Treasury's Post-2024 RFI Report on AI in Financial Services – Uses, Opportunities, and Risks

January 24, 2025

On December 19, 2024, the U.S. Department of Treasury ("Treasury") released a report on The Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector (the "Report"). The Report summarizes key themes from comments from a variety of industry stakeholders ("respondents") in response to Treasury's June 2024 Request for Information ("RFI"), and recommends several next steps for financial regulators, financial services firms, and government agencies more broadly for coordination purposes. Treasury received over 100 responses to its RFI, which focused on the adoption of artificial intelligence ("AI"), associated risks, and potential policy considerations.

The Report builds upon prior Treasury reports on AI, including a discussion of opportunities and risks relating to the use of AI by fintech and other non-bank financial firms in its November 2022 report on Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets and its March 2024 report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector ("March 2024 Report"). We previously discussed Treasury's March 2024 Report, both in terms of AI risk management and governance (Part 1) and managing AI-specific cybersecurity risks (Part 2). In contrast to the Treasury's March 2024 Report, this Report focuses on respondents' feedback pertaining to existing and new use cases for AI in the sector, and the associated *non*-cybersecurity related risks.

This Report, alongside Treasury's March 2024 Report, offers a foundation for financial sector firms and government agencies to collaborate on addressing AI data standards and challenges, while reinforcing financial firms' obligation to comply with existing regulations.

With the change in administration, it is unclear which of the issues identified in the Report will remain a priority for Treasury. However, we anticipate that avoiding a patchwork of overlapping but inconsistent AI regulation, harmonizing definitions, enhancing consumer protection, and increasing public-private information sharing on the benefits and risks of AI for the financial sector will likely remain areas of focus for

the Trump Administration, and therefore, at least those sections of the Report will remain relevant.

Current Uses and Opportunities of AI in Financial Services

The Report highlights the widespread use of AI technologies in the financial services sector, ranging from traditional AI (*e.g.*, statistical models using structured datasets) to emerging AI technologies (*e.g.*, generative AI). The Report distinguishes between these different AI technologies, highlighting that existing regulations directly address traditional AI risks but are just beginning to address some of the unique risks of emerging AI technologies.

Traditional AI vs. Generative AI Governance

Respondents noted that while the governance requirements for traditional AI that has long powered functions like credit underwriting are well understood, generative AI is a transformative technology raising new governance considerations. Unlike traditional AI, generative AI creates new content from its learnings based on training data and requires extensive resources, expertise, and oversight to address risks like hallucinations and third-party reliance. Respondents provided that these more resource-intensive governance obligations could limit smaller firms' adoption of such emerging technologies and increase concentration risks due to reliance on a few dominant third-party AI providers (*e.g.*, foundational model providers).

External and Internal Uses of AI

The Report underscores comments that highlight respondents' views on AI's external uses, such as personalized recommendations by payment providers, robo-advisors offering tailored advice, and AI-driven technologies for trading, insurance underwriting, and fraud detection. Respondents also noted that emerging AI technologies can be used to expand credit access to underserved populations by analyzing alternative data like utility bills and rental payments.

For internal uses, respondents emphasized the growing role of AI in compliance, risk management, and operations, with generative AI in particular enhancing tasks like report creation, data analysis, and detecting anomalies in anti-money laundering and sanctions compliance.

Potential Risks of AI and Suggestions for Risk Mitigation

The Report summarizes responses on six categories of key risks associated with AI and suggestions for mitigating each risk.

- **Data Privacy, Security, and Quality Standards.** Respondents highlighted that high-quality data is critical to AI's success and flagged that risks like data poisoning, breaches, and inconsistent privacy protections remain key challenges. Specifically, respondents noted that data poisoning attacks, which corrupt AI training datasets, could impair a model's performance or produce undesired outcomes. We previously discussed cyber risks associated with AI in response to Treasury's March 2024 Report as well as guidance from NYDFS on managing cybersecurity risks arising from AI.

  Suggested mitigations: Respondents proposed addressing data-related risks by adopting AI governance frameworks and leveraging technical solutions like homomorphic encryption and federated learning to enhance privacy. One respondent highlighted using AI models themselves to detect privacy policy violations, while others called for regulatory clarity on the use of AI and intellectual property laws, and for laws regulating data sharing.

- **Bias, Explainability, and Hallucinations.** The Report highlights respondents' concerns regarding: (1) AI model reinforcement of biases embedded in historical data and potentially discriminatory outcomes; (2) lack of explainability in AI outputs and decisions, which undermines trust and creates reputational risks; and (3) unique risks associated with generative AI, such as hallucination, where outputs are "confidently stated but incorrect." Respondents also raised concerns that third-party vendors withholding critical information makes it difficult for firms to assess and mitigate these risks effectively.

  Suggested mitigations: Respondents suggested that AI could reduce bias by using alternative variables, like rent and utility payments, to decrease reliance on credit scores, though improperly trained models could still amplify biases. One respondent proposed using retrieval augmented generation to ground outputs in verifiable data to improve explainability. While some respondents supported mandatory disclosures for transparency, others warned that could heighten cybersecurity risks.

- **Impact on Consumers and Consumer Protections.** The Report highlights respondents' concerns about the impact of AI on consumers, particularly regarding consumer-facing AI models, consumer data rights, and the application of existing consumer protection laws. Specifically, respondents noted that consumer-facing AI systems can exacerbate biases, mislead consumers, or misuse data without consent,

creating risks such as false positives (*e.g.*, wrongly granting credit) and false negatives (*e.g.*, improperly closing accounts due to imprecise suspicious activity detection). These risks raise significant concerns about fairness, privacy, and accountability in AI-driven consumer interactions. We have previously discussed AI and consumer-related issues in our three-part webinar (Part 1, Part 2, and Part 3) on Artificial Intelligence and Discrimination in the Insurance Industry.

Suggested mitigations: There were opposing views on mitigations for consumer-related risks. While some respondents supported mandatory disclosures to improve transparency and accountability, others warned that such measures could stifle innovation and heighten cybersecurity risks. Additional suggestions included pre-launch testing for AI models, regulatory pre-approval, and leveraging existing consumer protection laws like the Fair Credit Reporting Act ("FCRA") to address consumer risks.

- **Concentration-related Risks.** The Report highlights responses concerned with the concentration of advanced AI model development among a few large firms. Respondents noted systemic risks, such as a cyberattack that may cause industry-wide impacts, and the potential for unfair competitive advantage to exacerbate the risk of systemic and market vulnerabilities.

  Suggested mitigations: Some respondents suggested open-source AI tools and monitoring the concentration of AI providers. To avoid macro-level risks, some respondents suggested that firms developing AI models use incremental rollouts before full-scale implementation to minimize the potential for widespread disruption.

- **Third-Party Risks.** Respondents identified several risks stemming from financial firms' reliance on third-party AI providers. These include exposure to data breaches, unauthorized data sharing, and data processing issues. Additional risks highlighted by respondents involve inconsistent incident response times, operational disruptions, and lack of transparency into how AI models function, which complicates firms' ability to assess and manage risks effectively.

  Suggested mitigations: Respondents offered several potential mitigants, including strong third-party risk management ("TPRM") frameworks and robust due diligence processes, a topic we have previously discussed. Some respondents suggested updating interagency guidance to tackle generative AI-specific risks like concentration and leveraging "nutritional labels" to improve transparency on how AI models are trained and how data is processed. Other suggestions included stricter data security requirements for vendors and more robust disclosures to help firms validate open-source AI models more effectively.

- **Illicit Finance Risks.** The Report highlights respondents' concerns about adversaries exploiting AI tools to commit fraud, phishing, and identity manipulation, such as creating deepfakes, as we have previously discussed. In the financial services context, these concerns primarily relate to fraudsters gaining illicit access to legitimate customer accounts or using AI-generated media to deceive customer service agents and scam consumers.

  Suggested mitigations: Respondents recommended strengthening digital identity solutions, such as biometrics-based multi-factor authentication, to address these risks.

Policy Considerations

The Report consolidates respondents' comments on regulatory efforts into three categories: (1) regulatory frameworks; (2) federal, state, and other legislative efforts; and (3) international standards. Financial firms should monitor these areas as they will likely shape the future development and implications of regulatory obligations on AI in the financial services sector.

- **Federal-State Overlap.** The Report describes a fragmented regulatory landscape with overlapping federal and state efforts to establish guidelines via both guidance and prescriptive requirements. Regulatory pronouncements, both existing and proposed, touch on the use of AI and risk management frameworks, TPRM, conflicts of interest, consumer protection laws, and insurance-specific laws. Respondents emphasized the need for enhanced interagency collaboration to cohesively address emerging AI risks.

- **Inconsistent State Laws.** The Report also underscores the challenges posed by the emerging patchwork of conflicting state laws regulating AI use in financial services, which respondents noted could hinder responsible AI adoption and create risks of regulatory arbitrage. This patchwork issue resembles the challenges in U.S. privacy law, which we've previously discussed. Certain state regulatory initiatives have been sector-specific, such as regulations for insurers' use of AI in California, Colorado, and New York. We also recently discussed a draft amendment that proposes extending Colorado's life insurer requirements to auto insurers and health insurers.

- **International Standards.** Respondents highlighted the development of AI regulatory frameworks in foreign jurisdictions, with potential challenges for financial firms attempting to operate and comply with fragmented requirements across international jurisdictions, while also maintaining a firmwide risk management framework.

Potential Next Steps Identified by Treasury

The Report identifies potential next steps for firms within the financial services sector, for Treasury, and for other government agencies.

Financial Firms

- **Prioritize Review of AI Use Cases for Compliance with Existing Laws/Regulations Before Deployment.** The Report emphasizes that financial firms should review AI use cases for compliance with laws like fair lending and data privacy before deployment and periodically reevaluate compliance. Treasury advises firms to consider updates to their policies and procedures and their AI models.

Treasury and Government Agencies

- Continued International and Domestic Collaboration. The Report calls for collaboration through forums like the G7, engagement with stakeholders, alignment with NIST's AI Risk Management Framework ("RMF"), and coordination with the financial sector to develop disclosure mechanisms such as "nutritional labels" to improve transparency and consistency in AI standards.

- **Explore Solutions for Gaps in Existing Regulatory Frameworks.** The Report calls for government agencies to assess whether existing consumer protection laws, like the FCRA and the Gramm-Leach-Bliley Act, sufficiently address AI-related risks, and clarify expectations for evaluating models, identifying less discriminatory alternatives, and addressing uneven supervision between banks and nonbanks. The Report also recommends that agencies, regulators, and financial firms work together to assess how different levels of supervision for banks and nonbanks may affect how financial firms use AI.

- **Identify Enhancements to Existing Risk Management Frameworks.** The Report recommends that financial regulators continue to coordinate to enhance risk management frameworks and clarify supervisory expectations for their application. Treasury suggests regulators consider how existing frameworks, such as NIST's AI RMF, align with prudential risk management standards.

- **Facilitate Financial Services-specific AI Information Sharing.** Treasury suggests continued collaboration between government agencies and financial firms to facilitate information sharing. Treasury believes that such information sharing can help develop data standards, improve risk management practices, and support smaller firms, while monitoring concentration risks among AI providers. As an example of such information sharing, the Report cites the Treasury-led Cloud Executive Steering Group launched in May 2023.

Key Takeaways

The Report provides a comprehensive overview of the opportunities and risks associated with the use of AI in financial services, emphasizing the importance of proactive risk management and regulatory compliance. While it largely reinforces existing discussions on AI-related challenges, it offers valuable insights and practical recommendations for financial institutions. Based on the Report, firms may want to consider the following measures:

- Assessing Regulatory Compliance. Firms should consider requiring a regulatory compliance review for any higher-risk generative AI use cases that are moving into production, which may include a review for compliance with applicable laws relating to privacy, cybersecurity, bias, transparency, lending, and consumer protections.

- Establishing a Generative AI Risk Assessment Program and Inventory. Firms should consider implementing a generative AI governance program that (1) identifies low-risk AI uses cases that do not need a robust compliance review and do not need to be recorded in any AI inventory (*e.g.*, summarization and translation of public documents), (2) identifies prohibited use cases and ensures that there are no such use cases in production (*e.g.*, using a generative AI interview tool to decide whether to hire an employee based on its assessment of what their body language indicates about their trustworthiness), (3) identifies the risks associated with other generative AI use cases, along with the appropriate mitigation measures to address those risks, and (4) keeps track of higher-risk generative AI use cases in production to ensure that their risks, including regulatory compliance risks, remain sufficiently mitigated.

- Follow AI Regulatory Developments. Firms should closely monitor ongoing regulatory developments on AI. This Report, alongside Treasury's March 2024 Report, highlights several areas where future guidance, standards and laws are likely to emerge in the next 12 months that will significantly impact which generative AI use cases for financial institutions are permitted, which require significant compliance measures, and which are prohibited.

* * *

Please do not hesitate to contact us with any questions.

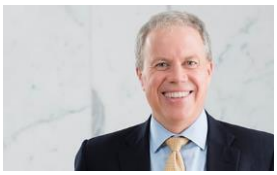
To subscribe to the Data Blog, please click here.

The cover art used in this blog post was generated by DALL-E.

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com

Avi Gesser
Partner, New York
+212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com



Gregory J. Lyons
Partner, New York
+1 212 909 6566
gjlyons@debevoise.com

Jeffrey L. Robins
Partner, New York
+ 212 909 6526
jlrobins@debevoise.com

Jeremy I. Liss
Associate, New York
+ 1 212 909 6687
jiliss@debevoise.com

Ned Terrace
Associate, New York
+1 212 909 7435
jkterrace@debevoise.com

Mengyi Xu
Associate, San Francisco
+415 738 5725
mxu@debevoise.com