

Psaros Center for Financial Markets and Policy

GEORGETOWN UNIVERSITY McDonough School of Business

Towards Responsible AI: Examining the *Financial Artificial Intelligence Risk Reduction Act*

Marshall Lux
Visiting Fellow

Rohan Mistry
Research Assistant

*Georgetown University's Psaros Center for
Financial Markets and Policy*

McDonough School of Business

February 2024

In December of 2023, Senator Mark Warner of Virginia (D-VA) and Senator John Kennedy of Louisiana (R-LA) proposed S. 3554, the *Financial Artificial Intelligence Risk Reduction Act*, aimed at regulating the use of artificial intelligence (AI) in the financial markets of the United States.¹ The proposed legislation is intended to mitigate the risks posed to the financial sector by the emerging technology. Technically speaking, there are a variety of definitions of AI, but it can generally be thought of as a set of programs and technologies that enable data analysis that were previously thought to require human intelligence. From portfolio management to lending, AI is uncovering new relationships in large data that would have otherwise been very difficult to discern with human involvement, helping to automate trading decisions to identifying cases of credit card fraud and unauthorized transactions.

The proposed bill has a few key goals and would require multiple federal agencies and regulatory bodies to take action, primarily the Federal Stability Oversight Council (FSOC). The *Financial Artificial Intelligence Risk Reduction Act* would:

- Require FSOC to produce a research report detailing the threats of AI on the stability of the financial system and identify specific gaps in existing regulations and guidance across federal agencies to the aforementioned threats.
- Allow FSOC to make recommendations to close these gaps and disclose appropriate opportunities for the use of AI in financial supervision.
- Mandate FSOC to coordinate financial regulators' responses to AI threats, such as "deepfakes."
- Initiate FSOC proceedings to see member agencies implement necessary changes following the report.
- Call on the Federal and Banking Information Infrastructure Committee to initiate a series of scenario-based tests to determine the effectiveness of defenses against financial market disruption and make recommendations accordingly.
- Amend the Securities and Exchange Act of 1934 to implement harsher penalties when actors use AI to manipulate markets.
- Make clear that anyone who uses an AI model is responsible for ensuring the model operates correctly and would be held liable regardless of intent.

These actions are in line with FSOC's current acknowledgment of the potential threat of AI in financial markets. FSOC, first established in 2010 under the Dodd-Frank Wall Street Reform and Consumer Protection Act with the charge of promoting financial stability and market discipline, identified AI as a critical vulnerability in its 2023 annual report for the first time.² While FSOC notes that AI has the potential to increase efficiency and innovation, "monitoring

¹Warner, Mark R. (2023, December 19). Warner, Kennedy introduce legislation to require financial regulators to respond to AI market threats [Press Release].

<https://www.warner.senate.gov/public/index.cfm/2023/12/warner-kennedy-introduce-legislation-to-require-financial-regulators-to-respond-to-ai-market-threats>

²Croce, B. (2023, December 19). Senators unveil bill targeting AI manipulation in financial markets. *Pensions&Investments*.

<https://www.pionline.com/regulation/ai-manipulation-markets-focus-bill-sens-warner-kennedy>

these rapidly emerging technologies will continue to be increasingly important, given the potential risks³ in the financial system.

Calls for legislation have coincided with such rapid growth in AI. The new technology, if left unchecked, poses threats that include the use of deepfake technology to deceive investors, trading algorithms that allow collusion by traders to manipulate markets, unfair outcomes that harm consumers and investors, information asymmetries that can be taken advantage of, and other issues that come with the evolutionary nature of the space.⁴ Additionally, there are monetary and strategic incentives in place to advance the technology as quickly as possible, spurred on by businesses and governments across the world, to maintain and gain market share in the current landscape of such technology.⁵

Some advocates are concerned that legislation will impede innovation. They believe regulators and policymakers must be aware of the potential consequences of overregulation in this space, as innovation in artificial intelligence is leading to breakthrough services, products, and technology that are helping to improve the quality of life and success of many businesses. Policymakers have often been tasked with tackling guidance surrounding emerging technologies, and while it is important to balance consumer safety with innovation, there is a fine balance in the legislative and regulatory process to prevent stifling innovation. Therefore, legislators and regulators must provide leeway for innovation to occur, while setting limitations in order to protect customers.

Artificial intelligence continues to gain momentum and spread throughout the business world, helping to expedite existing processes and achieve new goals. While the technology has existed for quite a few decades, its widespread use in finance has boomed in the last few years. The growth, accelerated by the COVID-19 pandemic, has been fueled by an abundance of available data and increased, more affordable computing capacity. For firms, AI is deployed in finance to drive competitive advantages and improve efficiency through cost reduction and productivity enhancement.⁶ The largest financial firms recognize the power of AI. BlackRock heavily invests in BlackRock Systematic, an earnings call model that uses AI technology to predict post-earnings market reactions based on the language used in an earnings call with over 60% accuracy.⁷ Similarly, JP Morgan spends more than \$15 billion a year on technology, part of which involves an AI research team focused on prospecting, marketing, and research. Globally,

³ Financial Stability Oversight Council. (2023). *Annual report 2023*. FSOC.

<https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf>

⁴ Croce, B. (2023, December 15). AI poses risks to U.S. economy, Financial Stability Oversight Council says. *Pensions&Investments*.

<https://www.pionline.com/regulation/ai-poses-risks-us-economy-financial-stability-oversight-council-says>

⁵ Bremmer, I., & Suleyman, M. (December 2023). Building blocks for AI governance. *International Monetary Fund*. <https://www.imf.org/en/Publications/fandd/issues/2023/12/POV-building-blocks-for-AI-governance-Bremmer-Suleyman>

⁶ Organization for Economic Cooperation and Development. (2023). *Artificial intelligence, machine learning and big data in finance: opportunities, challenges, and implications for policy makers*. OECD.

<https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf>

⁷ Savi, R., Shen, J., & Tsaig, Y. (2023, June 15). How AI is transforming investing. *BlackRock*.

<https://www.blackrock.com/us/individual/insights/ai-investing>

spending on AI is expected to exceed \$301 billion by 2026, resulting in a roughly 26.5% 5-year compound annual growth rate.⁸

One of the key attributes of artificial intelligence is its ability to learn and adapt without the intervention of humans. Regulation, as it stands today, is written on the assumption that it is people who make decisions, not machines.⁹ Such a mismatch begs the question of who is accountable when things go wrong. The potential danger of AI on financial markets comes from bad actors hoping to leverage AI to manipulate markets and automated algorithms that are designed to maximize profit. Research finds that a trading algorithm can manipulate prices and create collusive strategies to allow for supra-competitive trading profits.¹⁰ One study even finds that, through an advanced algorithm, the AI trader discovered market manipulation as an optimal investing strategy.¹¹ These problems illustrate one of the largest questions policymakers need to address: how should regulation deal with the mismatch between the intended outcome and what actually occurs?

Trading algorithms are not the only form of market manipulation done by AI. Deepfakes are AI-generated media that depict made-up events, often very realistically.¹² Utilizing deep learning technology, deepfakes often come in the form of highly believable and realistic pictures, face-swaps, or voice-cloning (copies of a person's unique vocal patterns to digitally recreate new audio using the person's voice). In May 2023, an ominous AI-generated image of black smoke flowing out of a government building near the Pentagon spread rapidly across social media. The image set off investor fears, declining the S&P 500 by 0.3% to a session low. While experts quickly dismissed the picture and markets recovered, the instance exploited the vulnerabilities the financial systems face from AI.

Furthermore, a cause of extreme caution is AI-powered models' explainability, as it can be a challenge to understand and articulate the decisions made by models.¹³ Often, these models are described as "black box"¹⁴ technology, meaning it is difficult or not possible to observe the specific reasons the model made each decision. Implementing analysis from AI models without

⁸Jyoti, R. & Kuppaswamy, R. (2023). *Create more business value from your organizational data*. IDC Research, Inc. <https://content.dataiku.com/idc-infobrief-2023>

⁹Smith, D. (2023, September 21). Senate testimony: AI risks to the financial sector. *University of Michigan*. <https://news.umich.edu/senate-testimony-ai-risks-to-the-financial-sector/>

¹⁰Parameshwaram, S. (2023, November 10). How AI-powered collusion in stock trading could hurt price formation. *Knowledge at Wharton*. <https://knowledge.wharton.upenn.edu/article/how-ai-powered-collusion-in-stock-trading-could-hurt-price-formation/>

¹¹Mizuta, T. (2020). Can an AI perform market manipulation at its own discretion? - A genetic algorithm learns an artificial market simulation. *2020 IEEE Symposium Series on Computational Intelligence, Australia*, 407-412. <https://doi.org/10.1109/SSCI47803.2020.9308349>

¹²Bateman, J. (2020, July 8). Deepfakes and synthetic media in the financial system: assessing threat scenarios. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237>

¹³Organization for Economic Cooperation and Development. (2023). *Artificial intelligence, machine learning and big data in finance: opportunities, challenges, and implications for policy makers*. OECD. <https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf>

¹⁴Blouin, L. (2023, March 6). AI's mysterious 'black box' problem, explained. *University of Michigan*. <https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained>

due diligence could potentially allow companies not to adhere to the internal governance, risk management, and controls put in place to maintain an ethical business. This opens the door for issues¹⁵ that are undetectable from the individuals constructing the model and thus cannot be adequately addressed, looping back to the question of accountability previously mentioned. There are a myriad of issues with black-box technology: faulty decision-making, biases that lead to inaccurate choices, neglected privacy risks, and missteps regarding adherence to legislation.

Additionally, a key aspect of artificial intelligence and AI-powered decision-making is the necessity of enormous amounts of data that must be gathered to train such decision-making models.¹⁶ This demands that data security and privacy should top the list of risks that need to be addressed by a financial institution adopting AI. Without ensuring proper measures, the inference capabilities of AI-powered technology could expose the model to sensitive and private information, which could be used to power its decision-making, even without such information explicitly being supplied. Private information such as location, personal habits, and more could be inferred and used by algorithms during their strategy to achieve maximum profits, questioning the relationship between individuals and financial institutions. This critical issue is further emphasized given that the intricacy of an AI algorithm could render itself vulnerable to malicious third parties. Such use of data could result in significant financial and reputational damage. In the status quo, multiple coalitions of major companies attempt to address the ethical concerns around digital privacy and AI, such as Partnership on AI (PAI) or the IEEE Global Initiative on Ethics of Autonomous and Intelligence Systems.

There has been a heightened awareness of the need for artificial intelligence legislation across the United States in recent years. At the federal level, President Biden signed an Executive Order in October 2023 on the “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”¹⁷ The Executive Order is a broad approach that addresses the future development of AI must be secure, adhere to major principles of American society, and consider relevant stakeholder views. Other legislation includes targeted acts to promote U.S. leadership in AI research, protect national security, address the impact on workers, and leverage AI in federal work.¹⁸ On a local level, in 2023, ten states included legislation on the technology in consumer privacy laws. Many of them enacted legislation restricting the use of such technology in insurance hiring and government spheres, setting up task forces to investigate its use across other

¹⁵ Albinson, N., Thomas, C., Rohrig, M., & Chu, Y. (2019). *Future of risk in the digital era*. Deloitte. <https://www2.deloitte.com/us/en/pages/advisory/articles/black-box-artificial-intelligence.html>

¹⁶ Sher, G. & Benchlouch, A. (2023, October 31). The privacy paradox with AI. *Reuters*. <https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/#:~:text=The%20technology's%20potential%20to%20infer.that%20demand%20immediate%20proactive%20solutions>.

¹⁷ United States Whitehouse. (2023, October 30). *Executive order on the safe, secure and trustworthy development and use of artificial intelligence* (E.O. 14110). United States Government. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

¹⁸ Covington Alert. (2023, October 20). U.S. Artificial intelligence policy: legislative and regulatory developments. *Covington and Burlington LLP*. <https://www.cov.com/en/news-and-insights/insights/2023/10/us-artificial-intelligence-policy-legislative-and-regulatory-developments#:~:text=Targeted%20legislation%20introduced%20so%20far,government%20leverage%20AI%20to%20deliver>

services and businesses. However, there is still a lack of emerging consensus on the future of AI policy, particularly governing its use in financial markets in any state, justifying the proposition of the *Financial Artificial Intelligence Risk Reduction Act*.¹⁹

In context, this bill arrives at a time when policymakers continue their attempt to be cognizant of evolving technology and products, enacting legislation and regulation as appropriate. However, some of these actions can only be taken after the innovations occur, leaving a window of time where the rules might not be clear. As policymakers navigate new terrain, they must be wary of the potential consequences of legislation and, if passed, its regulatory implementation. To avoid suppressing the benefits of artificial intelligence, legislators and regulators must strike the proper balance between control and freedom. At the same token, legislators must also avoid their own regulatory mismatch: not specifying an underlying issue can cause a disconnect between legislation and substantive change.²⁰ The dichotomy between intention and outcome is a key issue that must be addressed to ensure the proper functioning of markets and avoid costly problems resulting from unintended AI-powered decisions. The *Financial Artificial Intelligence Risk Reduction Act* paves the way for a thorough framework to identify risk while allowing flexibility to account for future innovations. Of course, while the risks of artificial intelligence can be mitigated, whether the risks be digitally manipulated videos made by malicious actors or stability-threatening advanced trading algorithms, politicians must continuously be aware of the thin line that divides powerful innovation and threatening dangers in an increasingly technologically advanced globe.

About the Georgetown Psaros Center for Financial Markets and Policy

The Georgetown Psaros Center for Financial Markets and Policy is the preeminent destination for unbiased expertise at the intersection of finance and policy. The Psaros Center provides thought leadership and actively contributes to shaping global finance. Located in Washington D.C., we connect policymakers, industry leaders, and scholars through solutions-driven platforms.

Housed at Georgetown University's McDonough School of Business, the Psaros Center for Financial Markets and Policy serves as an impartial, academic-based research center. The Psaros Center integrates practice with policy: facilitating a forum for solutions-oriented discussion, conducting relevant and original research on key global market issues, and engaging students interested in the nexus of finance and policy. Collectively, our efforts impact policy and practice by informing current industry professionals, the next generation of finance and policy leaders, and the world, to create meaningful change.

Psaros Center for Financial Markets and Policy

GEORGETOWN UNIVERSITY McDonough School of Business

¹⁹Zhu, K. (2023, August 3). The state of state AI laws: 2023. *Electronic Privacy Information Center*. <https://epic.org/the-state-of-state-ai-laws-2023/>

²⁰ Ho, D. (2024). *AI regulation has its own alignment problem: the technical and institutional feasibility of disclosure, registration, licensing, and auditing*, *The George Washington Law Review* (forthcoming 2024). https://dho.stanford.edu/wp-content/uploads/AI_Regulation.pdf