and verifying customer identities under Bank Secrecy Act (BSA) obligations.[31] Generative AI has been deployed to complement an investigation platform in collating and summarizing data and automating report creation and filing. AI is also being used in compliance with risk management guidelines, including managing operational risks, meeting capital and liquidity standards, improving stress test scenarios, and enhancing forecasting accuracy. Generative AI can automate back-office functions like recordkeeping, predictive texting, transcribing audio, and advanced document searches. Respondents emphasized that these applications help financial firms streamline processes and improve operational efficiency.

Overall, respondents viewed AI as a transformative tool for improving operational effectiveness across financial services and that AI-driven insights have the potential to support better decision-making in business operations.

B. Potential Risks of AI and Suggestions on Risk Mitigations

In addition to seeking information on existing uses and potential opportunities associated with the use of AI by financial firms, the AI RFI sought to further understand information on the potential risks and possible solutions to address these risks. Though many of the AI-related risks highlighted by respondents echo those already familiar to financial firms, it is clear from the comment letters that the expansion of AI within the financial services sector has the potential to amplify these risks. This has important implications for future work by Treasury and financial regulators because existing laws, regulations, and guidance, while applicable, may need to be enhanced to address AI-specific risks and to address the differences in supervision for banks and nonbanks. Furthermore, as AI adoption continues to expand, some respondents suggested that in several areas, the existing laws and regulations may face challenges in addressing emerging complexities. Potential challenges were identified in areas such as data standards, consumer protection, and third-party relationships, which, if not addressed, could leave the financial system and consumers vulnerable to unmanaged risks and unintended consequences. This section summarizes the risks and solutions to mitigate those risks offered by respondents, generally grouped into six categories: (1) data privacy, security, and quality standards; (2) bias, explainability, and hallucinations; (3) impacts on consumers, fair lending, and

[31] The Customer Identification Program (CIP) Rule requires certain financial institutions covered by the BSA to implement a written program to verify the identity of their customers. Such programs must be risk-based, appropriate for the size and type of business, and include certain minimum requirements. The CIP must be incorporated into the institution's AML/CFT compliance program.

financial inclusion; (4) concentration-related risks; (5) third-party risks; and (6) illicit finance risks.

1. Data Privacy, Security, and Quality Standards

Respondents generally highlighted that high-quality data—which is clean, complete, standardized, and comprehensive—is needed to develop and train models and test their efficacy, including whether they incorporate bias. They also noted that data security protections must be in place to ensure that the model, once trained, can mitigate the risk of "data poisoning." Finally, respondents also discussed the importance of data privacy, as well as the risks of any flaws in data. While many respondents flagged data-related risks, there was disagreement among respondents about how to address them, including whether additional laws and regulations were appropriate. This section provides additional detail about respondents' views on how to address data-related risks.

Some respondents believe that existing regulatory standards and guidance may alleviate some concerns associated with AI data risks. For instance, the federal banking agencies' published guidance on model risk management highlights the importance of a "rigorous assessment of data quality and relevance."[32] However, this guidance applies to banking organizations only and some respondents suggested a need for legislation or regulation to expand these frameworks to nonbank firms. Though third-party risk management and similar guidance could apply data standards to nonbank firms, some respondents also questioned this approach, saying that when data is transferred outside of financial firms for AI training or processing purposes, it may become more difficult for the financial firms themselves to enforce data security standards.

Respondents also noted that GLBA provides some protections for consumer data that is used or managed by certain financial firms.[33] Title V, Subtitle A of the GLBA prohibits the disclosure of nonpublic personal information by certain financial firms to unaffiliated third-parties unless the consumer is provided notice about the disclosures and has chosen not to opt-out.[34] However, in certain situations, GLBA also permits the sharing of nonpublic personal information without the notice and opt-out requirement.[35] Several respondents called for changes to GLBA, including by moving from an opt-out standard – where financial institutions are allowed to share customer data unless the customer explicitly declines – to an opt-in. On the other hand, some respondents felt that the GLBA

---

[32] Federal Deposit Insurance Corporation, Supervisory Guidance on Model Risk Management (Jun. 17, 2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.html; Board of Governors of the Federal Reserve System, Guidance on Model Risk Management (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm; Office of the Comptroller of the Currency, 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.

[33] GLBA, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[34] 15 U.S.C. § 6801-6809.

[35] These exceptions to the GLBA privacy protections include: disclosures that are required by law, disclosures to certain rating agencies, disclosures permitted by a consumer, disclosures for certain types of marketing, and disclosures necessary to provide financial product or service to the consumer. *See* 15 U.S.C. § 6802.

protections were sufficient and that additional enhancements to GLBA may negatively affect model development, particularly if data could not be used to train models or would need to be removed from a trained model. While robust state-level data privacy laws are emerging, they often provide a carve-out for data covered by GLBA.[36] The Consumer Financial Protection Bureau (CFPB) published a report concluding that the effect of these carve-outs is to potentially leave consumer financial data less protected than other types of data, and urged reconsideration of this approach.[37] Respondents had varying views: some supported continuing to provide GLBA carve-outs at the state level, while others argued a better approach would be to enact a robust data protection framework that addresses current data risks that would apply across firms, regardless of industry.

To address data-related risks, some respondents proposed solutions and techniques in addition to existing requirements for protection that firms could implement on their own. For example, one respondent proposed that organizations use AI governance and risk management frameworks as well as additional tools such as homomorphic encryption (allowing data to be shared without compromising the encryption) and federated learning to augment data privacy. Another respondent noted that AI models themselves may offer the ability to improve existing data privacy controls with enhanced detection of privacy policy violations that currently evade hard-coded, rules-based systems. Additionally, some firms described the strategies and techniques they are utilizing to minimize their risks related to data quality. Specifically, some respondents suggested using data curation for retrieval augmented generation, fine-tuning models on high-quality data sets, and other data augmentation methods. One respondent noted the use of application interactions, device fingerprints, and customer support interactions to help create well-curated and validated training data for AI models to use.

Despite the existing standards and practices, some respondents said they would like policymakers to provide greater clarity around how to use AI and comply with: copyright laws; patent laws; trade secret protections; data ownership, licensing, and secondary use restrictions; model ownership; and intellectual property (IP) protection laws. Some respondents noted that many firms currently have governance and/or risk controls in place to enable AI risk assessments regarding IP, including related data and AI model risks, as well as disclosures to inform consumers of potential data uses. However, feedback from respondents raised questions about whether these measures are sufficient. Some respondents argued that unauthorized data collection or data sharing should be prohibited. Another respondent argued that owners of proprietary data should be compensated when their data is used by a model.

Some respondents identified the need for more clarity on how data is shared. The use of third-party AI models and systems, which is discussed in greater detail below, raises

[36] CFPB, STATE CONSUMER PRIVACY LAWS AND THE MONETIZATION OF CONSUMER FINANCIAL DATA (Nov. 2024), https://files.consumerfinance.gov/f/documents/cfpb_state-privacy-laws-report_2024-11.pdf.

[37] *Id.*

specific data confidentiality and security concerns and some respondents argued for data standards to address these. For example, some respondents would like standards to allow transaction data to be shared among financial firms for the purpose of illicit finance detection and prevention. Other respondents argued that standards could also address acceptable forms of privacy-enhancing technologies and the appropriate use cases for synthetic data. Respondents also discussed challenges of sharing data outside of the U.S., raising national security concerns and asking for clarity around whether doing so would be permissible.

2. Bias, Explainability, and Hallucinations

Respondents noted that the quality of AI models is critical to minimizing the risks and realizing the opportunities of emerging AI technology noted by respondents. In response to the AI RFI, respondents described key concerns about bias, which is generally when a model's results reflect human or data biases, as well as explainability, which includes the difficulty of understanding how models generate output. Moreover, respondents noted the concern about hallucinations – a risk unique to Generative AI models - in which a model convincingly produces an incorrect output. To address these concerns, respondents also proposed potential mitigation strategies. This section discusses the feedback provided related to these risks and risk mitigations.

The AI RFI asked for information about the potential for AI models to reinforce historical biases, and multiple respondents noted the associated risks. As one respondent noted, it is important to remember that AI models are not as impartial as they may appear to be but, if properly developed, could in theory produce less discriminatory results than current approaches. For example, AI offers firms the ability to analyze a greater set of variables to predict creditworthiness. Respondents expressed optimism this could lessen reliance on credit scores, which present concerns particularly for groups historically subject to discrimination.[38] However, improperly trained AI tools may reinforce or exacerbate bias. For example, training data that reflects a history of racial redlining or sexism may introduce bias, as can queries inputted directly by users. As a result, AI systems may inadvertently reinforce existing prejudices, create unfair outcomes, or lead to potential legal violations. For example, multiple respondents raised concerns regarding bias in credit underwriting and decision-making. Fair lending laws prohibit discriminatory practices in consumer lending and, as discussed below, apply regardless of the technology used to make the credit decision. However, as noted by the CFPB in its response letter, the use of AI must align with established legal standards, and institutions are responsible for ensuring their AI applications do not result in discriminatory outcomes prohibited under civil rights laws.

[38] CFPB, WHO ARE THE CREDIT INVISIBLES? (Dec. 2016), https://files.consumerfinance.gov/f/documents/201612_cfpb_credit_invisible_policy_report.pdf. The report noted that Black and Hispanic consumers are disproportionately likely to be credit invisible or have a thin credit file.

Respondents highlighted how some financial institutions are attempting to be proactive in mitigating potential bias from using AI, including by establishing internal guidelines for bias mitigation; using auditing, testing, and controls; or applying codes of ethics. Some respondents stated that they consult the federal banking agencies' model risk management guidance to assess their own models for unintended bias. Other respondents expressed skepticism that firms' have put in place frameworks that are sufficient to address the risk that AI models will amplify biases and hallucinations. Additionally, respondents noted that some techniques that can reduce bias, such as curating training data or using different models, can be expensive and may not provide meaningful improvements.

Another key concern noted by respondents is the difficulty in gaining greater transparency into how the model works, or the "explainability" of, AI models. The AI RFI described explainability as "the ability to understand a model's output and decisions, or how the model establishes relationships based on the model input…."[39] Some respondents noted that AI model complexity can cause reputational risk and mistrust among customers if the models are not sufficiently transparent and explainable, as well as potentially being in violation of consumer protection laws that may require explanatory notices to consumers about a firm's decisions related to that consumer (such as whether to provide a consumer a credit product). Multiple respondents highlighted challenges with the transparency, explainability, and accountability of using AI in decision-making processes. Respondents pointed out that models that operate as "black boxes" provide limited insight into the model's outputs, and present challenges for explainability, particularly in consumer-focused use cases.[40] Additionally, Generative AI models in use today have exponentially more parameters than the traditional machine learning models. Because the parameters are used to develop the model's predictions, respondents explained that the dramatic increase in the number of parameters makes it even more difficult to explain which particular one(s) influenced the result.

In addition to concerns regarding complexity, respondents also noted that financial firms face challenges because they may not receive from model vendors and developers access to the type of information needed to assess risks and develop controls. Some respondents asserted that model vendors and developers should grant them access to the AI models as well as the nonpublic impact assessments to help fully understand the risks and needed controls. On the other hand, other respondents expressed concerns that requiring excessive information disclosures to improve explainability of a particular AI

[39] Treasury AI RFI, *supra* note 1.

[40] The CFPB published guidance on adverse action notification requirements that are technology-agnostic and stated that creditors subject to the Equal Credit Opportunity Act (ECOA) and the CFPB's Regulation B are not permitted to use AI, complex algorithms, or "black-box" models when the creditor cannot provide the specific and accurate reasons for denying credit or taking other adverse actions against consumers. *See* 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/.

model may create vulnerabilities to cyberattacks or increase risks of personal data or trade secret exposures.

Some respondents also highlighted that a key priority among both AI developers and their customers has been reducing the frequency of hallucinations for Generative AI technology. Though it is still challenging for AI models to pinpoint the source of the errors generating output hallucinations, some respondents argued that strong data protection protocols, standards, and strategies could reduce these events.

Some respondents shared how financial firms have attempted to proactively identify and mitigate potential risks associated with AI to provide more transparency, explainability, and accountability. One respondent stated that retrieval augmented generation provides more transparency as to the basis of the responses and therefore enables the user to better assess the credibility of the output. Another respondent mentioned using back-testing and continuous output monitoring to test the rigor of its AI models, and that it is developing further methods of increasing model transparency, including audit trails of AI model decision-making. With respect to accountability, one respondent recommended that AI users create impact assessments, risk classifications, and mitigation assessments.

3. Impact on Consumers and Consumer Protections

Several respondents focused on the potential negative impact of AI on consumers and described concerns related to consumer-facing AI models and systems, consumer data rights, and the application of existing consumer protection laws. Though many – if not all – of the use cases and risks described throughout this section have potential implications for consumers and financial inclusion, this section describes feedback that respondents provided related specifically to consumers.

As described above, some argued that AI may provide opportunities to improve or personalize customer service, offer personalized products, and expand access to certain products or services, particularly credit products and financial advice. However, others argued that the lack of transparency about consumer data collection and the use of AI models raises specific risks and concerns. Additionally, some respondents asserted that the potential for consumer-impacting AI systems to exacerbate biases, as highlighted above, steer consumers to predatory products, or "digitally redline" communities suggests careful consideration is necessary to ensure consumer rights are protected and existing laws are followed. Indeed, the Blueprint for an AI Bill of Rights calls for greater protections for "automated systems that… have the potential to meaningfully impact the American

public's rights, opportunities, or access to critical resources or services… such as… financial services…."[41]

Several respondents said there are unique risks for AI systems that interact directly with consumers, and underscored the importance of accuracy and disclosures in these use cases. While many of the largest banks are using chatbots, respondents noted that some banks are hesitant to employ large language models (LLMs) in customer-facing applications because of concerns that inaccurate, inconsistent, or incomplete answers could lead to liability and reputational damage. These risks for financial firms are not unfounded,[42] and respondents offered a variety of solutions. For example, some advocated for an approach where regulators could potentially require that chatbots and similar tools respond accurately to consumer inputs, mandate pre-launch testing for AI models, or even require regulatory pre-approval before deploying a customer-facing AI model and system. Alternatively, some respondents recommended requiring a clear disclosure to consumers when AI tools are used to inform decisions about credit and other products for a consumer.

Another area of focus, highlighted above in risks related to data privacy, security, and quality standards, is the treatment of consumer data and the on-going data collection practices at many firms. Several respondents suggested that existing privacy laws are sufficient. Other respondents agreed there are some protections for nonpublic consumer data, but pointed out that compliance may not be assessed evenly for banks and nonbanks. A large amount of data is collected about most consumers, who may be unaware of the scope and depth of information accessible to firms, and how that information can be used to make decisions about them. To combat this, some respondents asserted that data collection and usage should be disclosed to consumers. Others disagreed, stating that disclosures are ineffective or counterproductive, in that they may alert bad actors or hinder fraud prevention or data privacy efforts. Some respondents advocated for an opt-in approach to consumer data sharing instead, provided that consumers are able to withdraw consent later. However, some argued that consent can be meaningless if no comparable alternative is available. In part because of this, some respondents suggested regulatory requirements include limits on the amount of data that is collected about a customer may be appropriate. In addition to supporting consumer privacy rights, some respondents noted that such limitations could mitigate some risks to a consumer from a potential data breach.

In situations where the consumer data collected is incomplete or inaccurate, respondents disagreed on whether existing guidance were sufficient to address data quality problems in AI systems. Several respondents pointed to the dispute processes required by the FCRA, which allow a consumer to challenge incorrect data used to make

---

41 White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

42 Lifshitz, Lisa R. and Roland Hung, *BC Tribunal Confirms Companies Remain Liable for Information Provided by AI Chatbot*, American Bar Association Business Law Today (Feb. 29, 2024), https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-february/bc-tribunal-confirms-companies-remain-liable-information-provided-ai-chatbot/.

certain credit decisions, and argued this was sufficient. However, other respondents highlighted the current limits of FCRA. For example, one respondent noted that FCRA does not apply to all consumer data nor to all providers of consumer data and said that it would be hard for consumers to challenge incorrect data that is not covered by FCRA's processes. Another respondent encouraged the CFPB to require a human review of data that consumers challenge under FCRA.

Beyond the transparency-related and data-related concerns noted above, consumer-impacting AI systems have the potential to discriminate by exacerbating existing biases. A number of respondents also pointed out that existing laws prohibit certain types of discrimination, and these consumer protection laws apply to AI usage in financial services. For example, the CFPB explained that fair lending and other consumer laws—including UDAAP prohibitions—are technology-neutral. They also stressed that these laws apply to more traditional financial products and services like lending and credit scores, as well as tools like fraud screening, which are increasingly driven by AI.

Respondents noted that financial firms must be aware of the potential for the AI models they use to produce biased results and offered a number of ways to minimize the corresponding risks. Some have contracted with third-parties to ensure fair lending compliance. One respondent suggested that firms should incorporate fair lending principles into AI model inputs to improve the model outputs. Others stated that AI models themselves could help comply with fair lending laws and provide credit to those that are "credit invisible" due to a lack of any credit history, by using alternative data, including information on cash flows and bill payments. However, one respondent cautioned that using non-financial alternative data when consumers are "credit invisible" may not be accurate or predictive of credit quality.

Other respondents focused on specific actions that regulators could take to address fair lending risks. To monitor for potential discriminatory or predatory practices, respondents recommended regulators collect data on financial product pricing. Some respondents said that regulators should prohibit the use of data produced by AI models that lack sufficient explainability where it would impact a consumer. Some respondents supported the use of a search for "less discriminatory alternatives" to any AI models used, especially when there is evidence of disparities on the basis of protected characteristics, to comply with fair lending laws but asked for clarity from regulators on what the less discriminatory model would look like and what corresponding metrics or standards firms should use to evaluate AI models. However, some respondents stated that it can be challenging for firms to test for bias because not all firms gather demographic data of prospective borrowers.

Additionally, some respondents highlighted potential gaps in fair lending laws independent of AI. Some pointed to the differences in supervision for banks and nonbanks and argued that the effect of this is uneven enforcement of fair lending laws. Others

encouraged regulators to extend the anti-discrimination principles of the fair lending laws to products and services that are not currently covered to ensure fair access for all financial services such as bank accounts. Another respondent stressed these same issues for deposit accounts, which may not be covered by the protections of fair lending laws, and argued that over-reliance on AI models can amplify these challenges. Specifically, this respondent said that the use of imprecise AI models to detect suspicious activity has led to an increase in improperly closed bank accounts, and that banks do not have processes to appeal the decision or require timely return of frozen funds. Similarly, this respondent noted that the lack of a requirement for an adverse action notice related to deposit account decisions makes it difficult to determine whether discriminatory AI tools are used.[43]

4. Concentration-related Risks

Respondents highlighted the concentration risk of AI model development – in particular more advanced AI models like Generative AI – by only a few firms and the resulting impact on market competitiveness for both providers and users of AI. Additionally, some respondents noted the potential impact of AI on financial stability, both domestically and internationally.[44] This section provides a summary of feedback related to these risks.

With respect to concentration risk, some respondents noted that AI may create a competitive advantage for larger institutions over small institutions within the areas of both customer-facing financial services, investor-facing trading, and capital market functions. Respondents described that Generative AI models typically require a vast amount of training data, advanced computing power, and substantial financial investment, which increase smaller institutions' dependency on those of a few large companies. Respondents noted that specifically for Generative AI models, numerous applications could be based on only a handful of foundational models that are developed by a few AI providers. Respondents worried that this concentration risk could also lead to systemic and market vulnerabilities, as interruption at a single AI provider could create widespread disruptions across the financial system.[45] Respondents also noted that the possibility of systemic risk, or AI driven bank runs or instabilities, may be more amplified in the future. Additionally, respondents noted that interconnections between models or data, combined with lack of transparency, could result in more herding behavior that is more unpredictable. Some respondents recommended that regulators require firms to use incremental rollouts to allow monitoring and risk assessment before full-scale

---

[43] Note that, in some instances, FCRA may require an adverse action notice after a decision related to a deposit account. *See, e.g., CFPB Takes Action Against JPMorgan Chase for Failures Related to Checking Account Screening Information*, https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-jpmorgan-chase-failures-related-checking-account-screening-information/

[44] FSOC 2023 Annual Report, *supra* note 4. *See also* FSOC, ANNUAL REPORT (2022), https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.

[45] *See* FINANCIAL STABILITY BOARD, THE AI ADVENTURE: HOW ARTIFICIAL INTELLIGENCE MAY SHAPE THE ECONOMY AND THE FINANCIAL SYSTEM (Jul. 11, 2024), https://www.fsb.org/2024/07/the-ai-adventure-how-artificial-intelligence-may-shape-the-economy-and-the-financial-system/.

implementation or use circuit breakers to implement mechanism to limit the impact of AI systems that exhibit harmful or unintended behaviors, in order to mitigate risks on a macro level and minimize the potential for widespread disruption in financial systems.

To address these risks, respondents suggested a number of solutions, including enhanced existing operational risk management frameworks, increased use of and support for open-source AI tools, and monitoring the concentration of AI providers.

5. Third-Party Risks

As noted above, the high cost and technical expertise required for developing AI tools means that financial firms will need to rely on AI models and systems developed by others, perhaps with some tailoring to adapt the systems to the needs of an individual firm. Because of the reliance on externally developed AI tools, respondents emphasized the need for financial firms to rely on their third-party risk management (TPRM) processes and conduct robust due diligence. Though TPRM processes are already critical components of risk management for financial firms,[46] respondents noted that AI-related third-party risk are similar to those of other emerging technologies, including operational, reputational, legal, regulatory, compliance, and data risks, such as privacy breaches, unauthorized data sharing, data processing issues, and inconsistent incident response speeds. Responses to the AI RFI make clear that TPRM is of critical importance as AI systems continue to develop.

In some cases, regulators have provided guidance on appropriate third-party due diligence. Though specific to third-party relationships of banking organizations only, respondents generally agreed that the Interagency Guidance on Third Party Relationships: Risk Management[47] addressed many risks of third-party AI models and systems, though some respondents recommended updates or clarifications to address specific AI-related concerns such as concentration risks, supply chain risks, and the appropriate use of third-parties to assist banks with due diligence and monitoring responsibilities. Another respondent noted that existing laws already require insurers to impose privacy and data security requirements on third-party vendors, including those whose AI tools they might use. In addition to the existing regulatory guidance, respondents highlighted a variety of other TPRM techniques financial firms could consider. Suggestions included: enhanced governance frameworks for sensitive applications, ongoing risk assessments, information security controls, business continuity testing, strengthened cybersecurity tools, and data quality frameworks.

Other respondents questioned whether financial firms – particularly smaller ones – can reasonably manage third-party risks themselves given the increasing market power of

[46] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Interagency Guidance on Third-Party Relationships: Risk Management 88 Fed. Reg. 37920 (Jun. 9, 2023).

[47] *Id*.

a limited number of AI tool providers. For example, respondents pointed out that firms may not have the bargaining power to adjust their contract with the vendor to mandate the vendor's adherence with the financial firm's required standards. As a solution, some respondents urged exploration of existing statutory authorities like the federal banking agencies' authority to regulate and examine certain third-party service providers under the Bank Service Company Act (BSCA).

Though TPRM is not new to financial firms, respondents said that many firms may face significant challenges to establishing sufficient AI expertise within the organization. This can hamper the ability for institutions to understand the potential risks presented by a given AI tool and develop appropriate controls to mitigate identified risks. Respondents suggested that regulators could address this issue by working to develop standards for the testing and review of AI models before deployment. One respondent suggested the Federal Financial Institutions Examination Council could develop a framework to help banks assess third-party AI models and systems. Another respondent encouraged Treasury's Financial Crimes Enforcement Network (FinCEN) to develop guidance regarding firms' use of AI tools to meet their AML/CFT obligations. Other respondents recommended the development of a model data set by which firms could train models for financial services. The respondent suggested, however, that vendor onboarding and ongoing monitoring questions be updated to specifically address AI risk. Some respondents noted state insurance regulators' efforts to develop a framework for the regulatory oversight of third-party data and predictive models. Respondents stressed that even with a clear TPRM process in place, firms may face hurdles when evaluating AI systems. For example, some said that it may be difficult to ensure data quality and validating results, as some data could be proprietary to the AI developer, which may be unwilling to provide such data. In the case of open-source AI models, validation of code could be challenging because the developer tested the code focused on one use case, while the user could be converting it for a different use case. Such challenges may become more pressing as the use of open-source AI models continues to be more widely adopted, which is highlighted by some respondents. As a potential solution, many respondents supported enhanced disclosures. Several respondents favored the idea of simple disclosures modeled after the nutritional label approach, which could help financial firms evaluate the risks particular AI tools may pose.[48] Other respondents recommended that third-parties should be required to disclose any time an AI tool is used. Doing so could improve a firm's ability to monitor the risks that may be posed by third-parties far down the financial firm's supply chain. Other respondents suggested regulators could develop a certification or accreditation program that would allow AI models and systems to become certified as compliant with applicable standards. This would allow potential customers to easily identify the products that are aligned with these standards. Another respondent disagreed, cautioning that a licensing requirement could exacerbate concentration risks.

[48] Treasury previously committed to exploring the feasibility of nutrition labels as well as similar disclosure mechanisms. *See* Treasury AI Cybersecurity Report, *supra* note 4, at Section 6.6.

Many respondents explained that firms may face significant financial and logistical challenges switching from one third-party AI tool to another in the future. Two respondents offered regulatory suggestions to help reduce the risk of this so-called "vendor lock-in" problem: requiring third-party AI providers to facilitate easy transitions between competing AI systems or developing a supply chain risk management framework that includes "Know Your Customer"-like requirements for suppliers.

6. Illicit Finance Risks

Multiple respondents noted the growing use of AI tools by adversaries to enable illicit cyber activity and fraud. These threats include criminals thwarting customer identification programs through document and image manipulation or creation (e.g., "deepfake" images), the use of AI tools to create convincing text for communications and interactions with financial firms, and social engineering customer service agents to gain illicit access to legitimate customer accounts or scam customers themselves.[49] Respondents emphasized that AI tools – and particularly Generative AI tools – could "supercharge" phishing attacks by simplifying the creation of compelling phishing campaigns directed toward financial firms at scale. Several respondents noted the ability for Generative AI tools to generate malicious content for cybercriminals, including websites and malware.

In response to these enhanced threats, respondents identified the role of robust digital identity (digital ID) solutions to address the risks posed by AI-enabled tools intended to thwart identity verification and authentication systems, such as identity document validation, liveness checks, and biometric matching. Respondents noted that improvements in digital IDs, such as the emergence of passkeys tied to biometrics such as a facial scan or fingerprint (which enable passwordless logins) on mobile devices using the Fast Identity Online (FIDO) authentication standard, and multi-factor authentication (MFA) tools with risk engines that use data to determine the provenance of the user of those MFA tools, could help address fraud risks.[50]

[49] *See* FinCEN Alert FIN-2024-Alert004, FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions (Nov. 13, 2024), https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

[50] FIDO is an authentication standard that uses public key cryptography techniques to provide phishing-resistant authentication, where a user's device retains private keys associated with biometrics authenticated on the device, and registers a public key with an online service (such as a financial firm). These private-public key pairs are unique to each online service, and are bound to the user's device.

V. Policy Considerations

Through analysis of feedback received from the AI RFI, Treasury identified the following broad policy areas for further consideration: (1) regulatory frameworks; (2) federal, state, and other legislative efforts; and (3) international standards. This section discusses each of these policy considerations in further detail.

1. Regulatory Frameworks

While many financial firms operating in the financial services sector are subject to laws and regulations that are technology-agnostic and can apply to AI technologies, respondents noted different regulatory standards among financial firms for the same activities. Respondents advocated for Treasury to prioritize intergovernmental coordination to provide cohesive regulatory guidance as appropriate, facilitate information sharing, and aligning governance approaches for the same activities. Respondents also broadly agreed on the benefit of public-private partnerships to share trends, risks, and best practices.

There are a number of existing and proposed frameworks related to uses of AI in financial services. Within the United States, the regulatory landscape for governing AI uses in financial services is shaped by various government agencies offering guidelines and risk management frameworks for financial firms, including state governments, the Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), FinCEN, Office of the Comptroller of the Currency (OCC), National Credit Union Administration (NCUA), Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), CFPB, and the NIST.[51] While some risk frameworks or standards are voluntarily adopted by financial firms as a guide in managing risks associated with broad AI uses, some financial firms adopt these frameworks to meet regulatory expectations for model risk management principles tailored to particular institutions on their use of models. For instance, financial regulators have issued supervisory guidance that addresses model risk management and broadly covers the development, validation, and governance and controls related to models.[52] The federal banking regulators also issued TPRM guidance covering the life cycle of relationships with third-party providers, including third-party providers that help develop models for financial firms.[53] The SEC has focused on rulemaking regarding conflicts of interest associated with the use of predictive data analytics, and enforcement regarding activity

[51] For the business of insurance, the primary regulators are the 50 states, the District of Columbia, and the five U.S. territories.

[52] *See* FDIC, FRB, OCC, *supra* note 32; *See also* Federal Housing Finance Agency Advisory Bulletin 2022-02, Artificial Intelligence / Machine Learning Risk Management (Feb. 10, 2022), https://www.fhfa.gov/sites/default/files/2023-12/Advisory-Bulletin-2022-02.pdf.

[53] *See* FDIC, FRB, OCC, *supra* note 46.

involving potential violations of the federal securities laws.[54] In December 2024, CFTC issued an advisory on the use of AI in CFTC-regulated markets, reminding regulated entities of their obligations under the Commodity Exchange Act and the CFTC's regulations as these entities begin to implement AI.[55] The National Association of Insurance Commissioners (NAIC) adopted the Model Bulletin on the Use of Artificial Intelligence Systems by Insurers in December 2023, reminding state insurance regulators that decisions impacting consumers that are made or supported by advanced analytical and computational technologies, including AI, must comply with all applicable insurance laws and regulations.[56]

Nine federal agencies have released a joint statement noting that their existing legal authorities apply to the use of "emerging automated systems" – including those marketed as AI – that impact civil rights, fair competition, consumer protection, and equal opportunity.[57] The CFPB has established guidance and proposed standards to regulate the use of AI in lending and mortgage appraisals that may potentially violate consumer protection laws.[58]

In 2018, FinCEN joined the federal banking agencies in publishing a joint statement on innovative efforts to combat money laundering and terrorist financing, which acknowledged financial firms' experimentation with AI and described how regulators would approach pilot programs, including those involving AI, undertaken by banks.[59] Section 6209 of the Anti-Money Laundering Act of 2020 (AML Act) also requires FinCEN to issue regulations specifying standards for testing technology and related technology internal processes designed to facilitate effective compliance with the BSA by financial firms.[60] It further directs FinCEN to "focus particularly on using innovative approaches

---

54 SEC, Proposed Rule on 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. *See also* SEC's recent enforcement actions taken against companies' misleading statements to investors about use of AI, https://www.sec.gov/enforcement-litigation.

55 CFTC Staff Letter No. 24-17, Use of Artificial Intelligence in CFTC-Regulated Markets (Dec. 5, 2024), https://www.cftc.gov/PressRoom/PressReleases/9013-24.

56 NAIC, NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers (Dec. 2024), https://content.naic.org/sites/default/files/inline-files/2023-12-4%20Model%20Bulletin_Adopted_0.pdf.

57 CFPB, Department of Justice, Equal Employment Opportunity Commission, Federal Trade Commission, Department of Education, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, and Department of Labor, Joint Statement on Enforcement of Civil Rights, Fair Competition Consumer Protection, and Equal Opportunity Laws in Automated Systems (Apr. 4, 2024), https://www.dol.gov/sites/dolgov/files/OFCCP/pdf/Joint-Statement-on-AI.pdf?utm_medium=email&utm_source=govdelivery.

58 For example, in September 2023, the CFPB issued guidance about certain legal requirements that lenders 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. *See* 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 (Sep. 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/. *See also* CFPB, *supra* note 40.

59 FinCEN, FRB, FDIC, NCUA, OCC, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf.

60 The AML Act was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021). Section 6209 is considered the "testing methods" section.

such as machine learning."[61] In 2024, Treasury published the National Strategy for Combatting Terrorist and Other Illicit Financing, which noted that AI, including machine learning and LLMs such as Generative AI, has significant potential to strengthen AML/CFT compliance by helping financial firms analyze massive amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies.[62]

Treasury will consider potential next steps, as outlined in Section VI below, to enhance interagency coordination, address regulatory gaps identified by respondents, and improve information sharing between government agencies and the financial services sector.

2. Federal, State and Other Legislative Efforts

Respondents broadly agreed that conflicting state laws may lead to uneven requirements on AI developers, users, and financial firms of different sizes, as well as varied product functionalities for consumers. Many respondents pointed out the potential for regulatory arbitrage and were supportive of a federal legal framework that worked together with state legislation.

There is currently no comprehensive framework of federal AI laws. Increasingly, though, state governments are exploring ways to regulate AI use within their states. In 2023, legislators in 31 states introduced at least 191 AI-related bills. While only 14 of those bills became law, state legislators are continuing to propose a wide array of laws related to the uses of AI within the states. Separately, some state agencies have attempted to regulate AI deployment within specific sectors. For example, in California, the Governor's office issued an Executive Order directing the "study of development, use, and risks of AI," focused on developing a process for evaluating and deploying AI within California's public sector.[63] California is also working on establishing AI rules based on the California Privacy Rights Act. The Colorado Division of Insurance promulgated a regulation establishing governance and risk management requirements for life insurers that use external consumer data and information sources (ECDIS), which builds upon Colorado's 2021 law on predictive models in insurance ratings.[64] Additionally, the New York State Department of Financial Services (NYDFS) has issued guidance on the use of AI by insurers.[65] NYDFS' guidance contains information "for developing and managing the

---

61 *Id.*

62 Treasury, *supra* note 20.

63 California Executive Order N-12-23 (Sep. 6, 2023), https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12-_-GGN-Signed.pdf.

64 Colorado Division of Insurance Regulation 10-1-1, Governance and Risk Management Framework Requirements for Life Insurers' Use of External Consumer Data and Information Sources, Algorithms, and Predictive Models , https://doi.colorado.gov/announcements/notice-of-adoption-new-regulation-10-1-1-governance-and-risk-management-framework.

65 NYDFS Insurance Circular Letter No. 7, Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing, (Jul. 11, 2024), https://www.dfs.ny.gov/industry-guidance/circular-letters/cl2024-07.

integration of ECDIS, AI systems, and other predictive models to mitigate potential consumer harm."[66]

Treasury will consider potential next steps, as outlined in Section VI below, to evaluate regulatory frameworks for AI use in financial services, aiming to promote responsible AI innovation while mitigating the risks of regulatory arbitrage.

3. International Standards

Respondents highlighted that AI-related regulatory frameworks are being established in foreign jurisdictions with potential impacts on U.S. companies' current and future use of AI. Respondents noted that regulatory fragmentation may lead companies to tailor their AI governance practices, product development, third-party due diligence, and risk management separately for each jurisdiction in which they operate, presenting challenges for financial institutions to manage risks consistently on an enterprise-wide basis. Additionally, respondents pointed out that divergent approaches can also lead to dramatically different levels of consumer protection and access to AI-powered services from one jurisdiction to the next.

Treasury will consider potential next steps, as outlined in Section VI below, to continue international collaboration and engagement to facilitate interoperability efforts and harmonize standards, as appropriate.

[66] *Id.*

VI. Potential Next Steps

This section describes the potential next steps to be considered by Treasury, government agencies, and the financial services sector, based on feedback received from the AI RFI.

1. **Treasury recommends continuing international and domestic collaboration among governments, regulators, and the financial services sector to promote consistent and robust standards for uses of AI in the financial services sector.**

   Treasury recognizes the importance of international standards and recommends continued participation in international coordination efforts for AI governance at relevant international forums (such as the G7, FSB, OECD, and financial standard-setting bodies) to promote consistency across jurisdictions, which respondents identified as a concern. A recent example of Treasury's collaboration effort is its participation in ongoing discussions about AI at the G7 and its contributions to recent reports from the Financial Stability Board and the OECD.[67] Continued bilateral engagement on AI issues with various jurisdictions can also facilitate interoperability efforts and harmonize standards, as appropriate.

   Domestically, Treasury recommends continued collaboration between U.S. government agencies and the financial services sector. Respondents were largely supportive of the process that produced the NIST AI RFI and encouraged similar collaboration in the future. Building on this work, Treasury recommends further coordination with NIST and suggests using input from respondents on this AI RFI, among others, to inform this work. Treasury also recognizes the substantial efforts of financial regulators to understand the risks and benefits of AI for the entities that they regulate and to develop materials articulating their expectations and, in some cases, requirements for these institutions. Lastly, Treasury recommends continuing to coordinate with the financial sector, financial regulators, and government agencies to develop disclosure mechanisms, such as the nutritional label approach from the Treasury AI Cybersecurity Report and supported by AI RFI respondents, to help financial firms assess AI risks.

2. **Treasury recommends further analysis and stakeholder engagement to explore solutions for any identified gaps in the existing regulatory frameworks, and to address the potential risk of AI causing consumer harms, as identified by the respondents.**

---

[67] Financial Stability Board, *supra* note 4; OECD, Regulatory Approaches to Artificial Intelligence in Finance (Sep. 2024), https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html.

Existing laws and regulations already apply to many AI-related activities, but feedback from respondents suggested there are gaps or room for further clarifications that merit further exploration. Treasury recommends further analysis and continuing stakeholder engagement to explore potential gaps. In particular, Treasury recommends government agencies, regulators and financial firms evaluate respondents' concerns about how different levels of supervision for banks and nonbanks may impact AI usage in financial services and considering ways to ensure that firms are subject to consistent standards for AI usage. Treasury also suggests government agencies exploring respondents' concerns about whether existing consumer protection laws like FCRA, ECOA, and GLBA are sufficient to provide consumers with the ability to understand how their data is used, control who uses it, and correct errors, given the expanding usage of consumer data in AI models and systems. Additionally, regulators could clarify expectations on how to assess AI models and systems for discriminatory effects, including the assessment of potentially less discriminatory alternatives. After further analysis of gaps in existing frameworks, Treasury recommends regulators and stakeholders consider clarifying or supplementing standards for data privacy, security, and quality across financial services. Finally, Treasury reaffirms FSOC's recommendation, in its 2024 Annual Report, that Congress pass legislation that ensures that relevant agencies have adequate examination and enforcement powers to oversee third-party service providers that interact with their regulated entities.[68]

3. **Treasury recommends financial regulators continue coordinating to identify potential enhancements to existing risk management frameworks and working with other government agencies to clarify supervisory expectations on the application of frameworks and standards, where appropriate.**

   Treasury supports regulators' work in this area and their commitment to continue monitoring developments in AI technologies. Treasury recommends continued coordination among financial regulators to support their efforts in enhancing existing risk management frameworks.

   Treasury encourages financial regulators, where appropriate, to clarify their expectations for how the firms they supervise should apply the various frameworks and standards. For example, regulators could update existing guidance to clarify how the NIST AI RMF fits within prudential risk-management expectations.

4. **Treasury recommends the financial services sector and government agencies consider further facilitate financial services-specific AI information sharing, alongside the AI cybersecurity forum recommended in the Treasury AI Cybersecurity Report, to develop data standards, share risk management best**

[68] *See* FSOC 2023 Annual Report, *supra* note 6.

practices, and enhance understanding on the use of emerging AI technologies in financial services.

Treasury recommends continued engagement with stakeholders including participants from the financial services sector and government agencies to facilitate information sharing. A recent example of a Treasury-led public-private partnership is the "Cloud Executive Steering Group" launched in May 2023,[69] which aims to help financial firms on their secure cloud adoption. The steering group was established to help close the gaps identified in Treasury's report on the adoption of cloud services in the financial service sector.[70] The Treasury AI Cybersecurity Report recommended the establishment of a similar group dedicated to resolving the AI-specific cybersecurity threats detailed in that report. Treasury recommends further developing public-private partnerships to better enable information sharing. These partnerships will facilitate developing data standards development, sharing risk management best practices, and enhancing understanding on emerging AI technologies.

With respect to promoting market competition and addressing resource gaps between large and small institutions, as suggested in the Treasury AI Cybersecurity Report, Treasury recommends government agencies continue to explore ways of working with stakeholders to develop technology capabilities, including abilities to develop and deploy AI, for smaller financial firms. Treasury also recommends government agencies and the financial services sector consider monitoring concentration risks associated with AI providers.

5. **Treasury recommends that financial firms prioritize their review of AI use cases for compliance with existing laws and regulations before deployment and that they periodically reevaluate compliance as needed.**

Financial firms have a legal obligation to ensure their AI usage complies with existing laws and regulations. As respondents noted, many existing laws and regulations apply regardless of the technology used by the firm. Treasury recommends firms review their usage of AI models and systems to ensure compliance with the applicable laws and regulations and, if deficiencies are observed, Treasury recommends firms take immediate action to bring themselves into compliance. These actions may include updating policies and procedures, updating AI models, or switching to alternative AI providers. Additionally, as firms consider expanding AI use cases, firms should conduct similar due diligence to ensure their continued compliance with the applicable laws and regulations.

---

[69] Treasury, *Press Release: Treasury and the Financial Services Sector Coordinating Council Publish New Resources on Effective Practices for Secure Cloud Adoption* (Jul. 17, 2024), https://home.treasury.gov/news/press-releases/jy2467.

[70] Treasury, Financial Services Sector's Adoption of Cloud Services (Feb. 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

VII. Appendix: Abbreviations

AI	Artificial Intelligence
AI EO	Artificial Intelligence Executive Order
AI RMF	AI Risk Management Framework
AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CFPB	Consumer Financial Protection Bureau
CFT	Combating of Terrorism Financing
CIP	Customer Identification Program
CFTC	Commodity Futures Trading Commission
ECDIS	External Consumer Data and Information Sources
ECOA	Equal Credit Opportunity Act
EEOC	Equal Employment Opportunity Commission
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	US Federal Financial Institutions Examination Council
FHA	Fair Housing Act
FHFA	Federal Housing Finance Agency
FinCEN	Financial Crimes Enforcement Network
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
FTC	Federal Trade Commission
Generative AI	Generative Artificial Intelligence
GLBA	Gramm-Leach-Bliley Act
LLM	Large Language Model
ML	Machine Learning
NAIC	National Association of Insurance Commissioners
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NYDFS	New York State Department of Financial Services
OECD	Organization for Economic Co-operation and Development
OCC	Office of the Comptroller of the Currency
OMB	Office of Management and Budget
SEC	Securities and Exchange Commission
TPRM	Third-Party Risk Management
UDAAP	Unfair or Deceptive Acts or Practices


THE DEPARTMENT OF THE TREASURY
1789