Sandbox or Quicksand

The Perils of AI Exemptions from Federal Financial Laws

August

2026

Table of Contents

About

Americans for Financial Reform (AFR) is an independent, nonprofit organization founded by a coalition of more than 200 civil rights, community-based, consumer, labor, small business, investor, faith-based, civic groups, and individual experts. We fight for a fair and just financial system that contributes to shared prosperity for all families and communities.

Sandbox or Quicksand: The Perils of AI Exemptions from Federal Financial Laws was written by Patrick Woodall and published August 2026.

Overview

The House and Senate are both considering legislation to create broad exemptions from federal laws and regulations for the use of artificial intelligence (AI) by regulated financial firms.[1] It creates an incentive for firms to deploy risky AI systems in order to secure waivers from federal financial protections, including civil rights, consumer protection, and financial stability laws and regulations.

If it becomes law, this AI sandbox legislation will significantly increase the risk of harm from the deployment of AI in financial services, both to individual consumers and investors and to financial stability. AI creates new risks, and its use should be governed by rules that protect the public interest. This legislation does the exact opposite; it makes AI a reason to reduce accountability and provides a kind of subsidy to the use of AI in the form of regulatory waivers.

The legislation provides a path for firms to deploy AI without having to follow existing rules and laws, and an incentive for firms to use AI *in order* to secure exceptions. Practices that would be unlawful if initiated by a person would become permissible if performed by AI systems. It would let financial firms off the hook for wrongdoing merely by the virtue of using AI and let the firms capture all the benefits of AI and force the public to bear all of the risks.

The deployment of AI in finance without stepped up oversight already presents serious risks to household finances and to the stability of the financial system. AI systems can expose people to increasingly sophisticated and costly financial fraud, amplify racial disparities in access to sustainable credit and financial services, and pose significant risks to people's sensitive personal financial information. Financial firms use of AI in automated trading, risk management, and asset allocation creates serious risks of hyperinflating market bubbles, exacerbating and obscuring safety and soundness problems, and exposing institutions and their customers to cybersecurity dangers.[2]

This legislation rolls back oversight and multiplies these dangers.

---

[1] The Unleashing AI Innovation in Financial Services Act H.R. 4801 (as amended) was passed by the House Financial Services Committee June 24, 2026. A companion measure was included in §10509 of the final negotiated Senate version of Digital Market Clarity Act H.R. 3633 introduced July 22, 2026.

[2] The impact of AI on cybersecurity in financial services is increasingly worrisome as new models are developed and released. Azhar, Saeed. "Bessent, Powell warned bank CEOs about Anthropic model risks, sources say." *Reuters*. April 2026; Mozur, Paul, Adam Satariano. "Anthropic's New A.I. Model Sets Off Global Alarms," *New York Times*. April 2026.

The dangerous mechanism of the AI sandbox

The legislation encourages regulated financial firms to request—and regulators to approve—broad brush exemptions from federal laws and regulations. The legislation is designed to rubber-stamp highly risky AI test projects. The few guardrails that the bill contains are window dressing that obscure the lack of meaningful protections for people or the economy. The combination would make it nearly impossible to protect people or the economy from the harms of unregulated deployment of AI in financial services.

The stated purpose of the legislation is to "enable regulated entities to experiment with AI test projects without unnecessary or unduly burdensome regulations or expectation of enforcement actions." Financial companies can apply for exemptions from the rules under an extremely vague set of criteria, and regulators are required to approve any projects that are "more likely than not" to meet the guidelines. Together these remarkably loose standards would rapidly allow the deployment of risky AI projects. The legislation does not require compliance with core federal civil rights obligations—including fair lending and community reinvestment requirements—despite the well-documented racial and other biases of AI systems.[3] It makes only passing and wholly inadequate nods to consumer protection (primarily weak fraud language) and financial stability (similarly weak safety and soundness language). Nor does it require companies to disclose the use of AI to their customers, disclose what personal data is collected or used, or provide an opportunity for customers to opt-out of AI test projects.

Practices that would be unlawful if initiated by a person would become permissible if performed by AI systems.

These problems are compounded by the black-box nature of AI systems and their

[3] West, Sarah Myers, Meredith Whittaker, and Kate Crawford. AI Now Institute. "Discriminating Systems: Gender, Race, and Power in AI." April 2019; Leavy, Susan, Barry O'Sullivan, and Eugenia Siapera. "Data, Power and Bias in Artificial Intelligence." *AI for Social Good Workshop*. 2020; Chandler, Anupam. "The racist algorithm?" *University of Michigan Law Review*. Vol. 115, Iss. 6. 2017; Ferrara, Emilio. "Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies." *Sci*. Vol. 6, No. 3. 2024; Lloyd, Kirsten. Booz Allen Hamilton. "Bias Amplification in Artificial Intelligence Systems." Association for the Advancement of Artificial Intelligence Fall Symposium Series. 2018.

evolving and changing models.[4] Financial firms that deploy off-the-shelf AI systems may not fully understand what data elements the AI uses, how the AI evaluates the data inputs, and how these inputs are weighted to generate an output. Since machine learning AI models are designed to adapt as they assess inputs and outputs, it is hard for firms to know how the models operate over time. The legislation lacks any ongoing testing and auditing to determine whether an AI test project continues to operate as intended and does not develop emerging risks to the firm, people, or the financial system, especially related to racial bias in AI decision making.

The danger of this legislation is multiplied by the current crop of pro-AI, anti-regulation people leading financial regulatory agencies in the Trump administration. The legislation leaves most of the critical application and approval components up to the Trump appointed regulators that are either deeply conflicted or overly deferential to the AI and finance industries that will expose people to financial harms and fraud and imperil economic stability.

This policy brief describes the many shortcomings of the AI sandbox legislation including that it rubber-stamps the regulatory approval of risky and deregulatory AI test projects (Section I); that it exposes people to harms and risks with wholly inadequate safeguards against fraud, abusive practices, and racial discrimination (Section II); that it has inadequate protections to safeguard financial stability (Section III); that it contains overly broad parameters for AI test projects that could receive regulatory waivers (Section IV); that the applications offers gauzy guidelines instead of standards necessary to evaluate AI test projects that incentivizes even the riskiest pursuits (Section V); and that the application omits key elements necessary to evaluate any AI test project (Section VI).

I. Sandbox bill rubber stamps waivers; companies pick their own deregulation

The legislation allows companies to apply for broad waivers to regulatory supervision and enforcement, propose alternatives to current regulations and regulatory oversight, and requires regulators to approve almost all of the regulatory immunity proposals.[5]

[4] *See* Pasquale, Frank. *The Black Box Society: The Secret Algorithms Behind Money and Information*. 2015. (Cambridge, MA: Harvard University Press); O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. 2016. (New York: Broadway Books).
[5] The current House version has a few, very modest changes that were not included in the legislation the Senate added to the crypto legislation. The House version modified a provision that excluded the CFPB from overseeing AI test projects by banks (now the CFPB has the same pitifully weak oversight as other regulators); it added language

Financial firms are already deploying AI within the bounds of federal financial law across their business lines from customer service to credit scoring to automated underwriting to securities trading to risk management and more. Multiple existing laws are intended to protect consumers, investors, and the financial system from discrimination, predatory practices, market manipulation, and financial instability. There is no reason to waive these protections to hasten the risky deployment of AI without the safeguards that protect people and the economy.

The legislation would prevent regulators from enforcing federal laws or regulations for AI test projects except for the alternative compliance strategy proposed by the company. This pick your own deregulatory adventure policy will expose consumers, investors, and the financial system to substantial risks and harms that would be prohibited under current law.

Companies could request broad exemptions, allowing them to choose how they are regulated: The legislation does not limit the scope of supervisory or enforcement exemptions. It allows companies to identify regulations that they want to be waived or modified and an "alternative method" for compliance, with no limitation on the alternative method or waiver.[6] Companies could request total exemption from consumer protection, fair lending, risk management and capital requirements, investor protection, market integrity, or other federal statutes and regulations. Alternative compliance strategies could range from total immunity for non-compliance or very modest supervisory oversight, such as notification for violations without requirements for remediation. This lets companies determine how they are regulated because the approval of applications would constrain regulators to the specified alternative compliance strategies.

It requires presumptive approval of risky AI test projects: The legislation requires agencies to approve AI test projects if "it is more likely than not that the application meets the requirements for establishing an alternative compliance strategy and satisfies the standards."[7] The legislation provides descriptive

---

that acknowledged the cybersecurity risks from AI (without meaningful tools to make sure the AI test projects are cybersecure); and it allows regulators to promulgate rules to consider customers personal and sensitive information if "appropriate" (although the company data is protected in the legislation and the administration regulators are not obligated to promulgate strong privacy protecting rules).

[6] H.R. 4801 §4(a)(2)(A)(ii)(B)-(C); Clarity Act §10509(b)(1)(B)(i)(II)(bb).

[7] H.R. 4801 §4(a)(7)(B)(i); Clarity Act §10509(b)(1)(B)(ii)(II)(aa).

guidelines rather than standards (see below), but this language would even require regulators to approve applications that *probably* met the application guidelines but posed real risks of failing to meet even these weak guidelines. This is an especially permissive and dangerous standard for AI test projects that will change and evolve as the models operate, meaning the likelihood that a test project will meet the legislative conditions could decline substantially over time.

The legislation provides a path for firms to deploy AI without having to follow existing rules and laws, and an incentive for firms to use AI *in order* to secure exemptions.

It prohibits enforcement except under the company's own alternative compliance strategy:

Regulators are prohibited from enforcing federal statutes and regulations except under the alternative compliance strategy proposed by the companies that the regulators approve.[8] This narrow oversight would significantly constrain regulatory oversight and supervision and could allow AI risks and harms to people or the economy to build with little intervention or accountability. The legislation's emergency injunctive relief powers are too constrained to prevent an AI test project from failing spectacularly and/or manifesting unanticipated violations of federal financial statutes or regulations (see below).

It does not give regulators authority to impose needed limitations on AI test projects:

The regulators should be able to impose performance conditions on proposed AI test projects that identify risks of the proposal to consumers, financial institutions, or the financial system and require the applicants to prevent those risks or expeditiously terminate the project if it fails to prevent those risks. There are no provisions for ongoing supervision of AI test projects (and companies could request and agencies could approve alternative compliance strategies that excluded supervision). The legislation requires regulators that approve AI test projects to notify applicants the terms or the alternative compliance strategy, the termination date of the project, and any limitations on the size, scope, or growth of the project, or any other

[8] H.R. 4801 §4(a)(7)(B)(ii)(I); Clarity Act §10509(b)(1)(B)(ii)(II)(bb)(AA).

limitations, but most of these are elements included in the application itself and this provision merely codifies the approval of the project.[9] The addition of "any other limitations or conditions" does not provide meaningful conditions or limitations on risky AI test projects.[10] The legislation does not include a range of appropriate conditions on the proposed alternative compliance strategy or the proposed AI test project that can be imposed on applicants, especially including a termination "kill-switch" requirement for AI test projects that fail to prevent prescribed risks.

II. Sandbox bill poses extreme risks without safeguards against abuse or discrimination

Consumers and investors face real risks from AI used by financial firms, including well-documented biases in accessing affordable credit. AI systems can push market unsuitable, high-priced, predatory, or unfair products or services to unwary customers.[11] AI-powered debt collection can expose people to abusive collection tactics and disproportionately target people of color for collection lawsuits.[12] Automated fraud detection and identity matching can subject people to unfair account freezes and closures.[13] AI-powered customer service chatbots can provide incorrect or misleading answers to complex questions, trap people in customer service doom-loops, and consumer fraud fueled by AI has become an increasing problem for consumers throughout the financial industry.[14]

---

[9] §4(a)(2)(D)-(E); Clarity Act §10509(b)(1)(B)(i)(II)(dd)-(ee).

[10] H.R. 4801 §4(a)(7)(B)(i)(V)); Clarity Act §10509(b)(1)(B)(ii)(II)(aa)(EE).

[11] Evans, Carol A. and Westra Miller. "From catalogs to clicks: The fair lending implications of targeted, internet marketing." *Consumer Compliance Outlook*. Iss. 3. 2019 at 4; Ali, Muhammad et al. "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes." *Proceedings of the ACM on Human-Computer Optimization*. Vol. 3, No. CSCW. Art. 199. November 2019; Datta, Amit, Michael Carl Tshantz, and Anupam Datta. Carnegie Mellon University and International Computer Science Institute at University of California Berkeley. "Automated Experiments on Ad Privacy Settings." March 18, 2015.

[12] Knibbs, Kate. "AI is taking over the most cursed job in the world." *Wired*. May 26, 2026; Carns, Ann. "Debt collection lawsuits are rising. Here's what to do to fight back." *New York Times*. September 12, 2025; National Consumer Law Center. Response to U.S. Department of Treasury Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector. August 12, 2025 at 24 to 31.

[13] Marks, Oliver. "Revolut's clumsy automated FinTech bank compliance results in frozen accounts and lack of customer service." *ZDNet*. January 6, 2019; Monroe, Teri. "7 ways bank accounts are being frozen for seniors in 2026." *Saving Advice*. February 4, 2026.

[14] Consumer Financial Protection Bureau. Issue Spotlight. "Chatbots in Consumer Finance." June 2023; SailPoint. "AI Agents: The New Attack Surface." 2025.

It does not address well-documented racial biases in AI credit determinations: Many studies have documented that AI enabled underwriting and decision-making systems amplify existing racial disparities in the approval, pricing, and terms of loans, including mortgages, credit cards, student loans, and more that harm Black, Latine, Indigenous, and other people of color and people with disabilities.[15] The legislation does not make any reference to requiring AI systems to adhere to core civil rights, fair lending, or community reinvestment statutory or regulatory requirements.

It does not include any meaningful privacy protection for customers: The House legislation lacks any meaningful privacy or personal data protection for customers. The legislation would allow regulators to promulgate rules "as appropriate" on "the confidentiality, security, and privacy of information."[16] The Senate version does not include *any* privacy protection provisions. Data is the fuel for AI models, but the collection, aggregation, commodification, and algorithmic output models expose people's sensitive personal data. AI systems can also expose and share sensitive personal and financial information.[17] The legislation does not require companies to disclose the collection of customer data, disclose what data elements are collected, limit data collection from customers, limit the sharing or commercializing data collected from customers, provide any data rights to remedy errors or

The legislation is designed to rubber-stamp highly risky AI test projects. The few guardrails are window dressing that obscure the lack of meaningful protections for people or the economy.

[15] Johnson, Kristen, Frank Pasquale, and Jennifer Chapman. "Artificial intelligence, machine learning, and bias and finance: Toward responsible innovation." *Fordham Law Review*. Vol. 88, No. 499. 2019; Bowen III, Donald E. et al. Lehigh University and Babson College. "Measuring and Mitigating Racial Disparities in LLMs: Evidence from a Mortgage Underwriting Experiment." August 1, 2025; Protect Borrowers. "Educational Redlining." February 2020; Fuster, Andreas et al. "Predictably unequal? The effects of machine learning on credit markets." *Journal of Finance*. Vol. 77, No. 1. February 2022; Martinez, Emmanuel and Lauren Kirchner. "The secret bias hidden in mortgage-approval algorithms." *Associated Press*. August 25, 2021.
[16] H.R. 4801 §4(a)(9)(B)(vii).
[17] SailPoint. "AI Agents: The New Attack Surface." 2025.

opt out provisions for data collected by the AI test projects. The legislation *does* mandate data security for the financial companies' submissions to the regulators, but does not establish statutory protections for people's data.[18]

It does not provide adequate protections for consumers from known AI harms:

There is virtually nothing in the legislation that addresses the substantial harms consumers face from AI deployment in financial services. Automated credit determinations can push people into more expensive loans than they qualify for, deny them credit unfairly, or impose unfair loan terms.[19] AI-powered debt collection can expose people to abusive collection tactics and disproportionately target people of color for collection lawsuits. Automated fraud detection and identity matching can subject people to unfair account freezes and closures if the match is incorrect. AI-powered customer service chatbots and agentic AI can provide incorrect or misleading answers to complex questions, execute unauthorized transactions, and exacerbate consumer fraud fueled by AI, which has become an increasing problem for consumers throughout the financial industry.[20] The legislation provides no remedies for consumers harmed by errors or model failures, or require ongoing reporting to assess evolving machine learning systems.

Its injunctive relief provision fails to provide adequate regulatory enforcement or oversight:

The legislation allows — but does not require — regulators to sue to enjoin AI test projects that present "immediate danger to consumers or investors" but this language by itself cannot protect consumers or investors from AI risks.[21] This injunctive relief is highly constrained and wrapped in nebulous language (and again appears to exclude civil rights and fair lending protections). It is unclear what "immediate danger to consumers or investors" even means. It is a phrase that only exists in this legislation — it is not in other federal financial, consumer financial protection, or civil rights laws. Regulators could not provide timely protection from an immediate danger through a lawsuit, since immediate danger could be built into the AI model or only a mouse click or phone tap away.

[18] H.R. 4801 §4(a)(8); Clarity Act §10509(b)(1)(B)(iii).
[19] Chopra, Rohit. Consumer Financial Protection Bureau. "Director Chopra's Prepared Remarks on the Interagency Enforcement Policy Statement on 'Artificial Intelligence.'" April 25, 2023;
[20] FinRegLab. "The Next Wave Arrives: Agentic AI in Financial Services. September 2025 at 18 to 19.
[21] H.R. 4801§4(a)(7)(C)(iii)(I); Clarity Act §10509(b)(1)(B)(ii)(III)(cc).

The AI sandbox bill bestows a get out of jail free card to discriminatory, predatory, unfair, and risky practices by regulated financial firms.

And regulators would lack sufficient information to know that there were immediate dangers or intervene if the alternative compliance strategy excluded supervision (which they almost undoubtedly would). Importantly, the alternative compliance strategies could grant waivers from the very laws and regulations designed to *prevent* immediate danger from occurring in the first place. Even if an agency determines there is an "immediate danger" to consumers or investors, the agency could not rescind a waiver without seeking a court order. By the time they get the court order the harm will be widespread and likely irreversible given the speed of the technology.

It only grants authority to confront "unmitigable or irreparable" harms, which is too late:

The House legislation *only* allows agencies to issue cease and desist orders to AI test projects that are "causing unmitigable or irreparable harm to consumers, investors."[22] By the time an AI test project has caused unmitigable or irreparable harm, it is already too late, the harm is done and unfixable. Ongoing examination and supervision are intended to prevent companies from allowing practices or governance lapses that can harm people. The legislation can only stop the worst AI abuses after they have already harmed people irreparably. This language is also a rule of construction. (The Senate version does not have any cease-and-desist order provision.)

It makes inadequate protections against fraud and safety and soundness:

Although the legislation notes that it does not limit regulatory authority to take enforcement actions against fraud, market manipulation, or unsafe or unsound activities,[23] the alternative compliance strategies could make it difficult or impossible for regulators to detect, prevent, or enforce against either fraud. AI test projects that promoted digital payment platforms could easily subject customers to fraudulent

---

[22] H.R. 4801 §4(a)(7)(C)(iv).
[23] H.R. 4801 §4(a)(7)(F); Clarity Act §10509(b)(1)(B)(ii)(II)(dd).

transactions (this administration has already withdrawn several enforcement actions against widespread fraud on payment apps).[24] Those kinds of well-known frauds would not be covered by this provision which only covers the AI test project itself (so if the test project defrauded a consumer of an entity with an AI test project, it might be covered, but if the entity's AI test project facilitated fraud it would likely not be covered). AI test projects that managed asset allocation, performed institutional trading, or performed risk management activities could undermine safety and soundness, but it would be difficult for regulators to determine the impact of these AI driven decisions until the regulated institution faced financial trouble or economic stress.

III. Sandbox bill has inadequate protections for financial stability

AI can exacerbate risks to investor protection, market integrity, and financial stability. AI-powered high-speed trading can manipulate markets and harm investors.[25] Banks that rely on opaque black-box AI risk management models may substantially underestimate risks, similar to the presumption that subprime mortgages posed little risk to the financial system prior to the financial crisis.[26] And the small number of AI firms providing services to the financial sector can exacerbate fragility and instability if the widespread use of only a few models drives the industry to pursue correlated and self-reinforcing business strategies that can create unstable asset bubbles and crashes.[27]

---

[24] Comptroller Hsu, Michael J. Office of the Comptroller of the Currency. "Remarks in Support of the 2024 Conference on Artificial Intelligence and Financial Stability 'AI Tools, Weapons, and Accountability: A Financial Stability Perspective.'" June 6, 2024 at 6; Son, Hugh. "CFPB drops lawsuit against JPMorgan Chase, Bank of America and Wells Fargo over Zelle fraud." *CNBC*. March 4, 2025.
[25] Mizuta, Takanobu. SPARX Asset Management Co. LLC. "Does an Artificial Intelligence Perform Market Manipulation With Its Own Discretion? A Genetic Algorithm Learns in an Artificial Market Simulation." IEEE Symposium Series on Computational Intelligence, Computational Intelligence for Financial Engineering and Economics (CIFEr). May 21, 2020; Gensler, Gary, and Lily Bailey. Massachusetts Institute of Technology. "Deep Learning and Financial Stability." November 13, 2020; U.S. Securities and Exchange Commission. Staff Report on Algorithmic Trading in U.S. Capital Markets. 2020; Busch, Danny. "MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct market access." *Law and Financial Markets Review*. Vol. 10, Iss. 2. 2016.
[26] Danielsson, Jon, Robert Macrae, and Andreas Uthermann.. "Artificial Intelligence and Systemic Risk." *Journal of Banking and Finance*. Vol. 140. July 2022; Financial Stability Board. "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications." November 1, 2017.
[27] Lin, Tom C. W. "The New Market Manipulation." *Emory Law Journal*. Vol. 66. July 2017.

Application requires only passing consideration of systemic risk and money laundering:

The legislation requires companies to attest that the waiver for AI test project would not pose systemic financial risk, undermine anti-money laundering compliance, or present a "significant risk of loss" to the FDIC deposit insurance fund, but it provides no specificity as to the evaluation standards for these critical considerations.[28] The presumption appears to be that any application will not pose systemic risk, undermine anti-money laundering compliance, or risk deposit insurance solvency.

Its administrative authority doesn't pretend to protect financial stability until after it is too late:

The legislation *only* allows agencies to issue cease and desist orders to AI test projects that are "causing unmitigable or irreparable harm to financial stability."[29] This means that AI test projects are free to not just risk financial stability but *cause* irreparable harm to the financial system before regulators can step in and order the AI test to stop. (The Senate legislation does not include this cease-and-desist order language.)

Its injunctive relief provision to protect the financial system provides inadequate authority:

The legislation allows — but does not require — regulators to seek injunctive relief to AI test projects that "presents a risk" to financial markets, the FDIC DIF, or violating anti-money laundering. This provides very little actual remedy (even if regulators chose to exercise this provision).[30] The legislation acknowledges that AI test projects can present a risk to the financial markets and financial system, but it requires regulators to approve test projects as long as "it is more likely than not" that the project will not present systemic risk to the financial system or violate anti-money laundering statutes. This tension between these two provisions makes it nearly impossible for regulators to exercise injunctive relief to present risks that have already been acknowledged in approved test projects that *probably* do not present risks to financial stability, FDIC deposit insurance solvency, or money laundering.

---

[28] H.R. 4801 §4(a)(2)(C)(iii)-(iv); Clarity Act §10509(b)(1)(B)(ii)(III)(cc)(AA)-(CC).
[29] H.R. 4801 §4(a)(7)(C)(iv).
[30] H.R. 4801 §4(a)(7)(C)(iii)(II); Clarity Act §10509(b)(1)(B)(ii)(III)(cc).

Its safety and soundness enforcement authority lacks teeth needed to prevent dangerous risks:

The legislation notes that it does not limit regulatory authority to take enforcement actions against unsafe or unsound activities, but the alternative compliance strategies would make it difficult or impossible for regulators to detect or prevent AI models or practices that undermine safety and soundness.[31] Alternative compliance strategies are likely to preclude the kinds of supervision or examination necessary to evaluate emerging risks to safety and soundness.

IV. The sandbox bill grants overly broad parameters for AI test projects

The legislation allows regulated financial firms to apply for regulatory waivers for AI test projects, but there are few limits on the parameters for test projects that could expose consumers, investors, and the financial system at risk.

Broad test project definition can provide amnesty to peripheral AI use and algorithmic modeling:

The AI test project must make "substantial use of AI," but substantial is not defined and could allow products or services with less central AI components to be excluded from regulatory oversight.[32] The legislation's AI definition incorporates the broad existing federal law that is a "machine-based system" that makes "predictions, recommendations, or decisions" that use models and automated decision making.[33] This includes much of the current AI deployment in the financial industry (like credit scoring and automated underwriting) which should currently be complying with federal law. The legislation would allow these existing algorithmic models to receive exemptions from federal laws and regulations that they currently follow.

It does not limit the time, size, scope, or expansion of AI test projects:

The legislation lets the companies set

[31] H.R. 4801 §4(a)(7)(F); Clarity Act §10509(b)(1)(B)(ii)(II)(dd).
[32] H.R. 4801 §2(1)(B) and §2(3); Clarity Act §10509(a)(1)(A) and §10509(a)(3).
[33] 15 USC §9401(3).

all the parameters for AI test projects,[34] including the size, scope, and growth of the projects as well as the termination date (they must be at least one year and can be extended but potentially applicants could request decade-long or even permanent regulatory waivers for AI test projects.[35] This lets companies propose overly broad applications — including test projects that expand over time posing unknown future risk — without any limiting parameters whatsoever.

V. Test project application has gauzy guidelines instead of real standards

The application guidelines the agencies are supposed to use to evaluate applications for regulatory waivers are unduly broad, descriptive, and skewed to facilitate the approval of regulatory waivers for AI test project.

It establishes loose waiver eligibility guidelines not standards for AI test projects: The legislation requires companies to describe the proposed AI test project, the alternate compliance strategy to waive or modify an identified regulation, why waivers are essential to the company's operation, and how it would effectively manage risks from the AI test project. These are loose descriptive guidelines and not binding standards with performance metrics that would require companies to demonstrate that the project would not pose risks to consumers, the companies, or the financial system.[36] The legislation requires regulators to approve AI test projects that "satisfies the standards," but companies can easily satisfy these "standards" by merely describing their project.[37] The legislation's presumptive approval makes it difficult for regulators to object to proposals that provide simple narratives irrespective of their potential risks.

It does not require companies to justify the need for regulatory or enforcement waivers: The legislation

[34] H.R. 4801 §4(a)(2)(A)(ii)(IV)-(V); Clarity Act §10509(b)(1)(B)(i)(II)(dd)-(ee).
[35] H.R. 4801 §3(a)(2)(D)(i)(III)-(VI); Clarity Act §10509(b)(1)(B)(iv)(cc)-(dd).
[36] H.R. 4801 §4(a)(2)(C); Clarity Act §10509(b)(1)(B)(i)(II)(cc).
[37] H.R. 4801 §4(a)(7)(B)(i); Clarity Act §10509(b)(1)(B)(ii)(II)(aa).

presumes that federal statutes and regulations are "unnecessary or unduly burdensome" and these rules and the expectation of enforcement actions are impeding the deployment of AI.[38] It does not require applicants to identify how each specific statute and regulation impedes their use of AI. Companies need to state how the proposed alternative compliance method "is essential to the operation" of the company,[39] allowing them to merely state that the cost of compliance is essential to the operation without any consideration of the benefits of regulatory safeguards to their customers, the financial system, or the public. Many regulated financial companies are already deploying AI and complying with federal financial statutes and regulations without this sandbox legislation.

Application tilted to promote purported benefits of regulatory waivers for AI test project:

The legislation requires companies to explain how waivers for AI test projects would be beneficial, but it reads like a pitch deck for AI promoters.[40] Applicants are directed to describe the increased efficiency, increased innovation and competitiveness, improved risk management, or improved regulatory compliance under the test project regulatory waiver. Including business buzzwords commonly found in press releases as considerations tilts the scales of any application. Although applicants are also to describe how waivers will serve the public interest, expand access to financial products and services, and promote consumer or investor protection, these descriptions are also likely to be more public relations than measurable, substantiated benefits. An application rubric that is overly rooted in unquantifiable descriptions and explanations will make it difficult or impossible to identify and reject ineligible AI test projects.

VI. Test project application omits key elements needed for evaluation

The legislation does not require financial firms to include critical information necessary for regulators to assess and evaluate AI test projects. The legislation does not require firms to describe the data inputs or model descriptions nor does it provide any opportunity for public input regarding proposed AI test projects.

[38] H.R. 4801 §3; Clarity Act §10509(b)(1)(A).
[39] H.R. 4801 §4(a)(2)(B)(ii); Clarity Act §10509(b)(i)(II)(bb)(BB).
[40] H.R. 4801 §4(a)(2)(C)(i-ii); Clarity Act §10509(b)(i)(II)(cc)(AA)-(BB).

It does not require sufficient information on AI model or data inputs to evaluate AI test projects:

The legislation does not require applicants to specify the data elements the AI model would use, the rationale for using each data element, how data is collected, how data is shared and with whom, or the contours of the AI model (such as a meaningful description of how the data elements are weighted, how they are assessed, and how they are combined to generate the outputs). Nor does the legislation require (or even request) companies to provide the right of customers to review data, remedy data errors, request reviews for AI decision making, or redress data breaches or privacy infringement.

The legislation merely requires the applications to include "a description of the AI test project," which could be as little as stating that the applicant would use AI to perform a function inherent to the company's business line. For the regulators to meaningfully evaluate an AI test project, they would need to know both the what data elements will be used as inputs and a detailed description of how the AI model would evaluate the data to achieve an output determination. Without requiring data and model specificity, the regulators would be unable to assess the potential risks to consumers, investors, safety and soundness, systemic risk, or other potential unlawful outcomes such as stock market manipulation or failure to comply with anti-money laundering laws.

Application guidelines do not require granular information on risks: The legislation requires companies to identify how they will "effectively manage risks associated with the AI test project" and the House version requires it to describe "applicable" risk assessments, testing, and monitoring.[41] But that open-ended question does not require the applicant to identify what risks (fraud, deceptive practices, lending discrimination, price gouging, money-laundering, safety and soundness, etc.), risks to whom (consumers, investors, the applicant firm, the financial system, etc.), and what specific, concrete actions the applicant is pursuing to address those risks.

[41] H.R. 4801 §4(a)(2)(B)(ii)-(iii); Clarity Act §10509(b)(i)(II)(bb)(BB). Senate legislation does not include applicable risk assessments, testing, or monitoring.

It lacks basic public access or input into the application process: The AI test project application and approval process is entirely opaque. The usual practice is that public can comment on many bank licensing applications (for charters, branch closings and openings, mergers, and more). But there is no provision for public comment on AI test project waivers. These AI test project regulation and enforcement waivers are essentially requests for no action letters and should be published in the Federal Register and allow public comment, as provided by many financial regulators on no action letters.

• • •

The AI sandbox legislation encourages financial firms to deploy artificial intelligence to pursue broad waivers from federal financial laws and regulations. This bestows a get-out-of-jail-free card to discriminatory, predatory, unfair, and risky practices by regulated financial firms. It is an open invitation for financial firms to capture profits by ripping people off and pursing excessively risky business strategies that could have widespread damaging impacts on people, communities, and the economy.