1776 MAIN ST
SANTA MONICA, CA
90401-3208

TEL (310) 393-0411
FAX (310) 393-4818

August 12, 2024

To: Departmental Offices, Department of the Treasury

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

On June 12th, 2024, the Treasury Department issued a Notice requesting information on the uses, opportunities, and risks of Artificial Intelligence in the Financial Services Sector. In this letter, we provide a written comment in response to specific questions posed by the Treasury Department. Specifically, this comment is composed of two main sections: (1) we provide a broad summary including high level observations and possible remedies and (2) we provide detailed responses to specific questions posed in the request for information. Our responses are based on expert knowledge and synthesis of the business and academic literature. We provide the contact information for all authors of this comment at the end of this letter.

Comment Contents

RESEARCH AREAS
Children, Families, and Communities
Cyber and Data Sciences
Education and Literacy
Energy and Environment
Health, Health Care, and Aging
Homeland Security and Public Safety
Infrastructure and Transportation
International Affairs
Law and Business
National Security and Terrorism
Science and Technology
Social Equity
Workers and the Workplace

OFFICES
Santa Monica, CA
Washington, DC
Pittsburgh, PA
Boston, MA
Cambridge, UK
Brussels, BE
Rotterdam, NL
Canberra, AU

www.rand.org

Comment Summary

Artificial intelligence (AI) has been a transformative force in the financial industry, evolving from expert systems in the 1970s to sophisticated applications in various domains today, offering unprecedented opportunities for innovation and efficiency. This evolution has profoundly impacted financial services, including customer service, risk management, and investment strategies, propelled by significant technological advancements and the increasing availability of large datasets.[1] AI's integration into financial services is notable not only for its technological innovation but also for the fundamental changes it has brought to the industry's operational landscape. The historical trajectory of AI in finance highlights several pivotal milestones, from initial uses in algorithmic trading to more advanced technologies like High-Frequency Trading (HFT) and deep learning, which have revolutionized trading strategies and market operations.[2]

Over the past decade, AI's application has extended beyond trading to encompass financial management, credit risk analysis, and regulatory compliance, indicating its broad and versatile utility within the sector. This overview provides a concise examination of AI adoption in finance based on a comprehensive review of academic literature, industry reports, and other relevant sources, focusing specifically on AI applications within the financial sector rather than delving into broader topics such as the impact of AI on monetary policy or general use cases relevant across many industries. As AI continues to shape the financial services landscape, it presents both significant benefits and challenges, from enhancing operational efficiency and customer experience to raising concerns about algorithmic bias, data privacy, and the need for robust legal and ethical frameworks to ensure fair and transparent AI-driven decision-making processes.[3]

[1] Bonnie G. Buchanan, "Artificial Intelligence in Finance," The Alan Turing Institute, April 2019. As of July 26, 2024: https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_0.pdf.

[2] McGowan, Michael J., "The Rise of Computerized High Frequency Trading: Use and Controversy," *Duke Law & Technology Review*, 2010. As of 26 Jul 2024: https://scholarship.law.duke.edu/dltr/vol9/iss1/15/;

Buchanan, 2019;

Tierno, Paul, Artificial Intelligence and Machine Learning in Financial Services, Congressional Research Service, R47997, April 3, 2024, 2024. As of 26 Jul 2024: https://crsreports.congress.gov/product/pdf/R/R47997.

[3] See, for example Sytsma, Tobias, James V. Marrone, Anton Shenk, Gabriel Leonard, Lydia Grek, and Joshua Steier, *Technological and Economic Threats to the U.S. Financial System: An Initial Assessment of Growing Risks*, RAND, 2024. As of August 7, 2024: https://www.rand.org/pubs/research_reports/RRA2533-1-v2.html.;

Zhang, Bryan, Transforming Paradigms: A Global AI in Financial Services Survey, Cambridge Centre for Alternative Finance, January 2020. As of 26 July 2024:

High-level observations and possible remedies

In responding to the Treasury's request for information, we provide an assessment of the opportunities, risks, and policy implications, including an examination of potential gaps in the current regulatory framework. Our assessment is based on our expertise from prior research on topics related to technology, systemic risks, and financial services rather than new research. A key observation is the growing importance of nonbank entities in the AI ecosystem. These organizations, often operating outside the traditional financial services sector, play crucial roles in data collection, storage, model training, and deployment. Given their scale and interconnectedness, they pose risks to financial stability that warrant careful consideration.

Our perspective also highlights how AI may contribute to non-traditional sources of systemic risk in financial services. This includes the potential for AI to significantly alter the behavior of retail investors and the possibility of malicious actors exploiting AI technologies for nefarious purposes. These factors underscore the need for a nuanced and forward-looking approach to regulation and oversight.

Responses to Requests for Information

In this letter, we provide answers to questions posed in the request for information. Specifically, we provide responses to questions 2, 13, and 18. While we provide these detailed responses in the next section, below we provide a high-level summary of our answers.

Question 2

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

Answer Summary: AI's integration into capital markets has revolutionized operations, improving efficiency, accuracy, and risk management while offering innovative solutions for fraud detection, sentiment analysis, and regulatory compliance.[4] AI methodologies (e.g., machine learning and natural language processing) have significantly advanced trading and

https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf; Consumer Financial Protection Bureau, "CFPB Issue Spotlight Analyzes "Artificial Intelligence" Chatbots in Banking," 6 Jun 2023. As of 1 May 2024: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issue-spotlight-analyzes-artificial-intelligence-chatbots-in-banking/;

Leitner, Georg, Jaspal Singh, Anton van der Kraaij, and Balázs Zsámboki, "The rise of artificial intelligence: benefits and risks for financial stability," webpage, May 2024. As of 26 Jul 2024: publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html.

[4] OECD. "Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers." 2020: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/08/artificial-intelligence-machine-learning-and-big-data-in-finance_8d088cbb/98e761e7-en.pdf

investing. Below, Table 1 provides a high-level summary of AI use cases in capital markets, risk management, regulatory compliance, and customer services.[5]

Table 1. Use of AI models and tools

Application	Potential Use Cases
Capital Markets	AI presents a range of potential applications in capital markets. We discuss these in three categories: 1. **Trading and Investment**: Leveraging the ability to rapidly process and analyze vast quantities of data, AI has been used to optimize order routing, optimally allocate block trades, and analyze public sentiment to inform trading decisions.[6] 2. **Robo-advisors**: Platforms like Betterment currently use rule-based systems to analyze investor profiles and goals, but financial institutions aim to leverage generative models in the future to optimize investment strategies and enhance client experiences.[7] 3. **Financial forecasting and analytics:** AI has enabled more accurate forecasting and prediction in the financial sector. Firms employ machine learning (ML) applications to optimize liquidity and cash management, forecast startup performance, and monitor risk.[8]

[5] Given some overlap, we note that our responses to question 2 provides insight into questions 5, 8, and 12.

[6] Mayor, Tracy, "Why finance is deploying natural language processing," 3 Nov 2020,. As of 1 May 2024: https://mitsloan.mit.edu/ideas-made-to-matter/why-finance-deploying-natural-language-processing,

Financial Industry Regulatory Authority, AI Applications in the Securities Industry, June 2020. As of 1 May 2024: https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf;

Financial Industry Regulatory Authority, 2020: AI Applications in the Securities Industry. Available at: https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf (accessed 1 May 2024).

[7] JPMorgan Chase Bank, "IndexGPT," 11 May 2023. As of 1 May 2024: https://tsdr.uspto.gov/documentviewer?caseId=sn97931538&amp;amp;amp;docId=APP20230515101121#amp%3Bamp%3Bpage%5B%5D=1&amp%3Bamp%3Bpage%5B%5D=2&amp%3BdocIndex%5B%5D=1&amp%3BdocIndex%5B%5D=1&amp%3Bpage=2&docIndex=3&page=1;

Field, Hayden, "Why Betterment's robo-advisor doesn't use AI," 11 Oct 2022. As of 1 May 2024: https://www.emergingtechbrew.com/stories/2022/10/11/why-betterment-s-robo-advisor-doesn-t-use-ai.

[8] Basrai, Abbas, and Slim Ben Ali, "Artificial Intelligence in Risk Management." As of 1 May 2024: https://kpmg.com/ae/en/home/insights/2021/09/artificial-intelligence-in-risk-management.html,

Risk Management	AI tools leveraged for risk management across diverse applications within financial services, below we discuss the following three categories: 1. **Credit Risk Assessment**: AI supports holistically assessing customer creditworthiness from data, reducing time and costs associated with manual underwriting.[9] 2. **Fraud Detection, Anti-Money Laundering (AML)**: AI identifies anomalies in transaction data that may indicate fraud and other illicit activities, enabling mitigation of financial crimes.[10] 3. **Cybersecurity and Data Protection**: AI methods have augmented legacy, signature-based, threat detection approaches – enabling the detection of malicious activity without known signatures at improved quality and cost.[11]
Regulatory Compliance	AI enables financial institutions to automatically check compliance, provide alerts for potential breaches, and answer questions about regulations, policies, and guidelines.[12]

Wiggers, Kyle, "PitchBook's new tool uses AI to predict which startups will successfully exit," 20 March 2023. As of 1 May 2024: https://techcrunch.com/2023/03/20/pitchbooks-new-tool-uses-ai-to-predict-which-startups-will-successfully-exit/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJXLfE6mvgN-Xzwi6AGicvrQvKsqX5Et7taMBlStjt7W1KnuhoZfRKLebfjdC8xcwQM7CfLjbdpKgcCJ0FZCclomrD3ofGpQ5j5agCHn8AK7USXW0PuCcyo_05I9CHOjgLR6D9siTgCs4woWcazjiHppxZFps9jI9gCss_zBfaNz;

Boukherouaa, El Bachir, Khaled AlAjmi, Jose Deodoro, Aquiles Farias, and Rangachary Ravikumar, "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance," *Departmental Papers,* Vol. 2021, No. 024, 22 Oct. 2021, 2021, p. A001. https://www.elibrary.imf.org/view/journals/087/2021/024/article-A001-en.xml

[9] Lee, Julie, "AI-Driven Credit Risk Decisioning: What You Need to Know," 6 Mar 2024. As of 1 May 2024: https://www.experian.com/blogs/insights/ai-driven-credit-risk-decisioning/.

[10] U.S. Department of the Treasury, "Treasury Announces Enhanced Fraud Detection Process Using AI Recovers $375M in Fiscal Year 2023," 28 Feb 2024b. As of 1 May 2024: https://home.treasury.gov/news/press-releases/jy2134

[11] U.S. Department of the Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," March 2024a. As of 1 May 2024: https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

[12] Agarwal, Rahul, Andreas Kremer, Ida Kristensen, and Angela Luget, "How generative AI can help banks manage risk and compliance," 1 March 2024. As of 1 May 2024: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance.

Customer services	AI is being used to modernize online platforms and core support functions, gain customer insights, chatbots, automate typical employee processes, automate tasks, streamline workflows, and help agents be more productive.

Question 13

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

Answer Summary: The use of AI in combating illicit finance presents both opportunities and challenges. While there are examples of how AI can help detect and prevent fraud, money laundering, and other illicit activities, we also note, closely related to the question asked, that AI could also equip bad actors with advanced tools. For example, AI could help automate sophisticated money laundering techniques, create convincing fake documents that bypass identity verification measures, and facilitate the sale of illicit goods and services. Existing regulatory frameworks and privacy-protected data sharing mechanisms will need to evolve to address AI-driven illicit activities. Gaps in expertise and technical capacity could hinder law enforcement and regulatory adaptation.

To combat AI-driven illicit finance, policymakers should fund research on emerging illicit finance typologies enabled by AI, modernize regulatory frameworks, facilitate data sharing, support digital identity solutions, enhance technical expertise and capacity, and close existing regulatory gaps.

Question 18

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

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

Answer Summary: Nonbank firms (including Big Tech, FinTech, and retail firms) are emerging as significant players in AI-driven financial innovation, offering a range of services and products to consumers, merchants, and financial institutions. Examples include using AI in embedded finance, tailored investment strategies, peer-to-peer lending, identity verification, fraud prevention, and customer service. Nonbanks' integration of AI into financial services introduces unique and potentially significant risks that are difficult to quantify. Risks related to interconnectedness, single points of failure, and larger cyberattack surfaces could impact the stability of the financial system. This is particularly the case with nonbank entities that face less regulatory scrutiny than insured depository institutions. Key regulatory gaps include differential supervisory obligations between banks and nonbanks, governance of partnerships and outsourcing, and the need for clear regulatory jurisdiction to prevent arbitrage and ensure effective oversight.

To address risks posed by nonbank firms using AI in financial services, policymakers should closely monitor their systemic importance, mature standards for secure data sharing, explore AI model transparency measures, clearly allocate oversight responsibilities for partnerships and outsourcing, and clarify regulatory jurisdictions and formal mechanisms for interagency coordination.

While foreign investment in U.S. AI efforts can support innovation and economic growth, it can also pose risks to national security, particularly if adversarial entities exploit investment to access sensitive technologies and data. The Committee on Foreign Investment in the United States (CFIUS) is tasked with reviewing such transactions, but the rapid pace and volume of AI investments--along with other demands on CFIUS--may strain its review capacity. Additionally, differences in screening regimes among U.S. allies and partners could provide adversaries with indirect access to U.S. AI technology.

To address these risks, we recommend that CFIUS be fully authorized and resourced to prevent and mitigate national security threats arising from foreign investment in U.S. AI efforts, and that the U.S. government deepen its work with allies and partners to ensure the safety of global investments in AI.

Possible Remedies and Recommendations

Our comments in response to the questions listed above focus on challenges related to financial stability, security, and systemic risk. In particular, our comments highlight how the use of AI in financial services aggravates the systemic importance of nonbank entities. Our detailed discussion of questions in the request for information, particularly to questions 13 and 18, result in the following set of recommendations[13] to be considered by the Treasury Department:

- Monitor the size and interconnectedness of nonbanks using AI in financial services to assess systemic importance.
- Develop standards for securely sharing customer data to encourage competition and level the playing field.
- Where feasible, collaborate with the financial sector and government partners to explore "nutrition labels" for AI systems to clarify data sources and usage.
- Allocate responsibilities and supervisory reporting for partnerships and outsourcing arrangements.
- Define regulatory jurisdiction over nonbank financial services using AI and establish interagency coordination mechanisms.

[13] Our recommendations are entirely based on expert insights from the authors rather than findings from new research.

- Fund research on emerging illicit finance typologies enabled by AI.
- Modernize regulatory frameworks to address the use of automated agents in financial activities.
- Encourage data sharing to enhance AI-driven Know Your Customer (KYC) solutions and combat illicit finance.
- Support the development of digital identity and verifiable credential solutions.
- Invest in building technical expertise and capabilities of regulatory agencies and law enforcement in domains such as AI/ML, data analytics, digital forensics, and FinTech.
- Close regulatory gaps that facilitate the use of AI in illicit finance, including digital asset activities.
- Support the expansion of CFIUS authority over critical technologies.
- Collaborate to strengthen safeguards for protecting sensitive personal data.
- Ensure CFIUS is adequately resourced to examine foreign investments in AI technology and identify non-notified transactions.

Detailed Response to RFI Questions

Using a question and answer format, we respond to questions in the Treasury Department's Request for Information in this section. Specifically, we provide detailed responses to questions 2, 13, and 18 below.

Response to Question 2

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

Answer: AI's integration into capital markets has revolutionized operations, enhancing efficiency, accuracy, and risk management while offering innovative solutions for fraud detection, sentiment analysis, and regulatory compliance.[14]

AI methodologies, such as machine learning (ML) and natural language processing, have led to notable advancements in firm trading and investing. In response to this question, we provide insight on a subset of use cases of AI models and tools related to capital markets, risk management, regulatory compliance, and customer services. We provide further details in the sections below.

Capital Markets

Trading and Investment

Leveraging the ability to rapidly process and analyze vast quantities of data, AI has been used to optimize order routing, optimally allocate block trades, and analyze public sentiment to inform trading decisions.[15] For example, asset management firms adopted AI to identify new opportunities, allocate portfolios, and execute high-frequency trading[16] by analyzing large volumes of market data, identifying patterns, and executing trades faster than human traders.[17] A recent study found that AI-based large language models led to profitable investments.[18]

[14] OECD, 2021.

[15] Mayor, Financial Industry Regulatory Authority. Mayor, Financial Industry Regulatory Authority.

[16] Congressional Research Service, "Artificial Intelligence and Machine Learning in Financial Services," R47997, June 26, 2023. As of October 5, 2023: https://crsreports.congress.gov/product/pdf/R/R47997/2.

[17] Ta, V.-D., Liu, C.-M., & Addis, D. (2018). Prediction and Portfolio Optimization in Quantitative Trading Using Machine Learning Techniques. In *Proceedings of the 9th International Symposium on Information and Communication Technology*, Danang City, Viet Nam. https://doi.org/10.1145/3287921.3287963

[18] Kirtac, K., & Germano, G. (2024). Sentiment trading with large language models. *Finance Research Letters, 62*, 105227. https://doi.org/10.1016/j.frl.2024.105227

Another study indicates that market participants utilizing AI, like hedge funds, react rapidly to new data, particularly machine-readable disclosures, causing swift movements in stock prices.[19]

Robo-advisors

AI-driven "robo-advisors" have gained popularity in financial institutions due to their ability to offer personalized investment advice at a lower cost than traditional advisors. In contrast to rule-based systems (e.g., Betterment) that analyze investor profiles and goals, AI-driven robo-advisors aim to leverage more advanced models and tools, particularly generative models, to manage portfolios, provide efficient and automated investment management, optimize investment strategies, and enhance client experiences. Additionally, robo-advisors make financial services more accessible to broader audiences, including those with smaller investment portfolios, by lowering the entry barriers and offering user-friendly interfaces.[20]

Robo-advisors are often described as having the potential to democratize the use of financial advisory services.[21] By increasing information efficiency, reducing fees, and making services easily available 24/7, a wider range of consumers can afford and access investment advice. However, while banks and, more so, finance companies have been launching and advertising some version of robo-advisors since 2010, this technology appears to still be in an early adoption phase, in which consumers are slow to adopt and trust these tools.[22] As a result, more research is needed on the adoption and use of robo-advisors and the use of these services and potential risks as it scales. A multitude of legal and technical risks already exist including the question of whether robo-advisors can feasibly fulfill their fiduciary obligations. This would require evidence that advice is in the client's best interest (i.e., rather than the interests of the firm who owns or made the AI). A client's actual risk tolerance may be hard to capture through automation, for example, based primarily on surveys, as modern behavioral finance theories have pointed to clients as complex actors, influenced by individual emotions and heuristics, and biases.[23] At the same time, robo-advisors can have their own potential to affect these

[19] Cao, S., Jiang, W., Yang, B., & Zhang, A. L. (2023). How to Talk When a Machine Is Listening: Corporate Disclosure in the Age of AI. *The Review of Financial Studies, 36*(9), 3603-3642. https://doi.org/10.1093/rfs/hhad021

[20] Bartram, S. M., Branke, J., & Motahari, M. (2019). *Artificial Intelligence in Asset Management*. ERN: Neural Networks & Related Topics (Topic).

[21] Sironi, Paolo, *FinTech innovation: from robo-advisors to goal based investing and gamification*: John Wiley & Sons, 2016.

[22] Belanche, Daniel, Luis V Casaló, and Carlos Flavián, "Artificial Intelligence in FinTech: understanding robo-advisors adoption among customers," *Industrial Management & Data Systems,* Vol. 119, No. 7, 2019, pp. 1411-1430.

[23] Barberis, Nicholas, and Richard Thaler, "Chapter 18 A survey of behavioral finance," *Handbook of the Economics of Finance*: Elsevier, 2003, pp. 1053-1128. https://www.sciencedirect.com/science/article/pii/S1574010203010276,

Hirshleifer, David, "Behavioral Finance," *Annual Review of Financial Economics,* Vol. 7, No. Volume 7, 2015, pp. 133-159: https://www.annualreviews.org/content/journals/10.1146/annurev-financial-092214-043752 behavioral biases, as well as risk tolerance.[24] And, as more clients are added, a robo-advisor needs to maintain appropriate levels of security, integrity, and resilience. Possible side effects of scaling these kinds of services include customer segmentation, concentrated risks as a result of common advice or algorithms, and a disruption of service due to capacity constraints.

Financial forecasting and analytics

AI has enabled more accurate forecasting and prediction in the financial sector. Firms employ ML applications to optimize liquidity and cash management, forecast startup performance, and monitor risk. AI's advantage is its ability to process large amounts of data as close to real-time as possible. Two main areas include improving research and automating the role of financial advisors. In improving research, firms are interested in improving data analysis and prediction. By applying machine learning algorithms to vast amounts of data to develop predictions and applying natural language processes to improving search capabilities. Some private investment and hedge firms already engage in this type of research, but AI increases the possibility for greater amounts of research, produced faster, at lower costs, and with less reliance on human expertise. However, the same caveats, limitations, and assumptions that exist in traditional research will also exist in AI-enabled forecasts and analytics. This could lead to some overconfidence in potential conclusions without regard for the latter issues. In addition, AI has been known to hallucinate creating synthetic or false information.[25]

Risks and Challenges

While AI introduces better performance and efficiency in the financial system, it also brings significant risks to financial stability through market manipulation, collusion, herding behavior,

[24] D'Acunto, Francesco, Nagpurnanand Prabhala, and Alberto G Rossi, "The Promises and Pitfalls of Robo-Advising," *The Review of Financial Studies,* Vol. 32, No. 5, 2019, pp. 1983-2020. As of 8/7/2024:https://doi.org/10.1093/rfs/hhz014,

Bhatia, Ankita, Arti Chandani, and Jagriti Chhateja, "Robo advisory and its potential in addressing the behavioral biases of investors — A qualitative study in Indian context," *Journal of Behavioral and Experimental Finance,* Vol. 25, 2020/03/01/, 2020, p. 100281. https://www.sciencedirect.com/science/article/pii/S2214635019302394

[25] Roychowdhury, Sohini, "Journey of Hallucination-minimized Generative AI Solutions for Financial Decision Makers," paper presented at Proceedings of the 17th ACM International Conference on Web Search and Data Mining, Merida, Mexico, Association for Computing Machinery, 2024. https://doi.org/10.1145/3616855.3635737,

Xiao, Wenyi, Ziwei Huang, Leilei Gan, Wanggui He, Haoyuan Li, Zhelun Yu, Hao Jiang, Fei Wu, and Linchao Zhu, "Detecting and mitigating hallucination in large vision language models via fine-grained ai feedback," *arXiv preprint arXiv:2404.14233*, 2024.

Alkaissi, H., and S. I. McFarlane, "Artificial Hallucinations in ChatGPT: Implications in Scientific Writing," *Cureus,* Vol. 15, No. 2, Feb 2023, p. e35179. , making them "risky for high-stakes domains"

Magesh, Varun, Faiz Surani, Matthew Dahl, Mirac Suzgun, Christopher D. Manning, and Daniel E. Ho, "Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools," *ArXiv,* Vol. abs/2405.20362, 2024.

uniformity, interconnectedness, and biased outcomes. Below, we present four categories of potential risks.

1. **Market manipulation and collusion**: AI-based trading has the potential to intensify illegal trading practices aimed at market manipulation, making it harder for supervisors to detect these activities, especially if there is collusion among AI systems. One study found that AI traders can implicitly collude to manipulate market prices and generate higher profits.[26] This collusion happens without any explicit agreement or communication, which means it doesn't violate antitrust laws but still has significant effects. The authors described mechanisms of collusion as homogenized learning biases (artificial stupidity) and price-trigger mechanisms (artificial intelligence). Another study stated that autonomous AI agents might independently discover methods to manipulate markets in their quest to maximize profitability, without any input from developers.[27] Highlighting recent incidents where companies and individuals have been deceived by deepfakes, panelists of a House-sponsored regulatory roundtable voiced concerns that the growing frequency of such attacks to manipulate the market could cause significant financial loss and diminish trust in the institutions attacked and U.S. financial institutions overall.[28]
2. **Data quality and bias**: Dataset quality significantly impacts AI and ML outcomes and performance, making it a key risk. Learned biases in datasets can lead to discriminatory decisions and undesirable outcomes for market participants, as biases introduced during data collection or cleansing can degrade algorithm performance and harm consumers over time.
3. **Uniformity and procyclicality**: The dependence of AI models on similar datasets poses a risk of uniformity and procyclicality. Due to economies of scale and scope in data collection, a limited number of large data producers, such as major tech companies, dominate the market. When most ML applications are trained on these same datasets, there is an increased likelihood of uniformity and procyclicality in standardized AI models.[29]

[26] Dou, W. W., Goldstein, I., & Ji, Y. (2024). *AI-Powered Trading, Algorithmic Collusion, and Price Efficiency*. Jacobs Levy Equity Management Center for Quantitative Financial Research Paper. Retrieved from https://ssrn.com/abstract=4452704 or http://dx.doi.org/10.2139/ssrn.4452704.

[27] Mizuta, T. (2020, 1-4 Dec.). Can an AI perform market manipulation at its own discretion? – A genetic algorithm learns in an artificial market simulation –. *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*.

[28] House Committee on Financial Services, "AI Innovation Explored: Insights into AI Applications in Financial Services and Housing," Staff Report from the Bipartisan Working Group on Artificial Intelligence, July 18, 2024.

[29] Aldasoro, I., Gambacorta, L., Korinek, A., Shreeti, V., & Stein, M. (2024). *Intelligent financial system: how AI is transforming finance* (Working Papers, Issue). Retrieved from https://www.bis.org/publ/work1194.pdf

4. **Interconnectedness**: Due to the rise of AI, financial firms, digital service providers, and software vendors are becoming more interconnected, allowing cyber incidents to spread through channels faster, potentially posing systemic threats to the financial system.[30]

Risk Management

Credit Risk Assessment

AI supports assessing customer creditworthiness from data, reducing time and costs associated with manual underwriting.

For credit lending decisions, there is hope that AI could perform better than traditional models in predicting, for example, default risk.[31] However, much of the literature suggests that the expertise of loan officers may not be easily replicated due to discretionary factors that are hard to capture in machine-based models.[32] AI models in this context can also improve the ability to collect information about customers related to their financial transactions, as well as leverage new and unconventional data sources, including publicly available data, social media, and third-party online vendors.[33] When engaging, firms might be liable for intellectual property and privacy risks. However, even when soundly legal, these practices are poised to raise privacy concerns as new applications of data result in new types of consequences for consumers in the future. Finally, AI models have been known to introduce data biases across a variety of sectors that could lead to illegal and unfair treatment of potential lending clients in the financial sector.[34] Of note, Article 22 of the EU's GDPR framework prohibits the sole use of automated

[30] Leitner, G., Singh, J., Kraaij, A. v. d., & Zsámboki, B. (2024). *The rise of artificial intelligence: benefits and risks for financial stability* (Financial Stability Review, Issue). Retrieved from https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html#toc2

[31] Van Thiel, Diederick, and Willem Frederik Fred Van Raaij, "Artificial intelligence credit risk prediction: An empirical study of analytical artificial intelligence tools for credit risk prediction in a digital era," *Journal of Risk Management in Financial Institutions,* Vol. 12, No. 3, 2019, pp. 268-286.

[32] Costello, Anna M., Andrea K. Down, and Mihir N. Mehta, "Machine + man: A field experiment on the role of discretion in augmenting AI-based lending models," *Journal of Accounting and Economics,* Vol. 70, No. 2, Nov 1, 2020, p. 101360. https://www.sciencedirect.com/science/article/pii/S0165410120300628.

[33] Uykur, Denizhan, "The new physics of financial services-understanding how artificial intelligence is transforming the financial ecosystem-part of the future of financial services series| Prepared in collaboration with Deloitte," 2018.

[34] Parikh, Ravi B, Stephanie Teeple, and Amol S Navathe, "Addressing bias in artificial intelligence in health care," *Jama,* Vol. 322, No. 24, 2019, pp. 2377-2378. ,

Ntoutsi, Eirini, Pavlos Fafalios, Ujwal Gadiraju, Vasileios Iosifidis, Wolfgang Nejdl, Maria-Esther Vidal, Salvatore Ruggieri, Franco Turini, Symeon Papadopoulos, Emmanouil Krasanakis, Ioannis Kompatsiaris, Katharina Kinder-Kurlanda, Claudia Wagner, Fariba Karimi, Miriam Fernandez, Harith Alani, Bettina Berendt, Tina Kruegel, Christian Heinze, Klaus Broelemann, Gjergji Kasneci, Thanassis Tiropanis, and Steffen Staab, "Bias in data-driven artificial intelligence systems—An introductory survey," decision-making that could “produce legal effects concerning him or her” and was used to rule against using automated credit scoring for credit agencies unless certain conditions are met.[35]

Fraud Detection, Anti-Money Laundering (AML)

AI identifies anomalies in transaction data that may indicate fraud and other illicit activities, enabling mitigation of financial crimes.[36]

AI-powered algorithms can analyze extensive data in real-time to detect fraudulent activities more accurately than traditional rule-based systems.[37] Financial institutions and FinTech lenders use these algorithms for various purposes, including client onboarding and know-your-customer (KYC) checks, anti-money laundering (AML) and terrorist financing screening on a shared platform during onboarding and ongoing customer due diligence, and identifying suspicious activities during continuous monitoring.[38] This capability mitigates the risk of financial fraud, a long-standing concern in the sector, by continuously analyzing vast amounts of data in real-time to identify anomalies and patterns indicative of fraudulent activity, enabling immediate alerts and swift responses to potential threats.[39]

Cybersecurity and Data Protection

AI methods have augmented legacy, signature-based, threat detection approaches – enabling the detection of malicious activity without known signatures at improved quality and cost.[40]

WIREs Data Mining and Knowledge Discovery, Vol. 10, No. 3, 2020, p. e1356. https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1356;

Ferrara, Emilio, "Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies," *Sci,* Vol. 6, No. 1, 2023, p. 3.

[35] European Union, "Article 22 of the General Data Protection Regulation (GDPR)," 2016. As of October 5, 2023: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[36] U.S Department of Treasury, February 2024.

[37] Kuttiyappan, Damodharan, & V, Rajasekar. (2024). AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis. *EAI Endorsed Transactions on Scalable Information Systems*, 10.4108/eai.23-11-2023.2343170.

[38] OECD, 2021.

[39] Bachir, B. E., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., & Ravikumar, R. (2021). *Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance*. IMF Departmental Paper No 2021/024. Retrieved from https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717;

Zhang, Z., Hamadi, H. A., Damiani, E., & Taher, C. Y. Y. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access, 10*. https://doi.org/10.1109/access.2022.3204051

[40] U.S Department of Treasury, February 2024.

Broadly, the financial services sector is facing a growing number of costly cybersecurity threats and cyber-enabled crime.[41] The use of AI in the financial sector introduces both increased security and efficient detection.

AI can significantly enhance cybersecurity measures by rapidly identifying and responding to cyber threats. These systems can analyze network traffic patterns, detect anomalies, and quickly respond to potential breaches.[42] This improves the overall security posture of financial institutions by effectively addressing sophisticated cyber threats that traditional methods might miss.[43]

Risks and Challenges

These same AI technologies can be leveraged by malicious actors, expand the scope for cyber threats and fraud, and introduce new unique cyber threads to AI including data poisoning, input attacks, and model extraction or model inversion attacks.

Data poisoning involves attackers injecting false data into an AI system's training set, causing the model to learn incorrect patterns and make inaccurate predictions. Input attacks, such as adversarial attacks, manipulate the input data to deceive the AI system into making wrong decisions or misclassifying information. Model extraction or inversion attacks occur when attackers reverse-engineer an AI model to either steal the underlying algorithm or infer sensitive information about the training data, compromising the model's integrity and privacy.[44]

The complexity of AI models, particularly deep learning ones, often results in a "black box" effect, making it challenging for even developers to grasp the internal workings of these systems.[45] This lack of explainability in how inputs are processed, and outputs are produced means that AI-driven cybersecurity decisions lack clear justification and comprehensibility. As a

[41] International Monetary Fund, "Rising Cyber Threats Pose Serious Concerns for Financial Stability," IMF Blog, April 9, 2024. As of October 5, 2023: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

[42] Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2017). A survey of deep learning-based network anomaly detection. *Cluster Computing, 22*, 949-961.

[43] U.S. Department of the Treasury, March 2024.

[44] Bachir, B. E., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., & Ravikumar, R. (2021). *Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance*. IMF Departmental Paper No 2021/024. Retrieved from https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717

[45] Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Nieble, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). *The AI Index 2024 Annual Report*. Retrieved from https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf

result, cybersecurity measures that depend on these AI models are at risk of becoming opaque and highly vulnerable to breaches and AI-based cyber threats.[46]

Moreover, the accessibility and advancement of AI have empowered malicious actors to utilize sophisticated generative AI tools, making fraud against banks and their customers more complex and challenging to identify. For example, in January 2024, a Hong Kong-based firm fell victim to a deepfake scam, where an employee was deceived into transferring $25 million to fraudsters who convincingly impersonated her colleagues on a video call.[47]

Response to Question 13

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

Answer: The use of AI in illicit finance is dual edged. Expectations are high for AI to help combat fraud, money laundering, and other forms of illicit finance, spurred in part by notable successes.[48] A related concern for financial institutions is how AI may provide criminals, adversaries, and other threat actors with new methods to conduct illicit activities. Below, we answer the questions above by first describing the dual role of AI in illicit finance and second identifying potential regulatory gaps.

AI's Dual Role in Illicit Finance

This section discusses several examples of the dual-edged nature of AI: AI-enabled money laundering, AI-enhanced document fraud, and AI-related illicit goods and services. It also concludes by noting that the application of AI to combatting illicit finance bears drawbacks and unintended consequences.

AI could enable sophisticated money laundering techniques by automating and scaling illicit activities, making detection and prevention more challenging. A 2023 survey of AML

[46] Zhang, Z., Hamadi, H. A., Damiani, E., & Taher, C. Y. Y. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access, 10*. https://doi.org/10.1109/access.2022.3204051

[47] Cooban, Anna "Hong Kong Company Scammed Out of $35 Million by Deepfake CEO," CNN, February 4, 2024. As of October 5, 2023: https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

[48] See for example: Reuters, "Visa Prevented $40 Bln Worth of Fraudulent Transactions in 2023- Official," July 23, 2024 (https://www.reuters.com/technology/cybersecurity/visa-prevented-40-bln-worth-fraudulent-transactions-2023-official-2024-07-23/);

Department of the Treasury, "Treasury Announces Enhanced Fraud Detection Process Using AI Recovers $375M in Fiscal Year 2023," press release, February 28, 2024 (https://home.treasury.gov/news/press-releases/jy2134).

professionals found that 46 percent of respondents ranked sophisticated money laundering techniques, including those using generative AI, among their leading challenges.[49]

AI-enhanced document fraud involves using AI to create convincing fake identity documents that can bypass KYC checks, facilitating the creation and sale of fraudulent accounts. This includes using deepfakes and automated document and video generation services, which can scale the production of fake identities and deceive enhanced ID verification systems.[50]

AI-related illicit goods and services have increasingly been observed on dark web markets, reflecting both low-level and sophisticated criminal activities. [51] These include the sale of AI-generated explicit images, deepfakes, and falsified identity documents. AI tools are also used to create scam sites and disseminate financial disinformation at scale. These activities enhance illicit markets by facilitating the creation and distribution of illegal goods and services.[52]

The application of AI to combating illicit finance can also present drawbacks and unintended consequences. For example, biases present in training data can lead AI-enabled systems to "unfairly target as suspicious the financial activities of certain types of individuals or entities, or produce risk profiles and decisions that deny them access to certain financial products and services."[53] Limited explainability of AI models can compound this problem by undermining financial institutions' ability to justify their risk management and regulatory compliance decisions.[54]

Furthermore, the race between AI-driven detection systems and AI-enabled illicit activities could lead to an escalation in the sophistication of both sides. As financial institutions and regulatory bodies develop more advanced AI tools to detect and prevent illicit finance, adversaries may simultaneously enhance their techniques to evade detection, creating a continuous cycle of adaptation and counter-adaptation.

[49] Feedzai, *The State of Global AML Compliance 2023*, August 2023 (https://feedzai.com/aptopees/2023/08/Feedzai-The-State-of-AML-Compliance-2023.pdf).

[50] Akartuna , Eray Arda, *AI-Enabled Crime in the Cryptoasset Ecosystem*, Elliptic, 2024, pp. 41–43 (https://www.elliptic.co/resources/ai-enabled-crime-in-the-cryptoasset-ecosystem).

[51] Akartuna, 2024.

[52] Akartuna, 2024.

[53] Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT*, July 2021, pp. 42–43 (https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html).

[54] Shabsigh, Ghiath and El Bachir Boukherouaa, "Generative Artificial Intelligence in Finance: Risk Considerations," International Monetary Fund, *Fintech Notes* No. 2023/006, August 22, 2023, p. 9 (https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570).

Regulatory Gaps for Illicit Finance

The potential role of AI in illicit finance exposes several regulatory gaps that are unique to the use of AI.

One gap is the focus of Bank Secrecy Act (BSA)/AML regulations and sanctions authorities on legal persons and real-world entities. The potential of AI to automate financial activities through bots and other virtual entities could complicate the enforcement of regulations designed in an era predating such automation. Automated illicit finance coupled with privacy-enhanced digital assets traded in unregulated markets could create a perfect storm for law enforcement to effectively detect and investigate. Existing legal frameworks may also be inadequate for prosecuting AI-related illicit activities or imposing appropriate penalties, particularly when legal liabilities are ambiguous or ill-defined.

Data access is another critical issue. Effective AI-driven KYC solutions require access to large datasets, but data privacy regulations and restrictions on data sharing can hinder this access. Inter-firm and cross-border data issues further complicate this issue. Data sharing between financial institutions within the same jurisdiction can be hindered by competitive concerns and regulatory restrictions, limiting the effectiveness of collaborative efforts. Differing data privacy laws can impede information sharing across jurisdictions. This fragmentation creates inconsistencies and gaps that sophisticated criminals can exploit, making it challenging to coordinate efforts against AI-driven illicit finance.

Regulatory agencies and law enforcement may lack the necessary knowledge base and technical capacity to effectively detect and investigate AI-driven illicit finance, especially in the many relatively small jurisdictions across the country. These capability gaps could hinder the enforcement of existing laws and insufficiently equip regulators with the information they need to update regulation.

Policy Remedies for Illicit Finance

Based on our review of the literature, previous work and our knowledge of the regulatory structure, below we list several remedies to consider in addressing the dual role of AI and regulatory gaps discussed above. As noted earlier, these recommendations are not based on new research.

- Modernize regulatory and legal frameworks to anticipate the use of automated agents in financial activities and include provisions for prosecuting related illicit activities and imposing appropriate penalties.
- Encourage data sharing between financial institutions and other relevant firms to enhance the effectiveness of AI-driven KYC solutions and collaborative efforts against illicit finance.
- Continue to support research and development of digital identity or verifiable credential solutions, including those for automated agents.
- Invest in building the technical expertise and capabilities of regulatory agencies and law enforcement in domains such as AI/ML, data analytics, digital forensics, and FinTech, including providing resources and technical assistance to smaller jurisdictions.
- Close existing regulatory gaps that could facilitate the use of AI in illicit finance, such as by bringing more digital asset activities into the regulatory perimeter.

Response to Question 18, part A

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

Answer: When considering promoting responsible innovation and competition, it will be important to consider the role nonbank firms are already playing in AI-driven financial innovation and their potential to increase that influence. Nonbank firms, such as Big Tech companies, have access to vast amounts of consumer data, which could give them a competitive advantage over traditional financial firms. Nonbank firms are emerging as significant players in AI-driven financial innovation, leveraging advanced technologies to offer a range of financial services and products to consumers and merchants, and providing AI solutions to traditional banks.[55] These firms, often early adopters of AI, are interconnected within financial services and potentially integral to AI enabled investment strategies and peer-to-peer lending, while also offering AI services for identity verification, fraud prevention, and customer service enhancement. Despite potential advantages, the integration of AI by nonbank entities introduces several uncertain but consequential risks, such as increased systemic interconnectedness, potential single points of failure, expanded cyberattack surfaces, and regulatory gaps, all of which could impact the stability of the financial system. Below, we describe the importance of nonbank firms to financial innovation, discuss uncertainty and potential systemic risks posed by nonbank firms, identify potential regulatory gaps in detail, and pose several policy recommendations in response to the questions above.

Nonbank Firms Are Important Sources of AI-Driven Financial Innovation

Nonbank firms are increasingly using AI to offer financial services and products to consumers and merchants, and to provide AI services to banks. These nonbank firms have often been early adopters of AI technologies and are positioning themselves as leaders in the integration of AI into financial services.[56]

[55] We use the term *nonbank firms* referring to Treasury's definition of "new entrant non-bank firms" (U.S. Department of the Treasury, *Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets*, November 2022, p. 1. As of August 7, 2024: https://home.treasury.gov/news/press-releases/jy1105):

> non-incumbent non-bank firms that offer consumer financial products and services. New entrant non-bank firms may be one of the following: "Big Tech firms," which are large technology companies whose primary activity involves the provision of platform-based digital services; "fintech firms," which are companies that specialize in offering digital financial services to consumers or enable other financial service providers to offer digital financial services used by consumers; and "retail firms," which refers to new entrant non-bank firms that are not fintech or Big Tech firms.

[56] Citi, *AI in Finance: Bot, Bank & Beyond*, June 2024: https://www.citigroup.com/global/insights/citigps/ai-in-finance.

Several examples of financial services and products provided by nonbanks include embedded finance, investment, and peer-to-peer (P2P) lending. Embedded finance integrates financial services into existing platforms. Firms including Square, Shopify, and Amazon are using AI to tailor financial products such as loans and payment processing directly within their platforms. In the investment sector, firms such as Robinhood are exploring AI to offer personalized investment strategies and advisory services. P2P lending platforms such as Prosper employ AI to assess credit risk and match borrowers with potential lenders more efficiently.[57]

Nonbanks also provide AI services to international financial institutions. Firms such as J.P. Morgan Chase & Co and Morgan Stanley are employing AI capabilities based on OpenAI software.[58] Socure provides AI for identity verification, fraud prevention, and BSA/AML screening. Zest AI offers machine learning models to help banks and credit unions improve their credit underwriting processes. Kasisto provides AI-driven chatbots to enhance customer service and operational efficiency for financial institutions.[59]

[57] Vir Singh, Arjun, Mohammad Nikkar, Michael Bateman, et al., "The Intersection of AI & Financial Services," Arthur D. Little, November 2023 https://www.adlittle.com/en/insights/viewpoints/intersection-ai-financial-services;

Telis Demos, "AI Gives Robinhood Another Arrow in its Quiver," *The Wall Street Journal*, July 2, 2024 (https://www.wsj.com/finance/investing/robinhood-could-use-ai-to-break-into-advisory-3653f9aa);

U.S. Securities and Exchange Commission, "EDGAR Search Results for CIK 1416265," As of October 5, 2023: https://www.sec.gov/edgar/browse/?CIK=1416265.

[58] Ghosh, Palash, "J.P. Morgan Chase Launches IndexGPT for Institutional Clients," *Pensions & Investments*, May 15, 2024 (https://www.pionline.com/money-management/jp-morgan-chase-launches-indexgpt);

Marr, Bernard, "The Future of Banking: Morgan Stanley and the Rise of AI-Driven Financial Advice," *Forbes*, April 16, 2024 (https://www.forbes.com/sites/bernardmarr/2024/04/16/the-future-of-banking-morgan-stanley-and-the-rise-of-ai-driven-financial-advice/).

[59] Socure, "Socure Makes History as the World's First AI Technology to Successfully Solve for Account Opening Identity Fraud After 10+ Years of R&D," *PRNewswire*, January 16, 2024 (https://www.prnewswire.com/news-releases/socure-makes-history-as-the-worlds-first-ai-technology-to-successfully-solve-for-account-opening-identity-fraud-after-10-years-of-rd-302034136.html);

Zest AI, "Zest AI Announces FairBoost, A Tool for Fairer and Clearer Credit Underwriting for Lenders," *PRNewswire*, June 26, 2023 (https://www.prnewswire.com/news-releases/zest-ai-announces-fairboost-a-tool-for-fairer-and-clearer-credit-underwriting-for-lenders-301862754.html);

Kasisto, "Our Products," webpage, undated (https://kasisto.com/products/).

Socure employs proprietary AI/ML algorithms, including generative AI and natural language processing techniques, which suggest the use of LLMs developed in-house (Socure, "Socure Launches Compliance Product Suite Leveraging GenAI to Optimize Accuracy of Identity Verification," webpage, October 2, 2023. As of August 7, 2024:

Nonbank Financial Innovation Poses Uncertain but Consequential Risks

The integration of AI by nonbank firms into financial services creates risks that are not only important due to their possible impact on the U.S. financial system but are also difficult to measure or predict. This is particularly concerning because nonbank entities are often not subject to the same regulatory scrutiny leading to gaps in oversight. Several key areas illustrate the nature of these risks:

- The widespread adoption of AI by nonbanks could lead to greater homogeneity in risk assessments and credit decisions, increasing the interconnectedness of financial institutions. This interconnectedness could amplify shocks and lead to systemic risks, particularly if AI models fail to perform adequately during periods of structural shifts or sudden market changes.[60]
- The concentration of core AI services, especially in the provision of cloud services, could create single points of failure, potentially triggering systemic disruption.[61]
- The increased interconnectivity and disaggregation of services characteristic of nonbank financial applications introduces more links to each product chain and user interface. This can increase the cyber-attack surface and create complex webs of operational dependency.[62]
- The integration of nonbank AI systems into financial institutions could expose the financial sector to novel cyber threats, such as model inversion attacks, where attackers could extract sensitive information from AI models, and adversarial attacks, where malicious inputs are designed to deceive AI systems.[63]

https://www.socure.com/news-and-press/socure-launches-compliance-product-suite-leveraging-genai-to-optimize-accuracy-of-identity-verification).

Zest AI does not appear to use LLMs directly in its credit analysis but offers "LuLu," a customized generative AI tool for lending organizations, though the underlying LLM developer is not specified (Zest AI, "Zest AI Unveils First AI Lending Intelligence Companion," webpage, February 29, 2024. As of August 7, 2024: https://www.zest.ai/insights/zest-ai-unveils-first-ai-lending-intelligence-companion).

Kasisto has developed its own "banking industry-specific" LLM in-house, named "KAI-GPT" (Kasisto, "Kasisto Launches KAI-GPT, the First Banking Industry-Specific Large Language Model," webpage, May 31, 2023. As of August 7, 2024: https://kasisto.com/press-releases/kasisto-launches-kai-gpt-the-first-banking-industry-specific-large-language-model/).

[60] Boukherouaa, El Bachir, Ghiath Shabsigh, Khaled AlAjmi et al., *Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance*, International Monetary Fund Departmental Paper No. 2021/024, October 22, 2021, pp. 17–19 (https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717).

[61] Feyen, Erik, Jon Frost, Leonardo Gambacorta, et al., 2021.

[62] Feyen, Erik, Jon Frost, Leonardo Gambacorta, et al., 2021.

[63] Boukherouaa, El Bachir, Ghiath Shabsigh, Khaled AlAjmi et al., 2021.

- Big Tech companies' access to vast amounts of consumer data could enable them to target customers' behavioral biases, potentially encouraging them to take on excessive risks.[64]
- Nonbanks are subject to less regulation and supervision compared to banks. This regulatory gap can lead to inconsistencies in risk management practices and oversight, potentially increasing overall risk to the financial system.[65]
- The existing regulatory framework may not adequately accommodate the rapid integration of Big Tech into the financial system, potentially leading to regulatory arbitrage and increased financial instability.[66]

Regulatory Gaps for Nonbank Entities

Nonbanks may be outpacing the development of regulatory frameworks, leading to gaps that need to be addressed to mitigate associated risks.

One significant regulatory gap lies in the differential supervisory and regulatory obligations financial institutions face compared to nonbank providers of financial services and products. Regulated financial institutions are subject to stringent oversight and compliance requirements, such as capital reserve standards, regular audits, consumer protection laws, and other prudential regulations designed to ensure their stability and protect consumers. By contrast, nonbank financial service providers and tech suppliers often operate under a less rigorous regulatory regime. Furthermore, current regulations may not adequately cover new entrants and innovative business models, exacerbating inconsistencies in oversight and enforcement. Some suggest that the increasing diversity of financial service providers and business models necessitates an expansion of the regulatory perimeter.[67]

Another regulatory gap relates to the governance of partnerships and outsourcing. Financial institutions often partner with Big Tech companies, such as cloud providers, and other nonbank firms, which can limit the scope of regulated institutions to enforce specific requirements. This creates a need for clear regulatory guidance on the governance of such partnerships and outsourcing arrangements.[68]

[64] Eichengreen, Barry, "The Challenge of Big Tech Finance," *Project Syndicate*, April 9, 2021 (https://www.project-syndicate.org/commentary/regulatory-challenges-of-big-tech-finance-by-barry-eichengreen-2021-04) cited in Tierno, Paul, *Big Tech in Financial Services*, Congressional Research Service R47104, July 29, 2022, p. 27 (https://crsreports.congress.gov/product/details?prodcode=R47104).

[65] Calem, Paul, "The Role of Machine Learning and Alternative Data in Expanding Access to Credit: Fintechs' Regulatory Advantage Is to the Detriment of Consumers," *Bank Policy Institute Blog*, October 6, 2022 (https://bpi.com/the-role-of-machine-learning-and-alternative-data-in-expanding-access-to-credit-fintechs-regulatory-advantage-is-to-the-detriment-of-consumers/).

[66] Tierno, Paul, *Big Tech in Financial Services*, Congressional Research Service R47104, July 29, 2022, pp. 21–25 (https://crsreports.congress.gov/product/details?prodcode=R47104).

[67] Feyen, Erik, Jon Frost, Leonardo Gambacorta, et al., 2021.

[68] Feyen, Erik, Jon Frost, Leonardo Gambacorta, et al., 2021.

There are valuable lessons to learn from regulating digital assets, particularly in avoiding a "Facebook Libra moment" and confusion regarding regulatory jurisdiction.[69] Facebook Libra took policymakers by surprise with a disruptive financial innovation that exposed significant regulatory gaps and jurisdictional ambiguities, leading to urgent calls for regulatory action. This underscores the challenge of adapting existing regulatory frameworks to rapidly evolving technologies in the financial sector. Similarly, the rapid integration of AI by nonbank firms into financial services may create a complex regulatory landscape with overlapping responsibilities among various agencies. However, a lack of clear jurisdiction and coordination among regulators could lead to regulatory arbitrage, where firms choose to structure their operations to exploit gaps and inconsistencies in oversight. Additionally, the absence of coordinated regulatory frameworks can result in fragmented and ineffective supervision, increasing the risk of financial instability.

Policy Recommendations for Nonbank Entities

- Closely monitor the size and interconnectedness of nonbanks in financial services that use AI to assess their systemic importance.[70] This is a natural fit for the Financial Stability Oversight Council and could involve coordination with Treasury's Office of Financial Research, interagency partners such as the Cybersecurity and Infrastructure Security Agency, and international organizations such as the Financial Stability Board.
- Examine how the development of standards that enable market participants to securely share relevant customer data, such as open banking, could encourage competition and level the playing field among market participants.[71]
- Collaborate with the financial sector and government partners such as NIST, NTIA, and CISA to explore the concept of *nutrition labels* for AI systems, similar to a Software Bill of Materials, to clearly identify the data used to train AI models, their sources, and how data submitted to the model is incorporated.[72]

[69] In June 2019, Facebook announced plans to launch a digital asset called Libra, using blockchain technology and backed by 28 nonbank firms and nonprofits. Libra aimed to provide "an alternative to traditional financial services" for "billions of people worldwide" without banking access. However, lawmakers and regulators raised concerns that Libra could "threaten government-backed currencies and consumer privacy," while giving Facebook unprecedented financial influence (Telford, Taylor, "Why Governments Around the World Are Afraid of Libra, Facebook's Cryptocurrency," *Washington Post*, July 12, 2019. As of August 7, 2024: https://www.washingtonpost.com/business/2019/07/12/why-governments-around-world-are-afraid-libra-facebooks-cryptocurrency/). Facing intense regulatory scrutiny, Facebook rebranded and reformed the project but ultimately shut it down in January 2022 (Dwoskin, Elizabeth and Gerrit De Vynck, "Facebook's Cryptocurrency Failure Came After Internal Conflict and Regulatory Pushback," *Washington Post*, January 28, 2022. As of August 7, 2024: https://www.washingtonpost.com/technology/2022/01/28/facebook-cryptocurrency-diem/).

[70] Bordeaux, John, Jonathan W. Welburn, Sasha Romanosky, et al., 2023.

[71] Financial Stability Board, 2019.

[72] U.S Department of Treasury, March 2024.

- Clearly allocate responsibilities and supervisory reporting for partnerships and outsourcing arrangements to ensure accountability and effective oversight.[73]
- Clearly define the regulatory jurisdiction of agencies over nonbank financial services that use AI and establish formal mechanisms for interagency coordination to address gaps and overlaps.

Response to Question 18, part B.

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

Answer: Foreign investment in U.S. AI technology has potential for national security implications. While such investments can drive innovation and economic growth, they also pose risks, particularly when foreign entities with adversarial ties gain access to sensitive AI technologies and data that could be exploited for military or intelligence purposes. Additionally, economic espionage through foreign investment can undermine the integrity and competitive edge of U.S. firms and lead to the loss of critical technological advancements. Below, we explore these risks in detail, identify potential regulatory gaps that need to be addressed to safeguard national security, and present several policy recommendations.

Foreign Investment in U.S. AI Technology May Pose Risks for National Security and Financial Integrity

Foreign investment in U.S. AI technology can present risks that need to be carefully managed. Of primary concern is the potential for foreign entities with adversarial ties to gain access to sensitive AI technologies and data that could be used for military or intelligence purposes. This could expose the U.S. financial sector to risks such as manipulation of financial markets, more sophisticated financial fraud, cyberattacks, and breaches of sensitive personal data. For example, adversary access to AI algorithms or associated data used in algorithmic trading could facilitate an adversary's ability to disrupt U.S. financial trading systems.[74]

Foreign investment also raises concerns about economic espionage, which can undermine the integrity and competitive advantage of U.S. firms and lead to the loss of critical technological

[73] Feyen. Erik, Jon Frost, Leonardo Gambacorta, et al., 2021.

[74] For a discussion of threats to algorithmic trading systems, see Sytsma, Tobias, James V. Marrone, Anton Shenk, Gabriel Leonard, Lydia Grek, and Joshua Steier, *Technological and Economic Threats to the U.S. Financial System: An Initial Assessment of Growing Risks*, RAND, 2024. As of August 7, 2024: https://www.rand.org/pubs/research_reports/RRA2533-1-v2.html.

innovations. Specific to the financial sector, economic espionage could result in the theft of proprietary trading algorithms, risk management models, or customer data.

Regulatory Gaps for Foreign Investment

The Committee on Foreign Investment in the United States (CFIUS) is authorized to review transactions that may pose national security risks, including foreign investments related to critical technologies and sensitive personal data. Executive Order 14083 directs CFIUS to consider transactions involving artificial intelligence as fundamental to national security and sensitive personal data includes "financial data that could be used to analyze or determine an individual's financial distress or hardship."[75] The intersection of AI and finance is too important for a single adversarial investment to fall through the cracks, but cracks may be widening.

Lawmakers and regulators will need to keep pace with developments in AI technology to ensure CFIUS's mandate is sufficient. In the immediate term, the fast pace and large volume of AI investment—coupled with a number of other demands on the CFIUS caseload—is bound to be placing unprecedented stress on the review regime. Moreover, for those foreign investments not voluntarily disclosed to CFIUS, review teams from multiple member agencies must pour through and analyze the latest investment information to identify potential transactions of concern. And differences in screening regimes among U.S. allies and partners provides adversaries potential channels into U.S. AI technology.

Policy Recommendations for Foreign Investment

Below, we list several recommendations to consider in addressing risks and regulatory gaps discussed above, based on our expertise.

- Work with Congress to support the expansion of CFIUS authority as outlined by the U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, such as extending CFIUS's review scope to cover critical technologies identified by the White House Office of Science and Technology Policy.[76]
- Collaborate with public and private partners to establish safeguards for protecting sensitive personal data, informed by CFIUS findings.
- Ensure CFIUS and its constituent member review teams are adequately resourced to examine foreign investments in AI technology and to proactively identify transactions under CFIUS jurisdiction that have not been voluntarily reported (i.e., "non-notified" transactions).

[75] Executive Order 14083, *Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*, September 15, 2022 (https://www.govinfo.gov/app/details/FR-2022-09-20/2022-20450); 31 C.F.R. 800.241 Sensitive personal data (https://www.ecfr.gov/current/title-31/subtitle-B/chapter-VIII/part-800/subpart-B/section-800.241).

[76] House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*, December 12, 2023 (https://selectcommitteeontheccp.house.gov/media/policy-recommendations/reset-prevent-build-strategy-win-americas-economic-competition-chinese).

- Deepen U.S. Government engagement with allies and partners to ensure the safety of global investments in AI.

We thank you for your time and consideration. We would be happy to meet to discuss further the above points.

Sincerely,

Dr. Jonathan Welburn
Senior Operations Researcher
jwelburn@rand.org

Jim Mignano
Assistant Policy Researcher
jmignano@rand.org

Anujin Nergui
Assistant Policy Researcher
anergui@rand.org

Noreen Clancy
Senior Policy Researcher
clancy@rand.org

Anton Shenk
Research Assistant
ashenk@rand.org

Karishma Patel
Assistant Policy Researcher
karishma@rand.org

Lily Hoak
Assistant
lhoak@rand.org

About This Letter

Justice Policy Program

RAND Social and Economic Well-Being is a division of RAND that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This work was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

Technology and Security Policy Center

RAND Global and Emerging Risks is a division of RAND that delivers rigorous and objective public policy research on the most consequential challenges to civilization and global security. This work was jointly undertaken with the division's Technology and Security Policy Center, which explores how high-consequence, dual-use technologies change the global competition and threat environment, then develops policy and technology options to advance the security of the United States, its allies and partners, and the world. For more information, contact tasp@rand.org.

Funding

This letter in response to a Notice for Information was funded by gifts from RAND supporters.