

FROM PRINCIPLES TO POLICY: ENABLING 21ST CENTURY AI INNOVATION IN FINANCIAL SERVICES

HEARING BEFORE THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

DECEMBER 10, 2025

Serial No. 119–48

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

63–576 PDF

WASHINGTON : 2026

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
ANN WAGNER, Missouri	BRAD SHERMAN, California
ANDY BARR, Kentucky	GREGORY W. MEEKS, New York
ROGER WILLIAMS, Texas	DAVID SCOTT, Georgia
TOM EMMER, Minnesota	STEPHEN F. LYNCH, Massachusetts
BARRY LOUDERMILK, Georgia	AL GREEN, Texas
WARREN DAVIDSON, Ohio	EMANUEL CLEAVER, Missouri
JOHN W. ROSE, Tennessee	JAMES A. HIMES, Connecticut
BRYAN STEIL, Wisconsin	BILL FOSTER, Illinois
WILLIAM R. TIMMONS, IV, South Carolina	JOYCE BEATTY, Ohio
MARLIN STUTZMAN, Indiana	JUAN VARGAS, California
RALPH NORMAN, South Carolina	JOSH GOTTHEIMER, New Jersey
DANIEL MEUSER, Pennsylvania	VICENTE GONZALEZ, Texas
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	AYANNA PRESSLEY, Massachusetts
ANDREW R. GARBARINO, New York	RASHIDA TLAIB, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
MIKE FLOOD, Nebraska	NIKEMA WILLIAMS, Georgia
MICHAEL LAWLER, New York	BRITTANY PETTERSEN, Colorado
MONICA DE LA CRUZ, Texas	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	JANELLE BYNUM, Oregon
ZACHARY NUNN, Iowa	SAM LICCARDO, California
LISA McCLAIN, Michigan	
MARIA SALAZAR, Florida	
TROY DOWNING, Montana	
MIKE HARIDOPOLOS, Florida	
TIM MOORE, North Carolina	

Ben Johnson, *Staff Director*

C O N T E N T S

Wednesday, December 10, 2025

OPENING STATEMENTS

	Page
Hon. French Hill, Chairman of the Committee on Financial Services, a U.S. Representative from Arkansas	1
Hon. Maxine Waters, Ranking Member of the Committee on Financial Services, a U.S. Representative from California	2

STATEMENTS

Hon. Bryan Steil, Chairman of the Subcommittee on Digital Assets, Financial Technology and Inclusion, a U.S. Representative from Wisconsin	3
Hon. Stephen Lynch, Ranking Member of the Subcommittee on Digital Assets, Financial Technology and Inclusion, a U.S. Representative from Massachusetts	4

WITNESSES

Ms. Jeanette Manfra, Vice President and Global Head of Risk & Compliance, Google Cloud	5
Prepared Statement	7
Mr. Tal Cohen, President, Nasdaq	14
Prepared Statement	16
Mr. Nicholas Stevens, Vice President of Product, Artificial Intelligence, Zillow	23
Prepared Statement	25
Ms. Wendi Whitmore, Chief Security Intelligence Officer, Palo Alto Networks	31
Prepared Statement	33
Mr. Joshua Branch, Big Tech Accountability Advocate, Public Citizen	41
Prepared Statement	43

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Stephen F. Lynch: FinTech Regulatory Sandbox Guidelines FinTech Regulatory Sandbox Guidelines	126
Hon. Gregory W. Meeks: U.S. Halted Plans to Sanction Chinese Spy Agency to Maintain Trade Truce, FT Says	146
Hon. Maxine Waters: Coalition Letter Opposing H.R. 4801	148
Consumer Reports Opposing H.R. 4801	151

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Barry Loudermilk Ms. Jeanette Manfra	155
---	-----

IV

LEGISLATION

	Page
H.R. 4801, the Unleashing AI Innovation in Financial Services Act	157
H.R. 2152, the Artificial Intelligence Practices, Logistics, Actions, and Nec- essities (PLAN) Act	178
H.R. 1734, the Preventing Deep Fake Scams Act	183
H. Res. ———, Expressing the sense of the House of Representatives with respect to the use of artificial intelligence in the financial services and housing industries	188
H.R. ———, the Artificial Intelligence Innovation Sandbox Information Gen- eration and Harmonization of Testing Act (AI INSIGHT) Act	192
H.R. ———, the Fostering the Use of Technology to Uphold Regulatory Effec- tiveness in Supervision (FUTURES) Act	198

FROM PRINCIPLES TO POLICY: ENABLING 21ST CENTURY AI INNOVATION IN FINANCIAL SERVICES

Wednesday, December 10, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 10:12 a.m., in room 2128, Rayburn House Office Building, Hon. J. French Hill [chairman of the committee] presiding.

Present: Representatives Hill, Lucas, Sessions, Huizenga, Wagner, Barr, Williams of Texas, Loudermilk, Davidson, Rose, Steil, Timmons, Stutzman, Meuser, Kim, Garbarino, Fitzgerald, Flood, De La Cruz, Ogles, Nunn, McClain, Salazar, Downing, Haridopolos, Moore, Waters, Sherman, Meeks, Scott, Lynch, Green, Cleaver, Himes, Foster, Beatty, Vargas, Gottheimer, Gonzalez, Casten, Pressley, Tlaib, Torres, Garcia, Williams of Georgia, Pettersen, Fields, Bynum, and Liccardo.

Chairman HILL. The Committee on Financial Services will come to order. Without objection, the chair is authorized to declare a recess at any time.

Today's hearing is entitled From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services.

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

I now recognize myself for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. FRENCH HILL, CHAIRMAN OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM ARKANSAS

Advancements in artificial intelligence are not just on the horizon; they are here, and they are transforming our economy. Last Congress, Congressman Bill Foster and I served on Speaker Johnson and Minority Leader Jeffries' bipartisan congressional AI task force, and Congressman Steve Lynch and I led this committee's AI working group. In both forums, we examined how financial services firms and regulators are approaching artificial intelligence, analyzing its benefits and risks in a highly regulated environment.

Just this past fall, the Digital Assets, Financial Technology, and Artificial Intelligence Subcommittee, led by Chairman Bryan Steil, held a hearing where members evaluated how financial regulators and firms are using AI.

Today's hearing builds on our earlier work in last Congress and this Congress and will help us further examine AI use cases in the financial and housing industries. We will also consider how agencies are providing clear regulatory environment and assess where existing laws may fall short or require modernization and explore ways to foster innovation.

For decades, the financial services industry has pioneered the real-world application of AI and continues to be a standout leader. AI has shown its transformative potential to reshape how financial institutions operate from enhancing analysis, to managing risk, mitigating fraud, and, importantly, enhancing customer service.

However, as with any innovation, risks give rise to new challenges. Yet human progress is ever changing, never static, and AI represents the latest leg in this journey. To move forward, we must embrace and adapt for innovation.

This was the approach taken in the 1990s by former Congressman and former Securities and Exchange Commission (SEC) Chairman, Chris Cox, when Congress confronted the rapid commercialization of the internet. Rather than allowing fear to stall advancement, lawmakers adopted existing laws to fit the new technological era.

Congress established clear guidelines and principles early on, setting the stage for the rapid growth of the internet, enabling countless innovations and entire industries, and putting the United States at the forefront of that innovation and the internet's expansion.

Just as Congress navigated the uncertainties of the internet in the mid-1990s, we must use AI as an opportunity, not a threat, applying lessons of that era in order to confront today's technological landscape.

Identifying gaps and obstacles in our regulatory frameworks will help Congress create an AI landscape where innovation can flourish without unnecessary barriers while ensuring robust consumer protections and risk-based technological—technology-neutral regulations.

The committee is steadfast in its commitment to empowering U.S. firms to leverage AI's potential and drive the U.S. global leadership and adoption and innovation.

I thank all of our witnesses for joining us today and providing your valuable insights and perspectives, and I yield back.

It is now my pleasure to recognize the ranking member of the committee, Ms. Waters, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. MAXINE WATERS, RANKING MEMBER OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM ARKANSAS

Ms. WATERS. Thank you very much, Mr. Chairman.

AI is already embedding in the lives of millions of Americans, and we have a duty to ensure that it benefits society, not harms it. Unfortunately, Republicans have been complicit as Donald Trump bypasses Congress, directs Federal agencies to deploy biased AI with no safeguards, and now issuing an executive order that seeks to undermine all State oversight.

Republicans in Congress fail to acknowledge that despite all the benefits that AI may bring, it also poses challenges that demand our full attention. We are already seeing AI systems that hurt children, spread hate and discrimination, and amplify systemic risk in the financial system. As unemployment reaches new heights, reports continue to show AI replacing workers across industries. That is why the Biden Administration put in critical protections to ensure AI systems are transparent, explainable, and nondiscriminatory.

These are just basic safeguards to keep families and children safe. In some of the worst cases, chat boxes have encouraged self-harm, like suicide, carrying out sexually explicit conversations, and even provided dangerous misinformation and disinformation to minors but no one should be surprised that the same President who calls affordability a hoax is ignoring these very real concerns with AI. Since—twice this year, the White House and congressional Republicans have tried and failed to impose a moratorium on State AI laws, and now, despite those failures, Trump announced he would sign an executive order that would block States from adopting their own AI safeguards by threatening legal challenges and withholding Federal funding.

For this hearing, Republicans posed a bill—posted a bill that would give AI and its Big Tech creators a pass when they violate consumer, housing, banking, or securities laws. Democrats are not going to sit by and watch Trump and Republicans allow Big Tech to forcibly experiment on our communities. Any legislative efforts by Congress must ensure that consumers and investors understand the AI they are interacting with in the financial services space, while giving companies meaningful standards they can innovate under.

A partisan approach is not necessary if Republicans fight for their constituencies. Last Congress, I and then-Chair McHenry launched the first ever bipartisan AI task force. We held joint sessions, conducted oversight, and introduced bills to confront AI bias, deep fake scams, and discrimination, proving that innovation and oversight can go hand in hand. Democrats are leading these efforts because we believe in responsible innovation.

The stakes are too high, the risks are too great, and the consequences are too real to hand this technology over to Big Tech billionaires with no guardrails, no accountability.

Thank you, and I yield back the balance of my time.

Chairman HILL. The gentlewoman yields back.

I now recognize the chair of the Subcommittee on Digital Assets, Financial Technology, and Artificial Intelligence, Mr. Steil of Wisconsin, for 1 minute for an opening statement.

STATEMENT OF HON. BRYAN STEIL, CHAIRMAN OF THE SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL TECHNOLOGY AND INCLUSION, A U.S. REPRESENTATIVE FROM WISCONSIN

Mr. STEIL. Thank you very much, Mr. Chairman.

The U.S. must win the global AI race and the regulations that we may make here are incredibly consequential. We cannot get it wrong; we have. For example, the EU AI Act is a broad, horizontal approach that stifles innovation in Europe. In the U.S., I be-

lieve we should take a targeted, activity-specific approach to AI. As we examine use cases and those who develop and deploy AI today, we should examine if our rules need adjustments and tweaks to get this right. These use cases will only continue to evolve as generative and agentic AI technologies evolve. We must make sure we unlock innovation while protecting Americans. As the United States strives to win the AI global race, maintaining a “try first” approach will help preserve American dominance and agility. Let us win this race. I yield back.

Chairman HILL. The gentleman yields back.

I recognize the ranking member of the Subcommittee on Digital Assets, Financial Technology, and AI, Mr. Lynch, for 1 minute for an opening statement.

STATEMENT OF HON. STEPHEN LYNCH, RANKING MEMBER OF THE SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL TECHNOLOGY AND INCLUSION, A U.S. REPRESENTATIVE FROM MASSACHUSETTS

Mr. LYNCH. Good morning. Thank you, Mr. Chairman and Ranking Member Waters, for holding this hearing to continue examining AI innovation and regulation in the financial services sector. I also want to thank our panel of witnesses for helping the committee with its work.

Last Congress, I was proud to co-lead our bipartisan AI working group with my friend, Chairman Hill, to examine the benefits and risks of deploying AI technologies in banking, housing, credit lending, and other areas. These findings should continue to guide us as we pursue effective and responsible AI regulation. However, as ranking member of the Subcommittee on Digital Assets, Financial Technology, and Artificial Intelligence in this Congress, I am concerned that some of the regulations—regulatory proposals before this committee not only fail to include adequate guardrails but they also invite the financial services industry in adopting AI to choose which consumer protection and investor protection and safety and soundness regulations that they would like to avoid, which is reckless and dangerous.

In closing, I look forward to working with my colleagues to develop bipartisan AI legislation that promotes innovation while ensuring robust consumer and financial protection. I yield back the balance of my time.

Chairman HILL. The gentleman yields back.

Today we welcome the testimony of Jeanette Manfra, vice president, global head of risk and compliance at Google Cloud; Tal Cohen, president of Nasdaq; Nicholas Stevens, the vice president of product and senior developer of AI and engineering at Zillow; Wendi Whitmore, chief security intelligence officer at Palo Alto Networks; and Joshua Branch, Big Tech accountability advocate at Public Citizen.

We thank each of you for taking time to be with us. Each of you will be recognized for 5 minutes to give an oral presentation of your testimony. Without objection, your written statements will be made part of our record.

Chairman HILL. Mrs. Manfra, we will start with you. You are recognized for 5 minutes for your oral remarks.

**STATEMENT OF JEANETTE MANFRA, VICE PRESIDENT AND
GLOBAL HEAD OF RISK & COMPLIANCE, GOOGLE CLOUD**

Ms. MANFRA. Chairman Hill, Ranking Member Waters, and distinguished members of the committee, thank you for the opportunity to appear before you today. My name is Jeanette Manfra, and I am the vice president of risk and compliance at Google Cloud. We appreciate the House Committee on Financial Services holding this important hearing, and we look forward to sharing Google's perspective on the opportunity that artificial intelligence provides to America's financial sector.

Google believes that the introduction of AI in the financial services sector promises to usher in a transformative era for quality, accessibility, efficiency, and compliance in financial markets and services. AI offers many benefits, including the potential to enhance individual productivity, strengthen security operations, and drive database decisionmaking and operational efficiencies. These improvements will benefit institutions of all sizes, including small- and medium-sized financial entities.

At the same time, we also recognize that AI introduces risks that must be managed and mitigated. We believe that existing risk management frameworks and established governance practices can be applied to manage risks in the AI context.

For more than a decade, Google has used advancements in AI to further protect people from online scams, where malicious actors deceive users to gain access to money, personal information, or both. We offer a wide variety of protections powered by AI, including using Google Cloud's anti-money laundering AI service for financial sector customer risk scoring, utilizing AI-powered scam detection systems in search, an Android ecosystem that automatically identifies and blocks phishing messages and scam calls, and our efforts to ensure the integrity of Google ads on our platforms.

Additionally, Google further disincentivizes this malicious behavior by proactively filing litigation to dismantle massive fraud operations. In a recent example, in November 2025, we announced our filing to dismantle Lighthouse, a massive phishing-as-a-service operation. Bad actors built Lighthouse as a phishing-as-a-service kit to generate and deploy massive short message service (SMS) phishing attacks. These attacks exploit established brands, like EZPass, to steal people's financial information. Our legal action is designed to dismantle the core infrastructure of this operation.

We recognize that Google must work with industry participants, regulatory bodies, and technology providers to counter the critical threats posed by scams and frauds, and we are leading cross-industry efforts in combating fraud and scams in response.

We have introduced the Agent Payments Protocol, or AP2, an open-source protocol collaboratively developed with over 60 partners, including financial and technology companies, like American Express, Mastercard, and PayPal. AP2 aims to standardize and secure transactions made by AI agents on behalf of users, addressing key challenges such as authorization, authenticity, and accountability. This is an important step, and I look forward to discussing this with the committee.

We at Google have also introduced the Secure AI Framework, or SAIF, a conceptual framework for secure AI systems, including

those in the financial sector, and we have recently published an extension of the SAIF Risk Map to address the core operational components of agentic systems and their related risks and controls. In addition, we partnered with Amazon, Microsoft, IBM, Nvidia, and many others to co-found the Coalition for Secure AI, which is an open-source initiative to help all developers and deployers of AI create and maintain secure by designing AI systems and help advance the SAIF framework.

We recognize that we alone cannot solve these challenges. We have recently announced our endorsement of key bipartisan bills in Congress, crucial bills that we believe will help bring a decisive end to the financial harm and damage wrought by foreign cyber criminals. As the world focuses on the potential of AI, and governments and industry work on a regulatory approach to ensure AI is safe and secure, we believe that AI represents an inflection point for digital security. Regulators should support the development of global standards and their use across the financial services and regulatory landscape. In addition, regulators should foster industry collaboration and training based on such standards.

In closing, thank you for convening this really important hearing. We look forward to continuing to further raise awareness about cybersecurity, threats, and defenses for the financial sector and beyond.

[The prepared statement of Ms. Manfra follows:]



**Testimony of Jeanette Manfra
VP, Head of Risk and Compliance, Google Cloud
U.S. House Committee on Financial Services
December 10, 2025**

Chairman Hill, Ranking Member Waters, and distinguished Members of the Committee; thank you for the opportunity to appear before you today. My name is Jeanette Manfra, and I am the Vice President of Risk and Compliance at Google Cloud. We appreciate the House Committee on Financial Services holding this important hearing, and we look forward to sharing Google's perspective on the opportunity that artificial intelligence provides to America's financial sector.

Artificial Intelligence in the Financial Sector: Identifying Opportunities and Mitigating Risks

Google believes that the introduction of artificial intelligence (AI) in the financial services sector promises to usher in a transformative era for quality, accessibility, efficiency, and compliance in financial markets and services. AI offers many benefits, including the potential to enhance individual productivity, strengthen security operations, and drive data-based decision-making and operational efficiencies. AI can automate repetitive tasks such as responding to requests for proposals, localizing multilingual content, and conducting compliance checks. It can help handle complex, unstructured data, enabling firms to extract valuable insights through advanced conversational interfaces and data summarization techniques and facilitating informed decision-making and strategic planning. And it can prioritize critical threats, automate routine tasks, and improve threat detection and vulnerability management—enabling analysts to focus on significant issues, reducing burnout, and shifting security operations from reactive to proactive, ultimately improving overall security efficiency. Aggregate efficiency and productivity gains due to AI initiatives across the banking sector are [forecast](#) to be substantial, with estimates suggesting a potential addition of up to \$340 billion annually to the banking sector alone. Multinational corporations across many industries, including financial institutions, are exploring or already taking advantage of AI-based models.

At the same time, AI introduces risks that must be managed and mitigated. Google believes that existing risk management frameworks and established governance practices can be applied to manage risks in the AI context. In light of the unique complexities and potential impacts of AI, however, these models and frameworks may require regulatory clarifications to help firms effectively manage the new types of risks introduced by these advanced AI systems. In a recent [report](#) on AI risks in the financial management context, Google identified three key areas in which regulatory clarity can benefit all stakeholders. First, risk management guidance should specify documentation expectations for AI models. Second, regulators should take into account developers' use of practices such as grounding and outcome-based model evaluations, in addition to model explainability and transparency, in establishing the safety and soundness of AI-based models. Finally, regulators should recognize a set of controls, including

continuous monitoring, robust testing protocols, and human-in-the-loop oversight, that are appropriate for ensuring the responsible deployment of AI in financial services.

Google's Efforts to Utilize Artificial Intelligence to Combat Money Laundering, Fraud, and Scams

Google fights scams and fraud with consumer tools and enterprise offerings by taking proactive measures to protect users from harm, deliver reliable information, and partner to create a safer internet. For more than a decade, Google has used advancements in AI to further protect people from online scams where malicious actors deceive users to gain access to money, personal information, or both. For example:

- Our advancements in AI anomaly detection help companies identify, or even predict, abnormal patterns in unbounded data streams. Whether the companies are a large retailer identifying positive buying behaviors, a financial services provider detecting fraud, or a telecommunications company identifying and mitigating potential threats, they can use our tools to help detect behavioral patterns that provide useful insights.
- With Google Cloud's Anti-Money Laundering (AML) AI, we provide a consolidated machine learning (ML)-generated customer risk score as an alternative to traditional transaction alerting. The risk score is based on the bank's data including transactional patterns, network behavior, and Know Your Customer (KYC) data to identify instances and groups of high-risk retail and commercial customers. The product can adapt to changes in underlying data, delivering more accurate results, which increases overall program effectiveness and improves operational efficiency.
- In Search, AI helps us detect and block hundreds of millions of scam-results every day. We have made major investments in our AI-powered scam-detection systems that have enabled us to catch 20 times the number of scam-filled pages. These improvements help ensure that Search results are legitimate and protect users from harmful sites trying to steal sensitive data. We also provide tools like "About this result," which lets users learn more about online sources before clicking into them.
- Our Android ecosystem automatically filters out phishing messages and scam calls. All apps in Android Play are scanned daily for continued security. Proactive protections warn users before users visit an identified dangerous site, and theft protection keeps users' data safe before, during, and after theft attempts. Android's scam defenses protect users around the world from over 10 billion suspected malicious calls and messages every month. We are also [launching](#) new features on Android like using AI to [flag common scam messages](#) like fake toll fees or package deliveries. We are also protecting people from malicious links and scams in Google Messages. And for victims

of account compromise, we are making it safer and easier to regain access by expanding account recovery options with [Recovery Contacts](#).

- Google Ads works to ensure the integrity of the ads on our platforms, protecting users and enabling a safe ecosystem for advertisers and publishers. We have developed, and regularly update, a range of policies and methods tailored to the ads ecosystem. In 2024, for example, we suspended over 39.2 million advertiser accounts, the vast majority of which were suspended before they ever served an ad; and we removed 5.1 billion bad ads globally. Our AI-powered models contributed to the detection and enforcement of 97% of the pages we took action on last year.
- In 2024, our AI-powered detection systems blocked or removed more than 12 million fake business profiles and over 240 million reviews that violated our policies. The vast majority of the misleading reviews were removed from Google Maps before they were ever seen by our users.

In addition to building Google products that are secure-by-design, we focus on preventing financial scams through the development and enforcement of our policies. For example, Google Ads has in place the Limited Ads Serving policy, which has been key to dramatically reducing the volume of scam ads.

We also enforce a set of global policies for all cryptocurrency-related advertising by requiring all advertisers to obtain Google certification and adhering to the local laws of the countries for which the advertisers target. We further explicitly prohibit advertisements for initial coin offerings, DeFi trading protocols, or otherwise promoting the purchase, sale, or trade of cryptocurrencies or related products. These policies create a robust framework that underscores our commitment to user safety and the integrity of our advertising ecosystem.

To enforce these policies, we began embedding researchers and AI approaches in Google cyber security teams more than a decade ago. More recently, we have developed a [specialized large language model](#) that is fine-tuned for security and threat-intelligence. Some of these new tools are already up to 70% better at detecting whether a file is malicious and up to 300% more effective at identifying files that exploit vulnerabilities. And AI learns quickly, helping defenders adapt to instances of financial crime, for example.

Google further disincentivizes this malicious behavior by proactively filing litigation to dismantle massive fraud operations. In a recent example, in November 2025, we [announced](#) our filing to dismantle "Lighthouse," a massive Phishing-as-a-Service operation. Bad actors built "Lighthouse" as a phishing-as-a-service kit to generate and deploy massive "smishing" (SMS phishing) attacks. These attacks exploit established brands like E-Z Pass to steal people's

financial information. Our legal action is designed to dismantle the core infrastructure of this operation.

Collaboration Toward Responsible Artificial Intelligence Adoption

Whether to combat specific challenges like scams and fraud or to enable greater efficiency and productivity across society, responsible adoption of AI across sectors requires a collaborative approach among industry participants, regulatory bodies, and technology providers. Google has taken several steps to advance this objective.

We recognize that Google must work with partners to counter the critical threats posed by scams and frauds, and we are leading cross-industry efforts in combating fraud and scams in response, we have introduced the Agent Payments Protocol (AP2), an open-source protocol collaboratively developed with over 60 partners, including financial and technology companies like American Express, Mastercard, and PayPal. AP2 aims to standardize and secure transactions made by AI agents on behalf of users, addressing key challenges such as authorization, authenticity, and accountability. The protocol utilizes cryptographically-signed digital contracts called "Mandates" to create tamper-proof, verifiable records of user instructions for a variety of payment methods, from credit cards to cryptocurrencies. We expect AP2 to help foster new e-commerce experiences, such as automated purchasing, personalized offers, and streamlined travel bookings in a secure way.

Google has also introduced the Secure AI Framework (SAIF), a conceptual framework for secure AI systems, including those in the financial sector. And we have recently published an extension of the SAIF Risk Map to address the core operational components of agentic systems and their related risks and controls. SAIF has [six core elements](#):

- **Expand strong security foundations to the AI ecosystem.** Leverage secure-by-default infrastructure protections and expertise built over the last two decades to protect AI systems, applications and users. At the same time, develop organizational expertise to keep pace with advances in AI and start to scale and adapt infrastructure protections in the context of AI and evolving threat models. For example, injection techniques like SQL injection have existed for some time, and organizations can adapt mitigations, such as input sanitization and limiting, to help better defend against prompt injection style attacks.
- **Extend detection and response to bring AI into an organization's threat universe.** Detect and respond to AI-related cyber incidents in time by extending threat intelligence and other capabilities. For organizations, this includes monitoring inputs and outputs of AI systems to detect anomalies, and using threat intelligence to anticipate

attacks. This effort typically requires collaboration with trust and safety, threat intelligence, and counter abuse teams.

- **Automate defenses to keep pace with existing and new threats** Harness the latest AI innovations to improve the scale and speed of response efforts to security incidents. Adversaries will likely use AI to scale their impact, so it is important to use AI and its current and emerging capabilities to stay nimble and cost effective in protecting against them.
- **Harmonize platform level controls to ensure consistent security across the organization.** Align control frameworks to support AI risk mitigation and scale protections across different platforms and tools to ensure that the best protections are available to all AI applications in a scalable and cost efficient manner. At Google, this includes extending secure-by-default protections to AI platforms like Vertex AI and Security AI Workbench, and building controls and protections into the software development lifecycle. Capabilities that address general use cases, like Perspective API, can help the entire organization benefit from state of the art protections.
- **Adapt controls to adjust mitigations and create faster feedback loops for AI deployment.** Constantly test implementations through continuous learning and evolve detection and protections to address the changing threat environment. This includes techniques like reinforcement learning based on incidents and user feedback, and involves steps such as updating training data sets, fine-tuning models to respond strategically to attacks, and allowing the software that is used to build models to embed further security in context (e.g. detecting anomalous behavior). Organizations can also conduct regular Red Team exercises to improve safety assurance for AI-powered products and capabilities.
- **Contextualize AI system risks in surrounding business processes.** Conduct end-to-end risk assessments related to how organizations will deploy AI. This includes an assessment of the end-to-end business risk, such as data lineage, validation and operational behavior monitoring for certain types of applications. In addition, organizations should construct automated checks to validate AI performance.

In addition, Google co-founded the [Coalition for Secure AI \(CoSAI\)](#), an open-source initiative to help all developers and deployers of AI create and maintain secure by design AI systems and help advance the framework. CoSAI helps foster a collaborative ecosystem to share open-source methodologies, standardized frameworks, and tools. Since its launch, CoSAI has made significant strides in strengthening AI security in collaboration with industry and academia in areas including Software Supply Chain Security for AI Systems; Preparing

Defenders for a Changing Security Landscape; AI Security Risk Governance; and [Secure Design Patterns for Agentic Systems](#).

Further, across Google Cloud, we [model and promote the adoption of responsible AI data practices](#) that preserve our customers' privacy and support their compliance journey. Robust privacy commitments outline how we protect user data and prioritize privacy and the greater adoption of artificial intelligence rearms their importance. We adhere to a holistic approach to [AI risk management and compliance](#), including focusing on employing an AI risk assessment methodology for identifying, assessing, and mitigating risks; developing and using an automated, scalable, and evidence-based approach for auditing generative AI workloads; and emphasizing human oversight and collaboration in our risk assessments and governance councils.

Additionally, we use explainability tools to help understand and interpret AI predictions and evaluate potential bias; privacy-preserving technologies such as masking and tokenization and adhering to privacy laws; continuous monitoring and auditing for security vulnerabilities that AI might miss; investing in training programs to bridge the AI knowledge gap; and encouraging "interdisciplinary collaboration" between data scientists, risk analysts, and domain experts is also key.

Establishing Regulatory Harmony for Artificial Intelligence in the Financial Sector

Advances in AI have led to increased adoption in the financial services sector. A prominent use for this technology is to assist in key compliance and risk functions, including the detection of fraud, money laundering, and other financial crimes, as well as trade manipulation. As the use of these models grows, so do questions about managing risks associated with the models. In particular, regulators, financial institutions, and technology service providers have been looking at whether existing risk management guidance ("MRM Guidance")—which has traditionally been the regulatory regime applicable to managing risk in the financial services industry—continues to be relevant for AI models and, if so, how the guidance should be interpreted and applied to this new technology.

Advances in AI technology hold substantial promise for the future of banking and financial services. These very same technologies could also transform how financial regulators supervise activities and markets, and safeguard consumers. While we commend regulators for providing a sound framework in existing MRM Guidance for identifying and mitigating potential risks posed by AI models, more can be done to increase certainty, clarity, and effective and efficient risk mitigation strategies.

Regulators should support the development of global standards and their use across the financial services and regulatory landscape by explicitly recognizing such standards as

presumptive evidence of compliance with the MRM Guidance and sound AI risk mitigation practices. In addition, regulators should foster industry collaboration and training based on such standards.

We recognize that we alone cannot solve these challenges. We recently [announced](#) our endorsement of key bipartisan bills in the U.S. Congress – crucial bills that we believe will help bring a decisive end to the financial harm and damage wrought by foreign cybercriminals. As the world focuses on the potential of AI – and governments and industry work on a regulatory approach to ensure AI is safe and secure – we believe that AI represents an inflection point for digital security.

* * *

Thank you for convening this important hearing. We look forward to continuing to further raise awareness about cybersecurity threats and defenses for the financial sector and beyond.

Chairman HILL. Thank you very much.

Mr. Cohen, you are now recognized for 5 minutes for your testimony.

STATEMENT OF TAL COHEN, PRESIDENT, NASDAQ

Mr. COHEN. Thank you.

Chairman Hill, Ranking Member Waters, and members of the committee, thank you for the opportunity to testify on the impact of artificial intelligence on our financial system and the role of responsible innovation. My name is Tal Cohen, and I serve as president of Nasdaq. At Nasdaq, we aspire to be the trusted fabric of the global financial markets, connecting entrepreneurs and investors, fueling economic growth, fighting financial crime, and supporting millions of everyday savers and retirees. As a global technology provider and an operator of regulated markets, we have a unique perspective that shapes how we employ AI.

Our approach centers on three core principles: enhancing liquidity, ensuring transparency, and protecting integrity. AI is already making a measurable difference across all three of these within our solutions and I am going to start with financial crime, where the human cost is greatest.

In 2023, an estimated \$3.1 trillion in illicit funds flowed through the global financial system, and scam and bank frauds cost roughly 485 billion in losses worldwide. Behind these numbers are family losing savings, communities harmed by drug trafficking, human trafficking, and terrorism financing.

Nasdaq's cloud native AI enabled anti-financial crime platform, Verafin, is used by thousands of financial institutions to detect and prevent these crimes. Verafin analyzes vast data sets across its network to identify suspicious activity in ways no single institution could do otherwise.

This work went a step further with the launch of our agentic AI workforce. Our digital sanctions analyst has reduced the alert review workload for sanction screening by more than 80 percent, freeing compliance professionals to focus on complex, judgment-heavy issues while AI handles routine tasks.

AI also strengthens market integrity. Our surveillance platform uses machine learning to help exchanges and regulators detect insider trading across billions of daily transactions, rooting out market abuse that erodes investor confidence.

These achievements are only possible if you have the right governance and the right oversight in place. From the outset, Nasdaq established an enterprise-wide AI governance program aligned with the National Institute of Standards and Technology (NIST) AI risk management framework, overseen by an executive steering committee that includes our CEO. We also implemented a cross-functional governance committee led by legal, risk, regulatory, and technology teams.

Additionally, we adopted responsible AI principles covering transparency, fairness, privacy, reliability, and accountability, and we applied it across all products and internal operations.

And that brings me to the AI policy consideration before this committee. The U.S. has historic opportunity to lead in AI—if we

strike the right balance. From our perspective, the following principles are critical.

First, leverage existing regulatory frameworks. The financial sector is already heavily supervised. Many AI-related risks can be addressed with existing rules and mandates.

Second, focus on use cases and outcomes. Regulation should reflect risk profiles. An AI tool detecting drug trafficking or protecting seniors from fraud should be subject to higher standards than when that same tool is used to approve apartment rentals. They carry different risk profiles and require different regulatory treatment.

Third, Keep frameworks flexible and innovation friendly. Overly prescriptive rules tend to age poorly and risk pushing innovation overseas. We support sandboxes, pilots, and AI centers of excellence where regulators and industry can learn and work together.

Fourth, strive for harmonization. A patchwork of State-level AI laws creates uncertainty, raises costs, and can limit access to these tools. Federal coordination is the best way to protect investors while preserving U.S. competitiveness.

Applying these principles will ensure that AI is working to make our financial systems more fair, more efficient, and more resilient and that is the future we are working toward at Nasdaq and why we are grateful for the committee's leadership on these issues.

In closing, we support the administration's America's AI Action Plan and bipartisan effort in Congress to address harms such as nonconsensual deep fakes and synthetic media while preserving space for innovation. Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Cohen follows:]



Testimony of Tal Cohen

President, Nasdaq

Before the House Financial Services Committee

“From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services”

December 10, 2025

Thank you, Chairman Hill and Ranking Member Waters and other esteemed members of the House Financial Services Committee for the opportunity to testify about the exciting innovations we are bringing to financial services and markets from new Artificial Intelligence technologies. On behalf of Nasdaq, I appreciate the opportunity to testify on our strong belief that we need to deploy AI to make our markets better and our commitment to employ responsible governance in our services to investors and others by ensuring safe, fair and efficient markets and products.

Nasdaq serves as the trusted fabric of the world's financial system. We empower economic opportunities by designing and deploying technology, data, and advanced analytics that enable market participants to capture opportunities, navigate risk, and strengthen resilience.

We serve as an important architect to the world's most advanced markets by delivering scalable, agile infrastructure that empowers over 135 markets globally with deeper liquidity and seamless capital flows. With over 5,000 companies representing over 20% of the world's market cap listed on Nasdaq exchanges, we help companies access capital – and through our investor engagement solutions we help issuers build stronger relationships across the capital markets and to succeed as public companies. By integrating cutting-edge technology, comprehensive data, and innovative investment products, we fuel the innovation economy—enabling entrepreneurs to scale and investors to allocate resources with confidence.

Our solutions assist financial institutions in responding to risk-related challenges, supporting their efforts to meet regulatory requirements, preventing financial crime, and managing market manipulation effectively. Our solutions are focused on supporting our clients, individual investors and everyday Americans in three important ways:

- Enhancing Liquidity – Providing technology and solutions to power the world's most robust markets.
- Ensuring Transparency – Providing a robust data and analytics environment to connect corporates and investors with the data they need to make decisions.
- Protecting Integrity – Providing the wider financial system with technology and solutions to manage risk, protect markets, comply with regulations and fight financial crime.

We are at an extraordinary time in our industry, which is truly evolving at the speed of technology: the rise of private markets and private capital, the introduction and adoption of blockchain



technologies, the push towards always-on markets, and the integration of AI across every aspect of our industry. As a leading global technology provider *and* an operator of exchanges and other regulated businesses in the US, Canada and Europe, we understand the power of innovation to solve society's toughest challenges, as well the importance of appropriate regulation to ensure we create and protect a system that works for all. We are committed to driving resilient growth across our company and the clients we serve. We strongly support the Administration's "America's AI Action Plan" and this Committee's commitment to only moving forward with regulations that drive growth and innovation.

Our Approach and Journey to AI

We appreciate the opportunity to share our perspective on the potential impact and implications of Artificial Intelligence (AI) on the financial system and the regulatory approach to govern it.

Nasdaq has been a technology innovator since our birth in 1971 that led to the creation of electronic trading. Today, we take the same long-term approach to technology adoption to ensure we embrace growth and innovation in a responsible manner. We have a robust, coordinated process to govern the implementation of AI in our services and business operations to ensure that we scale our capabilities with proper security, oversight, and governance. We believe this is foundational to responsibly and securely unlock the power of AI to benefit society.

While recent developments regarding generative AI have brought AI into the forefront of public consciousness, AI has been integral to our services for years. We are already using AI technology to enhance transparency, liquidity, and integrity in the system.

How Nasdaq Uses AI

Nasdaq has integrated AI into its services for many years, approaching it from two primary perspectives: within our products and across our business operations. On the product side, we leverage AI throughout our suite to enhance intelligence, boost productivity, and improve efficiency. On the business side, we use AI to drive organizational productivity and free up employee time and resources, allowing our teams to focus on the highest-value work and the most pressing client challenges. Today, I wanted to share just a few examples of how we are harnessing AI's potential at Nasdaq.

- In protecting the integrity of our financial system, our anti-financial crime business is leveraging algorithmic and generative AI to fight criminal organizations involved in smuggling, drugs, terrorism and money laundering, more effectively than ever before. Financial crime is a multitrillion-dollar problem. Financial crimes are not victimless crimes. According to Nasdaq findings, an estimated \$3.1 trillion in illicit funds flowed through the global financial system in 2023 with losses from fraud totaling \$485.6 billion. To address this massive problem, our cloud-based platform is used by thousands of financial institutions of all sizes to dramatically improve the effectiveness and efficiency of their financial crime risk management programs.

Unlike conventional systems, this approach integrates multiple data sources and factors to determine the probability of fraud or money laundering, just as an investigator would. Our



vast, decentralized source of unbiased training data provides the big data set necessary to effectively deploy machine learning and identify the financial crimes that underpin society's most insidious crimes. After all, there is a money trail behind every act of terrorism or human trafficking. That is why we work to improve this technology every day to out-innovate the criminals, who are also using AI to develop new more sophisticated financial crime strategies.

This year, our anti-financial crime business announced the launch of its agentic AI workforce, a suite of digital workers that will deliver a step-change in compliance effectiveness and efficiency. Early results from the first two agents in beta — the digital Sanctions Analyst and the digital Enhanced Due Diligence Analyst — demonstrate agentic AI's potential to address the most resource-intensive compliance workflows. For example, when onboarding into a bank's alert triage workflow, our Digital Sanctions Analyst automates the acknowledgement, screening, and documentation processes, reducing alert review workload by more than 80% which allows analyst to focus on matters of higher risk.

- To further protect the integrity of our markets, in our Market Surveillance business, we use machine learning to detect market abuse, such as insider trading, market manipulation, and fraud. AI makes it possible for us to analyze billions of transactions and events every day to make it easier for our internal teams and our external clients, such as exchanges and regulators, to thwart fraud and manipulation. Advanced generative AI capabilities also help streamline the triage and examination process involved in investigating suspicious activity, empowering teams to more effectively monitor and detect potential market abuse.
- In using AI to drive improved liquidity in our markets, we introduced *Dynamic M-ELO* in 2024, the first exchange AI-powered order type. The technology is designed to deliver optimal outcomes by adapting to real-time market conditions and improving overall execution quality and fill rates.
- To bring more transparency to the financial system, in our data business, we use AI and machine learning to extract insights and value from large and complex data sets, such as market data, alternative data, and proprietary data to better serve corporates and investors. For example, we offer a product called Market Intelligence Desk, which uses AI to provide real-time market commentary and analysis for our listed companies, based on various data sources, such as news, social media, and trading activity.
- To further support this kind of transparency, in our governance business we are piloting new functionality within our Boardvantage service, which helps our clients manage their board meetings, documents, and communications, and uses AI to make it easier for board members to extract the most important information they need to oversee the risks and opportunities of the companies they govern.

These products are a result of our strong technology and product organizations, but also a reflection of a robust governance framework that analyzes the opportunities and risks of all new



product introductions, with particular attention to products that embrace new technology, such as AI.

Our AI Governance Program

As part of my remarks today, I want to give an overview of our AI governance program, which is a key part of our product development. The program addresses the new and unique risks that AI technology presents, while enabling us to explore new emerging opportunities. It is centrally managed and administered, eliminating the “AI sprawl” that plagues many companies.

Leading this effort is an executive steering committee that includes our CEO and senior members of our leadership team. Execution and risk are overseen by a cross-functional AI governance committee that is led in partnership between Legal, Risk and Regulatory Team, and the Technology team. The program is supported by company-wide policies, procedures and controls and our usage framework is aligned with the U.S. National Institute of Standards and Technology AI Risk Management Framework.

We knew years ago that AI technology needed to be pursued ethically, based on our core values which are the foundation of how we operate our business. As part of that effort, we adopted a set of *Responsible AI Principles* that reflect core tenets of ethical AI usage tailored to our business. These principles include a commitment to transparency, fairness, accessibility, efficiency, reliability, responsible data management, privacy, security, accountability, and oversight.

And, in addition to serving as the foundation of our AI strategy, these principles also guide our approach to collaboration with policy makers, regulators, law enforcement and other financial institutions in the private sector.

Considerations and Recommendations for the Regulation of AI

We recognize that AI poses both significant opportunities and risks that require careful oversight. We appreciate the efforts of the Committee and regulators to foster a supportive and balanced regulatory environment for AI innovation in the financial sector, while addressing the potential risks and harms that AI may pose.

We also believe that AI is a promising technology that can bring significant benefit to our industry and the wider economy, and that the environment for AI innovation in the United States is a foundational differentiator to our ability to compete globally.

Regulating AI is an interstate commerce issue and we believe that federal legislation is needed, and as Congress and agencies look to develop AI-related laws and regulations, we believe that such actions should consider the following:

- Existing regulations and regulatory structures should be leveraged wherever possible. Current laws and regulations already set the framework for how the financial sector operates, and regulators understand how companies they cover operate. Like prior technological innovations, the adoption of AI technology does not necessarily demand sweeping regulatory changes - many of the top concerns about AI can be addressed by existing laws and enforceable by agencies.



- New regulation should be risk-based and proportionate, meaning that it should focus on the potential outcomes in terms of benefits, risks, and harms of AI applications, rather than on specific technologies or methods. For example, the regulation applied to the use of an AI tool to detect drug trafficking or protect senior citizens from check fraud should not be the same as the regulation applied to use of the same AI tool to approve apartment rental applications. It is important to address potential bias in models, while also considering specific use cases where mitigation is necessary, rather than applying broad measures that could affect the effectiveness of systems designed to detect, deter, and prevent crime.
- The regulatory environment should endeavor to be flexible and adaptive, meaning that it should allow for experimentation and innovation and should be able to evolve, as the AI applications and market conditions change. We support the development and adoption of industry standards that provide practical guidance and benchmarks for industry and regulators.
- AI-specific regulation should be consistent and harmonized, meaning that it should avoid creating gaps, overlaps, or inconsistencies among different regulators, jurisdictions, or sectors, and that it should promote coordination and cooperation, among the regulators, the industry, and the international community. Within the federal government, while we oppose the creation of central regulator, we support leveraging NIST or another body to provide coordination across government to ensure consistent regulatory standards and development of the federal workforce knowledge of AI. We also believe that Congress should consider appropriate action to avoid the creation of a patchwork of differing state laws governing AI as this could stifle innovation, increase expense, reduce the availability of AI tools to various states and harm the competitiveness of the United States globally.
- The regulatory environment should be transparent and accountable, meaning that it should provide clear and timely guidance and feedback to the industry, as well as to the public, on the expectations and requirements for AI applications. We support creating and promoting safe platforms, such as sandboxes, pilots, and labs, where industry and regulators can test and learn from the AI applications, in a controlled and supervised environment, and where industry and regulators can share and exchange their experiences. To promote this, we encourage Congress and regulators to enhance their capability to oversee AI, by investing in their own AI tools, systems, and collaborating with industry and academia.

Nasdaq is certainly in agreement with aspects of the President's recently released "America's AI Action Plan." I want to mention a few areas.

- Establish regulatory sandboxes or AI Centers of Excellence around the country where researchers, startups, and established enterprises can rapidly deploy and test AI tools while committing to open sharing of data and results. This is consistent with Nasdaq's view that I



previously stated about creating and promoting safe platforms where industry and regulators can test and learn from AI applications and share their experiences.

- **Empower American Workers in the Age of AI** – One of the most significant ways that economies grow is through increased productivity. Technology improvements are and will continue to be a driver of increased productivity. But that means a workforce that is able to utilize newly developed AI tools to participate in the new economy and not be left behind by that economy. In addition, companies and governments will not benefit from the increased productivity that AI tools can provide if their workers do not have the capacity to use them.
- **Combat Synthetic Media in the Legal System** – As was put forth in a white paper authored by the Business Roundtable, a leading organization of America's CEOs, "Synthetic content has a wide variety of beneficial purposes but also has the potential to harm individuals, organizations and ecosystems if it is used to manipulate and misrepresent. As these technologies become widely accessible, policymakers should verify the authenticity and source of the content, or develop risk-based, context-driven and flexible guardrails that appropriately safeguard against these risks while protecting beneficial uses. These guardrails should reflect the importance of innovation in AI while emphasizing the significance of ensuring information credibility and authenticity." Nasdaq applauds the bipartisan passage of the "Take It Down Act" earlier this year. We believe that Congress should continue moving forward in that manner to move other significant and related legislation such as the bipartisan and bicameral "No Fakes Act".
- Nasdaq has worked with our partners such as the Business Roundtable and TechNet in responding to the RFI from the Office of Science and Technology Policy on Regulatory Reform on Artificial Intelligence to identify existing Federal statutes, regulations, agency rules, guidance, forms, and administrative processes that unnecessarily hinder the development, deployment, and adoption of artificial intelligence (AI) technologies within the United States. Although we certainly support the safe use of AI throughout society, the U.S. regulation must unleash, not hamper AI development and deployment.
- Lastly, we strongly believe that for the effective development and deployment of AI there must be a well-considered pre-emption of state laws regulating the use of artificial intelligence. We are in strong agreement with the Business Roundtable who supports broad federal preemption of state laws related to AI, including through a federal regulatory approach that facilitates the development and deployment of innovative AI technologies in the United States and avoids a patchwork of state regulation. Such an approach does not require comprehensive legislation to regulate AI technology but rather targeted guardrails, where appropriate, can be adopted through a collection of legislative, regulatory and executive actions.

Conclusion



Thank you for your attention and interest in this important and timely topic. We are at an extraordinary time in our industry, and Nasdaq is committed to using AI in a responsible, ethical, and transparent manner, and to contributing to the development of AI in the financial sector and the economy. We look forward to collaborating with the Committee and relevant regulators in cultivating a regulatory framework for AI that encourages innovation, while addressing the potential risks and harms that AI may pose.

I am happy to answer any questions you may have.

Chairman HILL. Thank you, sir.

Mr. Stevens, you are recognized for 5 minutes for your oral presentation.

**STATEMENT OF NICHOLAS STEVENS, VICE PRESIDENT OF
PRODUCT, ARTIFICIAL INTELLIGENCE, ZILLOW**

Mr. STEVENS. Chairman Hill, Ranking Member Waters, and members of the committee, thank you for the opportunity to testify today. My name is Nicholas Stevens, and I serve as vice president of product, artificial intelligence of Zillow. Our mission is to help people navigate one of the most meaningful and complex decisions of their lives: finding a home.

After 9 years at Zillow, improving the housing journey, I recently had the chance to live it again. My family just moved. At the end of the process, my 5-and 7-year-olds could not sleep. They were up at 3 a.m. and when my wife and I sat them down to ask what on earth was troubling them, they had two very nervous questions. A: "Are we bringing our cat, Lily, to the new home?" B: "Are we also bringing the TV?" I am happy to report that both have made it safe to our new home but everything in between—the search, the paperwork, the financing, the closing—was a reminder of how emotional and confusing this process can be. That is the friction we are trying to address with responsible AI.

Zillow has been applying AI to housing for nearly two decades, starting with the Zestimate, one of the first large-scale consumer uses of machine learning in real estate. It is not an appraisal or used for credit decisions. Rather, it empowers buyers and sellers with a ballpark estimate of home value. The Zestimate was so popular, it crashed our site because consumers were asking for information that has historically been available only to a select few. Today, 250 million unique users come to Zillow every month to dream, to rent, to tour, finance, buy, and sell their homes and with that scale comes real responsibility. Our products cannot just be clever. They have to be reliable, fair, and trust-affirming.

Since Zillow last appeared before this committee, Next Generation AI has moved from pilot to production. AI in real estate is not theoretical. It powers tools people are using today, and I will highlight a few examples.

We have built an AI to be a true assistant to real estate agents nationwide. It helps prioritize an agent's leads. It summarizes notes. It drafts emails and one of the agents' favorite features is that it suggests key topics to touch on in their clients' catch-up call.

Technology also allowed our company to go fully remote, and we now have employees in all 50 States.

Our latest computer vision experiences allow you to not only generate a home's floor plan so potential buyers can explore the inside in detail; we also let them fly around and get a sense of the exterior and yard.

The through line is that safeguards are built in, not bolted on. Internally, Zillow employees complete fair housing and privacy training, and anyone working with AI receives additional responsible AI training. Before we launch an AI feature, cross-functional teams conduct a model risk review focused on fairness, bias, privacy, and explainability. After launch, we perform periodic audits

and continuous monitoring so we can catch issues that only appear at scale.

Externally, this is even true with public partnerships. Now consumers can talk to Zillow directly inside ChatGPT's new in app experience, asking, for example, "Zillow, show me 2-bedroom homes that are wheelchair accessible," and in return, they get listings, photos, and maps from Zillow in a conversational flow.

We built this with a fair housing first design. Our Fair Housing Classifier helps detect and prevent potential digital steering. We also believe responsible innovation means raising the floor for everyone. Zillow open-sourced that same Fair Housing Classifier under a permissive license, and it is now in use by real estate platforms and researchers working to combat housing discrimination. That is a concrete example of innovation and compliance rowing in the same direction.

All of this argues for a right-sized national framework for AI in financial services, including housing. A coherent national baseline for fairness, transparency, privacy, and accountability would give consumers consistent safeguards and give companies the confidence to integrate strong protections from day 1. The alternative is a patchwork where the same consumer gets different quality experiences across State lines for the same transaction.

Even the latest AI technology would not have prompted me to explain to my kids that, yes, both our cat and the TV would be coming to our next home, but it can help tackle the structural challenges we all worry about: affordability, supply, and outdated processes.

As you consider a national framework for AI and modernization of our housing finance system, we stand ready to share data, technical expertise, and lessons from building these systems at scale. We appreciate the committee's leadership on this issue, and I look forward to answering your questions.

[The prepared statement of Mr. Stevens follows:]

Written Testimony of Nicholas Stevens

Vice President of Product at Zillow

**U.S. House of Representatives Financial Services Committee
Hearing on “From Principles to Policy: Enabling 21st Century AI Innovation in
Financial Services”****December 10, 2025**

Chairman Hill, Ranking Member Waters, and distinguished Members of the House Financial Services Committee, thank you for the opportunity to appear before you today. I am Nicholas Stevens, Vice President of Product at Zillow. Our mission is to help people navigate one of the most meaningful and complex decisions of their lives: finding a home. It's an emotional journey during which half of all buyers cry at some point, which is why we listen closely to consumers, identify pain points, and build technology that is simple, transparent, and trustworthy.¹

Zillow has been a leader in applying AI to housing from the very beginning. When we launched the Zestimate, one of the first large-scale consumer uses of machine learning in real estate, it was so popular that our site crashed. Consumers were telling us clearly: they wanted access to information that had historically been available only to agents.

Two decades later, more than 240 million unique users come to Zillow each month to rent, tour, finance, buy, and sell homes.² With scale, comes responsibility and possibility. Our products can't just be useful, they have to be reliable, fair, and safe.

Last time Zillow appeared before this Committee, we shared how we were beginning to integrate generative AI into our platform.³ Today, I can clearly say: next generation AI at Zillow has gone from a pilot to a live, consumer-facing, and reshaping housing in real time. These aren't experiments; they are real features supporting people as they navigate the housing journey. Our AI strategy strengthens our processes and enhances the customer experience; it is not innovation for its own sake. To that end, we're continuing to release technology-driven products and explore new

¹ <https://zillow.mediaroom.com/2022-06-02-Half-of-Americans-cry-at-least-once-while-buying-a-home>

² <https://investors.zillowgroup.com/investors/overview/default.aspx>

³ <https://docs.house.gov/meetings/BA/BA00/20240723/117527/HRG-118-BA00-Wstate-LindaO-20240723.pdf>

applications of AI to make the housing journey even simpler, more transparent, and more accessible.

AI also gives us new tools to help address the affordability and supply challenges that plague our housing market. Scaling responsibly requires clear national guardrails that encourage progress while protecting consumers, and Zillow is eager to contribute data, insights, and technical expertise to help develop that framework.

Transforming the Housing Journey Through Technology and AI

The best products solve real user problems. That's what we're doing with AI at Zillow.

For example, through our partnership with OpenAI, consumers can interact with Zillow in ChatGPT's new in-app experience. Instead of scrolling through filters, someone can simply ask: *"Zillow, show me 2-bedroom homes for sale in Little Rock under \$200,000."* In response, they see listings, photos, and maps in a conversational flow. This is a new interface for search — one that lowers barriers for consumers who might not know how to start. Zillow built this experience with a fair housing-first design, including safeguards to reduce biased or inappropriate responses and to protect listing data. OpenAI cannot use Multiple Listing Service data for training or reuse it outside the Zillow experience.

We also ensured our Fair Housing Classifier was built into the ChatGPT Zillow App, further emphasizing our deep investment in fair housing safeguards through our AI deployments. The Fair Housing Classifier helps detect and prevent potential "steering" — the illegal practice of influencing a buyer's choice of communities based on protected characteristics. More broadly, we incorporate model risk reviews, fairness evaluations, privacy safeguards, and ongoing monitoring into how we operationalize AI. Creating national standards for these important principles would help ensure consumers receive strong, predictable protections regardless of where they live or which platform they use.

Finally, we're using technology to help people on the path to homeownership answer their most common question: what can I afford? Fifty-eight percent of renters tell us they aspire to buy, but many don't know where to start. That's why we introduced BuyAbility, which gives a simple, personalized understanding of what someone can

afford based on real-time data. It's not using AI yet, but as rules and data flows modernize, tools like this can become even more accurate and more empowering.

The common thread across these examples is that these are real products available to millions of users to drive their own homeownership journey. From a product standpoint, every one of them is built with safeguards: fairness checks, privacy protections, human review, and ongoing monitoring.

Building Responsibly: Our Governance Model

Deploying AI responsibly is harder than shipping any other kind of feature. That's because AI can behave differently in different contexts. We can't just build and launch; we have to build, test, monitor, and adapt.

All Zillow employees complete fair housing and privacy training, and we also provide responsible AI training for anyone working with AI. Before we launch, we bring together product, compliance, legal, and engineering teams for a model risk review. We focus on promoting fairness, reducing bias, and ensuring transparency, so we can build AI systems that are safe and reliable. We also conduct periodic audits to ensure these systems are aligned to our fair housing principles.

We're also committed to sharing our innovations, to raise the floor for everyone. For example, Zillow has released its Fair Housing Classifier under an open-source license as part of our commitment to responsible innovation; already, 15 real estate platforms, research universities, and other groups are using it to combat housing discrimination. By developing this tool and releasing it freely, Zillow is demonstrating how innovation and responsibility can go hand in hand — we've advanced and shared technology that strengthens the housing market, protects consumers, and supports compliance with fair housing laws.

We also test new frontiers. Our early work with speech-to-speech AI and our integration with ChatGPT's in-app experience are examples where we're exploring what's possible, with appropriate safeguards and while focused on the consumer experience.

AI as a Driver of Affordability, Supply, and Modernization

For a product manager, the most important test of any product is whether the product solves a real problem for its users. In the housing market, those problems include a lack of affordability, limited supply, and outdated systems that frustrate consumers. We see opportunities for AI to help tackle all of those interconnected challenges.

For example, AI can help reduce loan origination costs, which have risen by over 40 percent since 2019, by automating manual work like document checks, compliance reviews, and loan summary generation.⁴ It could help local governments clear permitting and zoning backlogs by reviewing project submissions and quickly identifying issues and solutions when projects are submitted. It can also help builders submit compliant plans to accelerate the permitting process. Together, these innovations can unlock housing supply by reducing administrative delays.

The integration of AI into the homebuying system should go hand-in-hand with the modernization of that system, adapting rules so they continue to protect people while allowing for innovation and an improved consumer experience. Today, consumers can shop for a home on their phone, but may still be asked to sign mortgage documents in person with pen and paper. Disclosures aiming to make the consumer aware of important information are too often confusing, antiquated, and paper-heavy, and in some cases still rely on snail mail. These analog rules add friction without meaningfully helping consumers.

We believe modernizing our homebuying system should accomplish five key goals: seamless processes, flexible closings, modernized workforces, clear disclosures, and maintaining room for innovation.

Seamless processes in homebuying means consumers should be able to search, finance, and buy a home in one connected flow, rather than across disconnected systems. *Flexibility in closing* means that, whether in person, online, or hybrid, buyers should be able to close how they prefer, without mountains of paper. A *modernized workforce* will see loan officers and housing professionals able to focus on people,

⁴<https://www.mba.org/news-and-research/newsroom/news/2025/08/19/imbs-report-production-profits-in-second-quarter-of-2025>

while technology takes care of repetitive tasks. *Clear disclosures* should inform and protect consumers without intimidating or overwhelming them. And regulations should allow for *room for innovation* while protecting consumers and ensuring responsible AI usage.

Why a National Framework Matters for Product and Scale

When innovative companies like Zillow build AI-powered tools, the best approach is to build them once, test them thoroughly, scale them thoughtfully, and then responsibly oversee their operation. We are committed to helping consumers from coast to coast harness the power of AI in their quest to find a home, and they should have access to the same safe and effective tools no matter where they are in the country.

That is why Zillow supports a right-sized national AI framework developed in partnership with federal, state, local, and industry stakeholders — because a consistent baseline lets companies build once and deploy safely nationwide, while still giving states room to add protections based on local needs. A single framework means we can design fairness checks, privacy protections, and transparency tools into our products from the start, knowing they apply nationwide. It allows us to ship faster, scale responsibly, and deliver a consistent experience for every consumer.

This is also ultimately about capability. If AI regulation is hyperfragmented, the same digital assistant could have different capabilities in different places — what it can display, what it must ask or confirm before acting, or whether it can complete a task. We've seen a similar pattern in digital closings: some states permit remote online notarization while others are still catching up, leading to uneven experiences for the same transaction. Clear, interoperable guardrails can help keep AI capabilities consistent across state lines while respecting state policy priorities.

For consumers, a national framework means confidence. Whether you're renting an apartment in Florida or applying for a mortgage in Oregon, you know the same AI protections apply.

Zillow is eager to be a resource lawmakers can rely on while building this national framework — sharing real product learnings, consumer insights, and technical

expertise about what it takes to build and scale AI responsibly. We know industry can't figure this out alone, and the government shouldn't have to, either. The best solutions will come from working together.

Conclusion

At Zillow, our focus is straightforward: build tools that solve real problems, with the goal of earning — and keeping — people's trust. AI expands what's possible, and we apply it intentionally where it adds clear value. We continue to advance our core technology as we explore how AI can responsibly enhance both today's products and what we build next.

Clear, interoperable national guardrails, paired with right-sized modernization of outdated rules, will give innovators the foundation to build once, test thoroughly, and deploy at scale, while giving the public confidence that protections are consistent across state lines.

We encourage this Committee to continue its bipartisan work on a national AI framework and regulatory modernization. Zillow stands ready to be a partner — offering our data, insights, and technical expertise to ensure AI truly serves Americans.

Chairman HILL. Thank you very much.

Ms. Whitmore, you are now recognized for 5 minutes for your oral testimony.

STATEMENT OF WENDI WHITMORE, CHIEF SECURITY INTELLIGENCE OFFICER, PALO ALTO NETWORKS

Ms. WHITMORE. Good morning.

Chairman Hill, Ranking Member Waters, and distinguished members of the committee, thank you for the opportunity to testify. My name is Wendi Whitmore, and I am the chief security intelligence officer at Palo Alto Networks. We are an American cybersecurity company protecting more than 75,000 organizations in over 150 countries, including 97 of the Fortune 100, eight of the 10 largest banks, the U.S. Federal Government, and critical infrastructure operators.

The promise of AI for financial services is undeniable and realizing it requires the sector to simultaneously embrace AI for cybersecurity, and cybersecurity for AI. There is both urgency and opportunity for financial institutions to lead. The threat landscape is evolving as advanced AI and quantum computing reshape both innovation and risk.

Attacks are faster, more automated, and harder to detect. Time from compromise to data exfiltration is now 100 times faster than 4 years ago, and attackers are increasingly exfiltrating data within 1 hour.

Generative and agentic AI now super-charge every phase of the kill chain, enabling deep fake-driven fraud, know your customer evasion via face swapping, and tailored spear phishing, imitating trusted financial institutions. Our own research shows that agentic AI can compress a multi-day ransomware operation into only 25 minutes, from reconnaissance to compromise to data theft.

This reality underscores why the financial sector must do two things: one, adopt AI-driven security operations that operate at machine speed; and two, harden their AI ecosystems with a secure-by-design approach.

Today's security operation centers, known as SOC's, are drowning in fragmented data, and alerts from an average of 83 security solutions, forcing skilled analysts into inefficient, manual triage. Consequently, critical alerts are buried, with 75 percent of breaches having actionable logging that was never reviewed, leaving vulnerabilities exposed and degrading our core ability to rapidly detect and respond to threats.

AI-driven SOC's flip this paradigm, acting as a force multiplier for cyber professionals that substantially reduces detection and response times. The results of deploying AI in our own SOC are transformative. We ingest roughly 90 billion events every day. By leveraging AI, we reduce those to only 26,000 alerts, ultimately resulting in one single incident requiring manual investigation.

In financial institutions deploying AI-driven SOC's, we see four times more security data ingested into a consolidated platform, thousands of models providing real-time prevention and detection, automation cutting analysts' workload by three-quarters, and the mean time to respond falling by up to 90 percent. In one global financial markets utility, their mean time to respond fell from 24

hours to 14 minutes. Another large bank saved more than 1,000 analyst hours annually while improving threat hunting and reducing attrition.

AI adoption is integral to America's innovation leadership, which is why Palo Alto Networks was proud to support America's AI Action Plan, which recognize that the benefits of AI will stall if we do not secure AI itself.

Attacks against AI systems have fundamentally evolved beyond traditional cybersecurity considerations. They target how systems learn and how they reason. The answer to accelerate AI innovation is to embed security throughout the AI life cycle so that we can adopt AI tools confidently.

Secure AI by design provides the blueprint to integrate security from development through deployment and use, ensuring visibility, control, and protection at enterprise scale. Practically, that means discovering and governing external AI tools, including Shadow AI, securing AI infrastructure and data, monitoring and controlling AI agents, and safely building and deploying AI applications.

Building an AI-ready ecosystem is a team effort. As a Financial Services Industry (FSI) sector advisor and a participant in the Cyber Risk Institute innovator program, Palo Alto Networks helps align best practices with leading standards and reduce compliance friction for financial institutions. If we secure the future now through AI-driven defense and secure AI by design, we can unleash the full potential of AI innovation while protecting consumers, markets, and national security.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Wendi Whitmore follows:]

Written Testimony of:

Wendi Whitmore
Chief Security Intelligence Officer
Palo Alto Networks

Before the:

Committee on Financial Services

Regarding:

"From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services"

December 10, 2025
10:00 AM



Chairman Hill, Ranking Member Waters, and distinguished members of the committee:

Thank you for the opportunity to participate in today's hearing on AI innovation in financial services. My name is Wendi Whitmore, and I am the Chief Security Intelligence Officer for Palo Alto Networks.

For those not familiar with Palo Alto Networks, we are an American cybersecurity company founded in 2005 that has become a global cybersecurity leader – protecting over 75,000 enterprises in over 150 countries worldwide, including 97 of the Fortune 100, 8 of the largest 10 banks in the U.S., as well as the U.S. federal government and critical infrastructure operators.

As this hearing will reinforce, the enormous promise of AI is undeniable. Palo Alto Networks firmly believes that central to realizing this promise – for the financial services industry and beyond – is being thoughtful in our understanding of the AI-cybersecurity nexus. This requires appreciating 1) the opportunity for AI to turbocharge cyber defense, and 2) the necessity to fortify our AI ecosystem through a *Secure AI by Design* approach.

This perspective is informed from our unique vantage point in our industry. We first introduced machine learning (ML) capabilities as part of our malware protection more than a decade ago and now offer over 30 AI-driven products, with more in development. Investing over \$1.8 billion in R&D last year, we combine ML, deep learning, and AI to enable real-time, automated protection across networks, cloud environments, endpoints, and the AI ecosystem.

With financial institutions sitting at the center of the digital economy, the imperative for the sector should be clear: simultaneously embrace AI for cybersecurity, *and* cybersecurity for AI.

The Evolving Cyber Threat Landscape

The rapid development of powerful emerging technologies – from advanced AI to quantum computing – promises incredible opportunities for the sector, but also introduces entirely new classes of complex security risks we must proactively address. While AI will transform financial decision-making and the customer experience, quantum computing's arrival will necessitate a fundamental re-engineering of the cryptography underpinning all global transactions. This is why we must take these proactive security actions now: to responsibly secure the future of finance and unleash the full scale of innovation that these technologies will bring to the sector.

Over the past year, attacks have become faster, more automated, and harder to detect, with time from compromise to data exfiltration shrinking dramatically – now 100x faster than four years ago, and in one in five cases completed within an hour. The financial services sector bears disproportionate risk given the value of its data and interconnected systems, while its attack surface expands through Application Programming Interfaces (API), cloud adoption, and third-party integrations. At the same time, firms contend with evolving regulatory expectations, talent shortages for specialized roles, and the persistent tendency to elevate cybersecurity only after an incident.

Generative and agentic AI intensify these pressures by accelerating every phase of the attack chain and enabling threats such as deepfake-driven fraud, Know Your Customer (KYC) evasion via face-swapping, and tailored spear-phishing campaigns masquerading as communications from trusted financial institutions. Recent [Palo Alto Networks research](#) shows that agentic AI can compress what was once a multi-day ransomware campaign into roughly 25 minutes, including reconnaissance, compromise, and data exfiltration. As AI becomes more widely adopted, it will also exponentially expand the digital attack surface and create new vectors for adversaries and cyber-criminals to target – like training data and model environments.

These realities underscore the urgency for financial institutions to modernize defenses with AI-driven security operations that move at machine speed, and embrace Secure AI by Design to harden the expanding AI attack surface and reap the benefits of AI innovation.

Meeting the Moment: Leveraging AI for Cyber Defense

At Palo Alto Networks, we see firsthand how AI-driven cybersecurity is essential to protecting privacy, strengthening national security, and safeguarding our digital way of life. The risky outcome for society would be to *not* meaningfully leverage AI for cyber defense.

Every day, Palo Alto Networks detects up to 8.95 million new attacks. The process of continuous discovery and analysis allows threat detection to stay ahead of the adversary. This real-time awareness of the threat landscape allows our company to block up to 30.9 billion attacks each day. This would not be possible without AI.

We are committed to disrupting the status quo of the cybersecurity industry to simultaneously: 1) deliver transformative cybersecurity outcomes, 2) drive much-needed cost rationalization for network defenders, and 3) eliminate inefficient, manual processes. This innovative spirit will be critical to combatting not just the threats of today, but also the emerging risks – like encryption-breaking quantum computing – of tomorrow.

The Legacy Imbalance

Security Operations Centers (SOCs) are the nerve center of organizational cyber resilience, yet defenders across the financial services sector have historically drowned in alerts and fragmented data. For too long, the community's most precious resource – its people – have been forced into manual triage across dozens of disparate tools, an inefficient model that leaves vulnerabilities exposed, burns out analysts, and degrades core metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) – critical indicators that provide quantifiable data points for network defenders about how quickly they discover and contain potential security incidents. The average enterprise SOC ingests data from 83 security solutions across 29 vendors, making effective detection and response nearly impossible under legacy practices.

The consequences are stark: in 75% of breaches, logging existed that should have flagged anomalous behavior, but critical signals were buried and never actioned. Industry research indicates that over 90% of SOC's still rely on manual processes, leaving adversaries with the advantage. Palo Alto Networks reports that teams still take nearly six days on average to resolve cloud breach alerts; meanwhile, sensitive data can be exfiltrated in a matter of hours.

Financial institutions, in particular, are drowning in their own data and struggling to operationalize it, facing an unrelenting "more" – more tools to manage, more devices to monitor, more data to analyze, more attack surface to defend, and more attacks to repel. This imbalance undermines incident response at the very moment when speed and precision are paramount, threatening both national and economic security.

AI-Driven Security Operations Centers

AI-driven SOC's can flip this paradigm and give defenders the upper hand, acting as a force multiplier for cybersecurity professionals to substantially reduce detection and response times. The results from deploying this technology on our own company networks are significant. On average, we ingest 90 billion events daily, distilling them to 26,000 alerts, and ultimately to a single incident requiring manual investigation.

Financial services institutions are steadily migrating to AI-driven SOC platforms where they benefit from:

- 4x more data ingested with a single, complete source of AI-ready data.
- Over 3,000 AI models with real-time prevention and detection for a full context of threats.
- Automated operations to accelerate SOC workflows resulting in 75% less analyst workload and a 90% reduction in MTTR.

One customer, a global financial markets utility, had several overlapping products that were not talking to each other, leading to cumbersome and inefficient processes and overworked analysts. After deploying an AI-powered solution, their MTTR collapsed from 24 hours to 14 minutes. After deploying this same tool, a global insurance company:

- Prevented 22,831 threats and processed 113,271 threat indicators in less than five seconds, and
- Saved 3,000 hours on an annual basis.

Another large bank leveraging the AI-powered SOC saw similarly transformative outcomes, tremendous efficiency gains, and reduced SOC staff attrition:

- 180 hours/year saved by automating SIEM – the system that collects and analyzes log data from across an organization's IT environment – and threat intel reporting;
- 500 hours/year saved by automated data collection and enrichment;
- 360 hours/year saved by automating 4 CTO playbooks;
- 240 hours/year saved with automated threat intelligence and case information enrichment.

These dramatic improvements are critical to stopping threat actors before they can encrypt systems or steal sensitive information – which is now frequently happening in mere hours. Simply put, none of this would be possible without the power of AI.

AI Security Accelerates AI Innovation

AI adoption is integral to America's innovation leadership, which is why Palo Alto Networks was proud to [support](#) America's AI Action Plan.

While AI offers significant benefits to financial institutions, as demonstrated above, its rapid growth largely outpaces the adoption of security measures designed to protect it and expands the attack surface. According to an [October 2025 survey from the Conference Board](#), nearly three-quarters of S&P 500 companies now flag AI as a material risk in their public disclosures, which is a jump from just 12% in 2023. And cybersecurity risk, specifically, was among the most commonly cited risks across all public disclosures.

Traditional security tools rely on static rules that are no match for today's dynamic AI risks. They are easily overwhelmed by alerts and often miss advanced attacks like multi-step prompt injections or adversarial manipulations. The rise of autonomous AI agents makes things even more challenging, as these agents can take unpredictable actions that are difficult to monitor with legacy methods. Most current tools are simply not built to inspect or adapt to these behaviors in real time.

Rapid AI adoption has dramatically expanded the attack surface by exposing organizations' AI ecosystems (the infrastructure, data, models, applications, and agents) to unique threats that legacy cybersecurity solutions were not explicitly designed to address. Unlike traditional cyber exploits that target software vulnerabilities, AI-specific attacks can manipulate the very foundation of how an AI system learns and operates. These attacks are not just about breaching a network but also can be about corrupting the AI's probabilistic logic itself.

It is critical to recognize and address this security gap with defenses that are truly AI-native. AI security must be a cross-cutting imperative across and within every layer of the AI technology stack. By securing AI capabilities with equally advanced cybersecurity technologies, financial institutions can confidently accelerate safe AI adoption.

A Call to Action

Recognizing this new risk paradigm, we are encouraged by recent policy developments that reinforce that AI adoption and AI security can, and must, go hand in hand. American's AI Action Plan calls for "Secure-By-Design AI Technologies and Applications." It further notes, *"The U.S. government has a responsibility to ensure the AI systems it relies on – particularly for national security applications – are protected against spurious or malicious inputs. While much work has been done to advance the field of AI Assurance, promoting resilient and secure AI development and deployment should be a core activity of the U.S. government."*

Voluntary standards bodies, like NIST, are starting to weigh in, initiating work to develop control overlays for securing AI systems or AI security-specific profiles to established cybersecurity risk management standards, like the NIST Cybersecurity Framework.

We are also encouraged by recent federal actions to operationalize Secure AI by Design through acquisition. Most recently, the General Services Administration announced a governmentwide OneGov [agreement](#) with Palo Alto Networks to help federal agencies secure their AI deployments through a cost-effective and scalable platform.

Secure AI by Design Policy Roadmap

While the consensus on rapid AI adoption is broad, organizations frequently struggle with the lack of clarity on what effective AI security looks like in practice. To help close the gap between high-level intent and actionable strategy, we developed a Secure AI by Design [Policy Roadmap](#). The roadmap lays out a four-part construct for holistically understanding the unique attributes of the AI attack surface and threat environment (the “What”), ultimately guiding the development of purpose-built, actionable policy strategies and solutions for securing the AI era (the “How”).

Secure AI by Design is a comprehensive strategy that empowers organizations to unleash their full potential for AI innovation by fundamentally integrating security throughout the entire AI lifecycle and across the AI ecosystem. This proactive stance ensures that security is a feature, not an afterthought, which is crucial for building trust, maintaining compliance, and mitigating risks.

By embedding security controls from the start, Secure AI by Design provides the visibility, control, and protection necessary to confidently build and deploy AI-powered applications at enterprise scale. Key components of this portfolio, such as AI access security, security posture management, and AI runtime protection, work together to safeguard sensitive training data, secure the AI supply chain, and protect running models against novel threats. This unified, end-to-end security solution allows organizations to focus on the business benefits of AI – like efficiency and innovation – without compromising the confidentiality, integrity, and availability of their AI systems.

The Secure AI by Design approach helps address the four security imperatives organizations most pressingly face in AI adoption:

1. **Secure the use of external AI tools:** Organizations must continuously discover and inventory AI tools, applications, and agents used across the enterprise – including “shadow AI” accessed via browsers or APIs – to govern model risk through scanning and policy, and protect usage through continuous monitoring for emerging attack vectors such as prompt injection, model extraction, and data exfiltration.
2. **Secure underlying AI infrastructure and data:** Organizations must continuously assess security, safety, and compliance risks across infrastructure, applications, models, and datasets – both in the supply chain and at runtime – through automated posture

management, model scanning for malicious or anomalous components and backdoors, and continuous adversarial testing.

3. **Safely build and deploy AI applications:** Security must be integrated into development and deployment via red teaming tailored to AI systems, configuration baselines for inference-time controls and safe tool invocation, guardrails for transactions, and mechanisms to block unsafe or risky models and patterns in production.
4. **Monitor and control AI agents:** As autonomous and semi-autonomous agents proliferate, security must center on identity-first controls, least-privilege access, scoped tool permissions, separation of duties, and governance over agent-to-agent and agent-to-system communications, alongside runtime monitoring for anomalous behaviors.

Leveraging Secure AI by Design imperatives will help to build a framework where security controls and governance are key tenets of AI innovation. Securing the entire AI ecosystem from development through deployment and use – not added as an afterthought – will best position the financial services sector to address the complex threats emerging from rapid AI adoption and fully embrace the benefits of AI.

Secure AI by Design must be anchored in enterprise governance and clear lines of accountability. Financial institutions should maintain risk-tiered AI inventories, document model lineage and intended use, identify and enforce strict access controls to sensitive data, and implement testing and monitoring commensurate with risk. Governance structures, centered on Secure AI by Design, should enable board and senior management oversight, ensure auditable logs across the AI lifecycle, and align with established model risk practices familiar to prudentially regulated firms.

Recommendations to Drive AI Innovation in Financial Services

Palo Alto Networks is proud to be an integrated national security partner with the federal government and stands ready to help. To that end, we developed a set of recommendations for policymakers to consider at this pivotal moment for our nation's cyber defense and AI leadership:

1. Promote AI-driven security operations. Encourage modernization of security operations across the financial services sector by recognizing AI-driven SOC platforms as a best practice to improve detection, response, and resilience. Supervisory guidance should emphasize measurable outcomes – such as reductions in MTTD and MTTR.
2. Champion voluntary Secure AI by Design frameworks. Embed Secure AI by Design across the financial services ecosystem to secure the use of external AI tools, secure underlying infrastructure and data, monitor and control AI agents, and safely build and deploy AI apps.
3. Ensure that AI policies safeguard cybersecurity and innovation. Policymakers should carefully tailor any new guardrails to ensure they don't unintentionally restrict the use of AI-powered tools for cyber defense. Regulatory proposals should be risk-based and

explicitly protect the ability of AI developers or deployers to ensure, maintain, and improve network and information security or to prevent, detect, protect against, or respond to cybersecurity threats.

4. Enable secure innovation through controlled experimentation. Establish AI innovation labs and regulatory sandboxes across the prudential and market regulators to allow banks, insurers, payment companies, and fintechs to test AI systems – including cybersecurity for AI – in controlled environments. Applications should include clear risk management plans covering data protection – especially intellectual property and proprietary information, model robustness testing, and misuse prevention, alongside success criteria that quantify security outcomes and operational benefits.
5. Strengthen public-private collaboration on AI security best practices and AI-enabled threats. Encourage regular, operationally focused exchanges between financial institutions, cybersecurity providers, and regulators to share indicators, detection methods, red team findings, and best practices for securing AI models and infrastructure. Focus particular attention on AI-enabled fraud, identity abuse, and deepfake-driven social engineering targeting payments and high-value transactions.

Building the AI-Ready Ecosystem: People and Partnerships

AI innovation and secure deployment requires people, processes, and technology working in concert. As a Financial Services Information Sharing and Analysis Center (FS-ISAC) sector advisor, Palo Alto Networks contributes to a number of timely reports analyzing the current threat landscape and trends facing financial institutions and actively supports the work of the AI Risk Working Group as it explores AI in cybersecurity and the cybersecurity of AI. Palo Alto Networks is also proud to be a founding Alliance member of CISA's Joint Cyber Defense Collaborative (JCDC), and one of the original private sector partners in the JCDC's AI working group, which developed CISA's AI Cybersecurity Collaboration Playbook.

As a member of the Cyber Risk Institute (CRI) Innovator Program, Palo Alto Networks helps member firms implement the Financial Services Cybersecurity Profile. This harmonized compliance framework aligns with major standards, including NIST Cybersecurity Framework 2.0, the NIST Ransomware Framework, CISA's Cross-Sector Cyber Performance Goals, and SEC disclosure rules. By acting as a common global baseline for regulator examinations, this framework allows financial institutions to optimize compliance resources, reduce reconciliation time for exam issues, and simplify security oversight.

With AI and automation central to modern cyber defenses, it is critical we educate and train the cyber workforce of tomorrow with the advanced skills required for meaningful jobs that complement technological innovation. To that end, Palo Alto Networks is a proud signer of the Pledge to America's Youth. Led by the great work of the Palo Alto Networks Cybersecurity Academy, we are integrating AI into our core curriculum and offering hands-on, AI-in-action labs.

Thank you for your leadership on this issue and for the opportunity to testify. I look forward to your questions.

Chairman HILL. Thank you very much.

Mr. Branch, you are now recognized for 5 minutes for an oral presentation of your testimony.

**STATEMENT OF JOSHUA BRANCH, BIG TECH
ACCOUNTABILITY ADVOCATE, PUBLIC CITIZEN**

Mr. BRANCH. Thank you, Chairman Hill, Ranking Member Waters, and members of the committee. My name is J.B. Branch. I am an artificial intelligence policy expert at Public Citizen, a non-profit with more than 1 million members and supporters across the country.

Each day, we fight for everyday Americans by defending democracy, resisting corruption, and challenging corporate greed. I am here today to talk about the difference between responsible AI innovation, and the current reckless push by Big Tech to undermine State laws, weaken consumer protection, and place all of us at the mercy of a handful of AI billionaires.

For decades, the default posture toward regulating new technology has been deference to industry. Congress deferred to the expertise of social media companies. We now live with the consequences, including rampant misinformation and harms for children. We cannot make the same mistake with AI.

The scale, speed, and autonomy of AI creates risks far beyond previous technology. The good news is that most AI regulations are rooted in common sense. Algorithms should not discriminate. Companies should be held accountable for harm. Nonconsensual deep fake pornography is a devastating crime. These are American values and Americans agree. A Gallup poll shows 97 percent of Americans agree that AI should be subject to regulation—97 percent. States across the country have responded with bipartisan, common-sense safeguards that reflect this democratic will in action.

Yet, instead of respecting that will, we have seen relentless attempts to override it. Over summer, some in Congress attempted to strip all State AI laws. Even worse, they tried to slip the proposals into the must-pass National Defense Authorization Act. Big Tech tried to use our national security as leverage to avoid accountability.

What was once called a moratorium is now being repackaged as a sandbox. These are all the same: deregulation schemes designed to invalidate all existing safeguards and the hypocrisy is striking. Big Tech is attacking many of the State-based AI laws they helped to write. They praised those laws locally while lobbying to destroy them nationally.

I am equally alarmed by President Trump referring to basic protections as dangerous ideology. Several of the administration's policy priorities target civil rights principles in AI but fairness in AI simply means preventing discrimination, sexism, and antisemitism.

While the Trump Administration bashes equality as a dangerous ideology, it has simultaneously entered a Federal contract with Elon Musk's Grok, an AI system that Office of Science and Technology Policy (OSTP) Director Kratsios testified, violated the administration's own principles. Grok's behavior is well documented: racist slurs, sexism, and even referring to itself as Mecca Hitler. Is

this the type of AI we want deployed throughout the U.S. Federal Government?

I also want to speak about the impact AI will have on workers and rural communities like the one I was raised in central Pennsylvania. These communities know what broken promises feel like. We remember when steel mills closed and new jobs did not come. Now, Big Tech companies are telling us that data centers and AI will be salvation, and we have heard this before. So let me be clear: Data centers are at the bottom of the tech stack. They receive major tax breaks while local communities foot the bill and most employ fewer people than a single Wal-Mart. They do not replace the jobs that communities have lost. This is another extraction model.

I want to offer simple guiding principles. Responsible innovation requires enforceable accountability. Public Citizen respectfully submits that the better path forward is not a mystery. Reject blanket preemption and deregulatory sandboxes, allowing States to respond to evolving harm. Require transparency. Companies must be able to explain how their AI systems work and how decisions are made. When AI systems cause harm, companies must be held accountable. Invest in regulatory enforcement. Laws mean nothing if they cannot be enforced. Congress must ensure regulators have the staff, the authority, and the resources to do their job.

We all share the same goal: a strong middle class and leadership in responsible AI. Leadership means protecting workers, children, and democracy at the same time we foster innovation.

This is a defining moment. It is a test of who governs America, the people or the most powerful corporations on earth. Public Citizen urges Congress to stand up to Big Tech, reject backdoor deregulation, and deliver real, enforceable guardrails. Thank you, and I look forward to answering your questions.

[The prepared statement of Mr. Branch follows:]

From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services

Testimony of J.B. Branch, Big Tech Accountability
Advocate, Public Citizen, before the House
Committee on Financial Services

@jbbranch.bsky.social

December 10, 2025



December 10, 2025

Chairman French Hill and Ranking Member Maxine Waters
U.S. House Committee on Financial Services
U.S. House of Representatives
2128 Rayburn House Office Building
Washington, D.C. 20515

Chairman Hill, Ranking Member Waters, and Members of the Committee:

I am J.B. Branch, the Big Tech Accountability Advocate at Public Citizen and an expert in Artificial Intelligence (AI) governance. Public Citizen is a national nonprofit consumer advocacy organization with more than one million members and supporters nationwide. Since our founding in 1971, we have worked to ensure that government and corporate power are transparent, accountable, and responsive to the public interest. Public Citizen was at the forefront of responsible AI long before ChatGPT became mainstream. Our research and policy analysis has consistently warned of the very harms we witness today including AI-related threats to democracy, consumer manipulation and harm, worsening inequality, abusive working conditions, AI usage in warfare, and environmental impacts related to AI.¹

In the context of emerging technologies, Public Citizen advocates for innovation that is tethered to enforceable safeguards, democratic oversight, and meaningful public accountability. We commend the Committee for convening this hearing to examine the future of AI policy at a moment of extraordinary technological acceleration and public risk.

There is no doubt that AI will shape the American economy, workforce, national security, and democratic institutions for generations to come. **The only real question before Congress is who this technology will ultimately serve: the public or a narrow set of powerful corporate actors insulated from public accountability.** As this Committee

¹ Rick Claypool and Cheyenne Hunt, *Sorry in Advance!*, Public Citizen, April 18, 2023, <https://www.citizen.org/article/sorry-in-advance-generative-ai-artificial-intelligence-chatgpt-report/>; Craig Holman, *The Nature and Risks of AI-Generated Deepfakes in Political Communications*, Public Citizen, October 10, 2025, <https://www.citizen.org/article/the-nature-and-risks-of-ai-generated-deepfakes-in-political-communications/>; Robert Weissman and Savannah Wooten, *A.I. Joe: The Dangers of Artificial Intelligence and the Military*, Public Citizen, February 29, 2024, <https://www.citizen.org/article/ai-joe-report/>; Deanna Noel and Meghan Pazik, *Reigning in Big Tech: Policy Solutions to Address the Data Center Buildout*, Public Citizen, December 3, 2025, <https://www.citizen.org/article/reining-in-big-tech-policy-solutions-to-address-the-data-center-buildout/>; Tyson Slocum, *Congressional Testimony on Artificial Intelligence Data Centers Energy Needs*, Public Citizen, April 1, 2025, <https://www.citizen.org/article/congressional-testimony-artificial-intelligence-data-center-energy/>

considers questions of U.S. leadership in AI, Public Citizen urges lawmakers to recognize that AI will not be determined by stock prices or server capacity, but by whether our democratic institutions can still govern powerful technologies in the public interest.

Leadership within innovation requires moral clarity, civil rights protections, worker safeguards, consumer safety, and democratic governance.

Public Citizen’s work has shown that the harms associated with AI are no longer speculative. From deepfake election interference² and AI-generated child sexual abuse material³ to automated discrimination,⁴ workplace surveillance,⁵ and large-scale fraud,⁶ AI systems are already producing real-world damage at scale. National intelligences agencies,⁷ consumer protection regulators,⁸ and child safety organizations⁹ have repeatedly warned that AI has become a force multiplier for deception, criminal exploitation, and consumer harm.

At the same time, Congress is being pressed to pursue sweeping deregulatory proposals under the banner of “innovation.” This includes efforts to preempt state AI laws, weaken regulatory agencies, and the grant of broad immunity to AI developers. **Public Citizen strongly rejects the false premise that regulation and competitiveness are mutually exclusive.** The lesson of every major technological revolution, from railroads to pharmaceuticals to social media, is that the absence of early guardrails does not accelerate progress—it multiplies harms, destabilizes markets, and erodes public trust.

This testimony addresses six core issues now directly before this Committee: (1) persistent efforts to undermine state AI protections; (2) the politicization of fairness in AI

² Claudia Koon Ghee Wee, *Artificial Illusion: Global Governance Challenges of Deepfake Technology*, IAPP, April 23, 2025, <https://iapp.org/news/a/artificial-illusion-global-governance-challenges-of-deepfake-technology>

³ Rianna Pfefferkorn, *Addressing AI-Generated Child Sexual Abuse Material: Opportunities for Educational Policy*, Stanford Human-Centered Artificial Intelligence, July 21, 2025, <https://hai.stanford.edu/policy/addressing-ai-generated-child-sexual-abuse-material-opportunities-for-educational-policy>

⁴ Quinn, Emanuel, Urquhart, and Sullivan LLP, *When Machines Discriminate: The Rise of AI Bias Lawsuits*, Quinn Emanuel, August 18, 2025, <https://www.quinnemanuel.com/the-firm/publications/when-machines-discriminate-the-rise-of-ai-bias-lawsuits/>

⁵ AFL-CIO, *Artificial Intelligence: Principles to Protect Workers*, October 15, 2025, <https://aflcio.org/reports/workers-first-ai>

⁶ FBI, *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, Alert Number: I-120324-PSA, December 3, 2025, <https://www.ic3.gov/PSA/2024/PSA241203>

⁷ FBI, *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence*, May 8, 2024, <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>

⁸ Darren M. Walsh and Stuart D. Levi, *CFPB Comments on AI Offer Insights for Consumer Finance Industry*, August 23, 2024, <https://www.skadden.com/insights/publications/2024/08/cfpb-comments-on-artificial-intelligence>

⁹ Associated Press, *Advocacy Groups Urge Parents to Avoid AI Toys this Holiday Season*, November 21, 2025, <https://www.kcra.com/article/ai-toys-safety-holiday-warning/69512613>

governance; (3) the risks of politically driven censorship within AI; (4) the exploitation of workers and communities throughout the AI stack; (5) the growing risks posed by AI in the financial sector; and (6) the mounting evidence that the tech industry may be entering an AI investment bubble.

Public Citizen submits this testimony to urge Congress to abandon the deregulatory shortcuts of the past and instead build a durable federal AI framework that protects families, workers, consumers, civil rights, democratic institutions, and economic stability. That framework must establish a strong federal floor of protection while preserving the authority of states to respond to emerging harm in real time, especially as AI evolves faster than the currently polarized and paralyzed congressional process can realistically move. The stakes are no longer hypothetical. The harms are multiplying. The financial exposure continues to balloon. And the public remains vulnerable due to Congressional inaction.

I. Persistent Efforts to Undermine State AI Protections

In the absence of comprehensive federal AI legislation, states have emerged as the primary arena of meaningful AI governance in the United States. Over the past several years, state legislatures across the country have enacted bipartisan protections addressing deepfake abuse, algorithmic discrimination, biometric surveillance, automated hiring, consumer deception, and child safety. These laws reflect democratic will in action. They are not theoretical policy exercises. They are pragmatic responses to real-world harms that communities are already experiencing and demanding accountability.

Yet rather than build upon this state-led momentum, powerful interests in Washington pursue a coordinated campaign to dismantle it. Earlier this year, Republicans advanced one of the most sweeping deregulatory proposals in the history of U.S. technology policy: a federal AI moratorium that would have frozen the enforcement of state AI laws nationwide.¹⁰ The proposal would have barred states from enforcing existing protections for years at precisely the moment when AI-generated fraud, deepfake abuse, consumer deception, and automated discrimination are accelerating.¹¹

This proposal was extraordinary not only for its breadth, but for what it represented philosophically: a declaration that democratic state action must be suspended to preserve corporate freedom from oversight. The American public rejected that premise decisively.

¹⁰ Anthony Adragna, ‘Not at all Dead’: Cruz says AI Moratorium will Return, Politico, September 16, 2025, <https://www.politico.com/news/2025/09/16/not-at-all-dead-cruz-says-ai-moratorium-will-return-00566369>

¹¹ *Id.*

Ninety-seven percent of Americans agree that AI safety and security should be subject to rules and regulations, according to a Gallup poll.¹² In a rare moment of near-unanimity, the U.S. Senate defeated the moratorium proposal by a 99–1 vote,¹³ delivering a bipartisan rebuke to the idea that AI companies should be shielded from accountability through federal fiat.

That vote should have ended the debate. It did not. After the moratorium failed, proponents attempted a quieter route. Behind the scenes, and at the final hour, Republicans tried to sneak in nearly identical AI preemption language into the National Defense Authorization Act (NDAA)—a must-pass national security bill traditionally reserved for military funding, not sweeping technology deregulation.¹⁴

This maneuver was deeply troubling for three reasons. First, it attempted to use the urgency of national defense as political cover for sweeping corporate immunity in hopes that the American public and civic tech advocates were not being vigilant. Second, it sought to override state civil rights, consumer protection, and child safety laws without public debate, hearings, or meaningful scrutiny. Thirdly, it continued Republican efforts to pursue blanket corporate immunity in an entirely unrelated must-pass legislative vehicle. This was not governance. It was a deliberate attempt to subordinate the democratic process to corporate privilege.

Once again, bipartisan opposition prevailed.¹⁵ The preemptive language was ultimately kept out. But the strategy was unmistakable: when transparency fails, try stealth.

Most recently, obsession over this poorly considered deregulatory campaign has moved into President Trump’s executive branch. A leaked draft executive order would reportedly direct the Department of Justice to actively challenge state AI laws on the grounds that they “burden interstate commerce” and interfere with federal priorities.¹⁶ In effect, this order would weaponize federal litigation to achieve what Congress refused to authorize: nationwide invalidation of state AI protections.¹⁷

¹² Benedict Vigers and Justin Lall, *Americans Prioritize AI Safety and Data Security*, Gallup News, September 16, 2025, <https://news.gallup.com/poll/694685/americans-prioritize-safety-data-security.aspx>

¹³ U.S. Senate, *Senate Strikes AI Moratorium from Budget Reconciliation Bill in Overwhelming 99-1 Vote*, July 1, 2025, <https://www.commerce.senate.gov/2025/7/senate-strikes-ai-moratorium-from-budget-reconciliation-bill-in-overwhelming-99-1-vote/8415a728-fd1d-4269-98ac-101d1d0c71e0>

¹⁴ Julia Shapero and Sudiksha Kochi, *AI Showdown Splits Republicans in High-Stakes NDAA Talks*, The Hill, December 2, 2025, <https://thehill.com/policy/technology/5628534-trump-lawmakers-battle-ai/>

¹⁵ Ashley Belanger, *Republicans Drop Trump-ordered Block on State AI Laws from Defense Bill*, ArsTechnica, December 3, 2025, <https://arstechnica.com/tech-policy/2025/12/republicans-once-again-thwart-trumps-push-to-block-state-ai-laws/>

¹⁶ Public Citizen, *Legal Analysis of Leaked Draft AI Preemption Executive Order*, November 21, 2025, <https://www.citizen.org/article/legal-analysis-of-leaked-draft-ai-preemption-executive-order/>

¹⁷ *Id.*

If finalized, such an order would represent an unprecedented, reckless and illegal misuse of executive power to extinguish state consumer protection, civil rights, and child safety laws in service of industry demands. It would bypass Congress, override state legislatures, and concentrate extraordinary regulatory power inside the White House. This is precisely the opposite of democratic governance.

Taken together, these three efforts—the failed federal moratorium, the NDAA insertion attempt, and the leaked executive order—are not isolated events. They form an intentional Republican strategy backed by Big Tech political spending: (1) Freeze state enforcement through Congress; (2) if that fails, smuggle preemption into must-pass legislation; (3) and finally, override states through executive action. Each step moves further away from democratic accountability and closer to centralized corporate immunity.

All of this is at the behest of the AI industry, which argues that their companies should not be governed by the same rule of law that applies to every other powerful industry in America. Big Tech companies, who have invested heavily in AI, have also invested heavily in political spending. Between 2024 and 2025 large tech or electronic companies have spent over \$764.5 million in political spending.¹⁸ Over 75 percent of this was donated to Republican candidates and nearly half (46 percent) came from Elon Musk alone.¹⁹

It is important to underscore that states did not rush to regulate AI because of political ideology. They acted because Congress has failed to enact meaningful AI regulations. States legislated because deepfake exploitation,²⁰ automated discrimination,²¹ biometric surveillance,²² and AI-driven scams were already harming their residents.²³ To now strip those protections miles away in Washington, D.C.—after communities have debated them, passed them on a bipartisan basis, and begun enforcing them—would be a direct assault on federalism, democratic self-governance, and public trust.

This strategy leverages preemption, not as a floor for protection, but as a ceiling for accountability. Moreover, Congressional Republicans have not provided any meaningful

¹⁸ Rick Claypool, *Robo-Trump: Big Tech's Big Spending and the Republican Effort to Delete State Laws Against AI Harms*, Public Citizen, November 21, 2025, <https://www.citizen.org/article/robo-trump-big-tech-big-spending-and-republican-effort-delete-state-ai-laws/>

¹⁹ *Id.*

²⁰ Ilana Beller, *Tracker: State Legislation on Deepfakes in Elections*, Public Citizen, October 20, 2025, <https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/>

²¹ Gabrielle Martin, *Illinois Enacts New AI Legislation, Joining Colorado as the Only States Regulating Algorithmic Discrimination in Private Sector use of AI Systems (US)*, Employment Law Worldview, August 19, 2024, <https://www.employmentlawworldview.com/illinois-enacts-new-ai-legislation-joining-colorado-as-the-only-states-regulating-algorithmic-discrimination-in-private-sector-use-of-ai-systems-us/>

²² Bobby Allyn, *With no Federal Facial Recognition Law, States Rush to Fill Void*, NPR, August 28, 2025, <https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy>

²³ Bryan Cave Leighton Paisner, *US State-by-State AI Legislation Snapshot*, <https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html>

AI governance alternative. Instead, they seek to replace real-world safeguards with a vacuum. Those who are supporting federal preemption seem to believe in voluntary corporate promises. The past two decades of technologically driven social media harm should serve as a lesson that promises from the tech industry should not be taken at face value.

The public has learned from Congressional leaders' failure to reign in Big Tech companies during the social media experimentation of the early 2000s. While tech companies argued that Section 230 was an absolute necessity or that Congress should lean on their expertise, they unleashed onto the world a variety of harms that we have yet to control. Those harms include harmful algorithmic steering to children including self-harm and eating disorders;²⁴ election misinformation that challenges global stability;²⁵ and a toxic online atmosphere that has created echo chambers online while destroying neighborhoods in the real world.²⁶

Congress must learn from past mistakes and stand vigilant of AI just as the American public has. Polling demonstrates Americans reject the tech industries push to self-regulate AI by a 6-1 margin.²⁷ This includes 72% of Americans who prefer slowing down the development of AI and 82% of voters who say they don't trust tech company executives to self-regulate.²⁸ The American people are not asking for a pause on accountability. They are asking for protection. And the states have already begun to deliver.

II. The Politicization of Fairness and Civil Rights in AI Governance

As efforts to dismantle state AI protections have accelerated, a parallel and equally dangerous trend has emerged: the deliberate politicization of fairness, nondiscrimination, and civil rights in artificial intelligence governance. In recent years, some policymakers have sought to rebrand our most basic Constitutional principles as "ideological," "woke," or even "dangerous." This reframing is not accidental. It is a strategic effort to delegitimize civil rights enforcement throughout the U.S.

²⁴ Center for Countering Digital Hate, *YouTube's Anorexia Algorithm: How YouTube Recommends Eating Disorder Videos to Young Girls*, December 10, 2024, <https://counterhate.com/research/youtube-anorexia-algorithm/>

²⁵ Danielle Draper and Sbine Neschke, *The Pros and Cons of Social Media Algorithms*, October 2023, Bipartisan Policy Center, https://bipartisanpolicy.org/wp-content/uploads/2023/10/BPC_Tech-Algorithm-Tradeoffs_R01.pdf

²⁶ Jennifer Ouellette, *Study: Social Media Probably can't be Fixed*, ArsTechnica, August 13, 2025, <https://arstechnica.com/science/2025/08/study-social-media-probably-cant-be-fixed/>

²⁷ Sarah Fortinsky, *Majority of Americans are Concerned about Rapidly Developing AI: Poll*, The Hill, August 9, 2023, <https://thehill.com/homenews/4145203-majority-of-americans-are-concerned-about-rapidly-developing-ai-poll/>

²⁸ *Id.*

But at its core, algorithmic fairness simply means that automated systems should not produce discriminatory outcomes based on race, gender, religion, disability, age, or other protected characteristics.²⁹ That principle is neither novel nor partisan. It is embedded in decades of U.S. civil rights law, including the Civil Rights Act of 1964,³⁰ the Fair Housing Act,³¹ the Equal Credit Opportunity Act,³² and the Voting Rights Act.³³

Yet today, those same nondiscrimination principles are increasingly being recast as political ideology when applied to AI. The Trump administration’s own “Woke AI” executive order claims efforts to prevent biased algorithmic outcomes amount to “ideological biases or social agendas.”³⁴ This perversion of reality turns the Constitution on its head.

Equal protection under the law is not an ideology. It is quite literally the law and a principle underlying the premise of the American Dream. When policymakers treat civil rights as optional or partisan in the AI context, they are not defending neutrality. They are authorizing discrimination by default.

From a technical and legal perspective, fairness in AI governance involves three basic obligations:

1. **Bias detection and mitigation:** Developers must test for disparate impacts before deployment.³⁵
2. **Transparency and auditability:** Regulators and impacted users must be able to examine how decisions are made.³⁶
3. **Legal accountability:** When automated systems violate civil rights, there must be clear avenues for enforcement and remedy.³⁷

²⁹ Stanford Encyclopedia of Philosophy, *Algorithmic Fairness*, July 30, 2025, <https://plato.stanford.edu/entries/algorithmic-fairness/>

³⁰ Civil Rights Act of 1964, 42 U.S.C. § 2000, Pub. L. No. 88-352, 78 Stat. 241 (1964).

³¹ Fair Housing Act, 42 U.S.C. § 3601–3619 (1968 & Supp. V 2023) (amended by Pub. L. 90–284).

³² Equal Credit Opportunity Act, 15 U.S.C. § 1691 (2020).

³³ Voting Rights Act of 1965, Pub. L. 89-110, 79 Stat. 437.

³⁴ President Donald J. Trump, *Preventing Woke AI in the Federal Government*, Exec. Order No. 14099 (July 23, 2025), <https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government>

³⁵ Kate Goddard, Abdul Roudsari & Jeremy C. Wyatt, *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. Am. Med. Inform. Assoc. 121 (Jan.–Feb. 2012), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3240751/>

³⁶ Nagadivya Balasubramaniam et al., *Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements*, 159 Info. & Software Tech. 107197 (2023), <https://www.sciencedirect.com/science/article/pii/S0950584923000514>.

³⁷ NTIA, *Liability Rules and Standards*, in *AI Accountability Policy Report: Using Accountability Inputs*, Mar. 27, 2024, <https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs/liability-rules-and-standards>

These principles already govern credit decisions,³⁸ employment screening,³⁹ housing access,⁴⁰ and voting protections.⁴¹ AI does not change the need for civil rights enforcement; it amplifies it. Automated systems can now deny loans,⁴² screen out job applicants,⁴³ flag people for surveillance,⁴⁴ and influence elections on a scale never seen before, often without human oversight.⁴⁵

When lawmakers suggest that addressing these harms is suspect, the result is not neutral. The result is that companies deploying high-risk systems profit while impacted communities are left with no meaningful recourse. **Public Citizen's position is straightforward: civil rights are a legal and moral obligation.** Congress cannot meaningfully claim leadership in responsible AI while allowing the foundational principle of equal protection to be caricatured as partisan ideology.

³⁸ See *supra* note 32.

³⁹ 42 U.S.C. § 2000e-2(a)(1) (prohibits discrimination in employment).

⁴⁰ See *supra* note 31.

⁴¹ See *supra* note 25.

⁴² Lehigh University News, *AI Exhibits Racial Bias in Mortgage Underwriting Decisions*, Lehigh University News (Aug. 20, 2024) <https://news.lehigh.edu/ai-exhibits-racial-bias-in-mortgage-underwriting-decisions>

⁴³ Stefane Milne, *AI tools show biases in ranking job applicants' names according to perceived race and gender*, UW News (Oct. 31, 2024) <https://www.washington.edu/news/2024/10/31/ai-bias-resume-screening-race-gender/>

⁴⁴ Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color*, Brookings (Apr. 12, 2022) <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>

⁴⁵ Amy Hamblin, *Tackling the Threat of Deepfakes in Our Elections*, NextGen Policy (Oct. 17, 2024), <https://www.nextgenpolicy.org/lets-talk/tackling-the-threat-of-deepfakes-in-our-elections/>.

III. Federal Inconsistency and the Risks of Politically Driven AI Deployment

Even as some policymakers seek to dismantle state protections and recast civil rights as “ideological,” the federal government’s own conduct with respect to AI reveals a troubling pattern of internal inconsistency and politically driven deployment. On paper, federal AI policy emphasizes safety, transparency, and public trust.⁴⁶ In practice, those commitments are increasingly undermined by contradictory actions that prioritize speed, political loyalty, and corporate alignment over public protection. This inconsistency directly weakens the credibility of federal AI governance and signals to industry that safety principles are negotiable.

These commitments mirror global norms reflected in international frameworks and emerging foreign AI laws.⁴⁷ They also align with long-standing U.S. traditions of consumer protection, civil rights enforcement, and product safety regulation. Yet at the same time, high-risk AI systems continue to be fast-tracked into sensitive federal contexts without the level of independent testing, auditability, or public disclosure that these very principles require. When safety frameworks exist primarily on paper, they become aspirational rather than enforceable. Put simply, aspirational governance is not governance at all.

The federal government’s procurement of Elon Musk’s Grok system is a stark example of this breakdown between stated principle and actual practice.⁴⁸ Grok has been publicly documented engaging in racist and antisemitic tirades,⁴⁹ spreading conspiratorial content,⁵⁰ and even referring to itself as “Mecha Hitler.”⁵¹ These are not edge cases or obscure technical glitches. They are clear signals that the system does not meet even basic standards of safety, non-discrimination, or reliability that federal AI policy claims to uphold.

⁴⁶ Office of Management and Budget, Executive Office of the President, *Memorandum for the Heads of Executive Departments and Agencies, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, M-25-21, (April 3, 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf> (“OMB M-25-21”);

Office of Management and Budget, Executive Office of the President, *Memorandum for the Heads of Executive Departments and Agencies, Driving Efficient Acquisition of Artificial Intelligence in Government*, M-25-22, (April 3, 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf> (“OMB M-25-22”).

⁴⁷ IAPP, *Global AI Law and Policy Tracker*, <https://iapp.org/resources/article/global-ai-legislation-tracker/>

⁴⁸ U.S. General Services Administration, *GSA and xAI Partner on \$0.42 per Agency Agreement to Accelerate Federal AI Adoption*, September 25, 2025, <https://www.gsa.gov/about-us/newsroom/news-releases/gsa-xai-partner-to-accelerate-federal-ai-adoption-09252025>

⁴⁹ Lisa Hagen, Huo Jingnan & Audrey Nguyen, *Grok AI Produces Antisemitic, Racist Content on X*, NPR (July 9, 2025), <https://www.npr.org/2025/07/09/nx-s1-5462609/grok-elon-musk-antisemitic-racist-content>.

⁵⁰ Derek Robertson, *Grok’s ‘White Genocide’ Glitch and the AI Black Box*, Politico (May 15, 2025), <https://www.politico.com/newsletters/digital-future-daily/2025/05/15/groks-white-genocide-glitch-and-the-ai-black-box-00352709>

⁵¹ Dylon Jones, *How Musk’s Grok Chatbot Ended up Praising Hitler*, Politico Magazine (July 10, 2025), <https://www.politico.com/news/magazine/2025/07/10/musk-grok-hitler-ai-00447055>.

Moving a system with this record toward federal deployment is not a neutral technical choice. It is a policy decision to tolerate behavior that would be unacceptable from any human federal employee⁵² unless, apparently, they happened to be President Trump's donor or friend.⁵³ It directly contradicts commitments to protect civil rights, prevent harmful content, and ensure trustworthy AI in government operations. It tells the market that adherence to federal AI principles is optional when politically connected vendors are involved.

That signal carries real consequences, because the federal government is one of the largest contract purchasers in the world.⁵⁴ That purchasing power shapes markets, sets standards, and confers legitimacy. When AI systems are deployed across federal agencies, they are not merely tools. They become symbols of official approval by the U.S. government, and by proxy, the American people.

Politicized procurement, where alignment with political leadership or ideological agendas substitutes for independent technical and civil rights evaluation, creates several systemic risks:

1. **Erosion of public trust:** Citizens are less likely to trust automated systems that appear to reflect political priorities rather than neutral safety standards.
2. **Regulatory capture through the back door:** Procurement becomes a substitute for regulation, granting practical immunity to selected vendors.
3. **Institutional lock-in:** Once embedded in federal infrastructure, flawed AI systems become costly and difficult to unwind.
4. **Export of unsafe norms:** U.S. procurement decisions influence what other governments adopt as acceptable practice.

In short, federal deployment choices now function as *de facto* global standard-setting. That power carries responsibility. But it is not being exercised with sufficient restraint.

The United States does not regulate AI in a vacuum. Federal policy choices send powerful signals to allies, adversaries, and multinational corporations. When U.S. institutions appear to downplay safety, weaken civil rights protections, or politicize algorithmic governance, those signals travel globally.

At a time when democratic governments are struggling to articulate credible alternatives to digital authoritarianism, inconsistency in U.S. AI governance weakens the moral

⁵² U.S. Department of Labor, *OSHA Workers Rights and Protections*, <https://www.osha.gov/workers>

⁵³ Rachel Leingang, *Trump Nominee Reportedly Boasted of 'Nazi Streak' in Group Chats*, The Guardian, October 20, 2025, <https://www.theguardian.com/us-news/2025/oct/20/trump-nominee-paul-ingrassia-group-chats>

⁵⁴ K & L Gates Public Policy and Law Practice, *Government Contracts and Procurement*, K&L Gates 2011, https://files.klgates.com/files/upload/public_policy_govt_contracts.pdf

authority of democratic oversight worldwide. A government that cannot consistently apply its own principles at home is poorly positioned to advocate for rights-respecting AI abroad.

Public Citizen urges Congress to recognize that federal inconsistency is not a neutral condition. It actively destabilizes trust, weakens civil rights enforcement, and invites corporate opportunism. If AI is to serve the public, the rules governing its deployment must be stable, enforceable, and insulated from political expediency.

IV. The Exploitation of Workers and Communities Through AI Infrastructure and Automation

As AI reshapes the economy, its physical and economic footprint is increasingly borne by workers and communities that are promised prosperity but too often receive disruption, higher costs, and fewer protections. Nowhere is this more evident than in the rapid buildout of data center infrastructure and the accelerating deployment of workplace automation.

Across the country, particularly in rural and economically distressed regions, communities are told that data centers and AI infrastructure represent the next great engine of economic revitalization.⁵⁵ State and local governments are encouraged to offer generous tax abatements, discounted electricity rates, land concessions, and expedited permitting in exchange for the promise of “high-tech jobs” and long-term economic growth.⁵⁶

This narrative is powerful. It is also misleading.

Data centers sit at the very bottom of the technology value chain. Their construction phase may generate a brief surge in temporary jobs, but once operational, most facilities require only a small permanent workforce. The largest data centers employ roughly 100 to 200 employees.⁵⁷ This is less employees than hired at a Walmart Superstore.⁵⁸ Meanwhile, the long-term economic burdens remain local: higher electricity prices, strained grids, increased water usage, and land converted to infrastructure that produces little sustained community wealth.⁵⁹

⁵⁵ See *supra* note 1, Tyson Slocum testimony.

⁵⁶ *Id.*

⁵⁷ Tom Dotan, *The AI Data-Center Boom is a Job-Creation Bust*, February 25, 2025, The Wall Street Journal, https://www.wsj.com/tech/ai-data-center-job-creation-48038b67?gaa_at=eafs&gaa_n=AWETSqTcyMiO56lqVqVS2H8r9XX6qes4JPfji8qfDi38-ltKJdVlkx4V7rhXlogfJI%3D&gaa_ts=6935ae60&gaa_sig=x0Rel4lelrTOxtbZTHIZzYFWB4IRckINQd7yT0tuosvop1qgcOtgF24d8G9-YfhKICzdtFqYVGvFA7tPWg1Kw%3D%3D

⁵⁸ Matthew Yglesias, *Maybe Wal-Mart Should Hire Some People*, Slate, April 4, 2025, <https://slate.com/business/2013/04/wal-mart-labor-saving-gone-too-far-superstore-needs-to-hire-some-people.html>

⁵⁹ See *supra* note 1, Tyson Slocum testimony.

Americans have seen this story before. Steel towns were promised stability. Shale gas communities promised prosperity. Offshoring was supposed to create “new opportunities.” Each cycle left workers more exposed, and communities more fragile. AI infrastructure is now being sold with the same familiar optimism and the same thin guarantees.

AI data centers are also among the most energy-intensive industrial facilities ever deployed.⁶⁰ Their electricity demand is measured in orders of magnitude. In many regions, utilities are already signaling that residential and small business ratepayers will bear the cost of grid expansion required to serve hyperscale AI infrastructure.⁶¹

This creates a deeply inequitable cost shift. Working families, many of whom will never directly benefit from AI development, are being asked to subsidize some of the wealthiest corporations on the planet. Meanwhile, environmental review processes are frequently accelerated or weakened in the name of “innovation competitiveness.”⁶² If AI is truly a national priority, then its infrastructure costs should be borne transparently and fairly—not quietly shifted onto households least able to absorb them.

Beyond physical infrastructure, AI is transforming the workplace itself. Employers are rapidly adopting AI systems for:

- **Productivity monitoring and worker surveillance**⁶³
- **Automated scheduling and performance scoring**⁶⁴
- **Hiring, promotion, and termination decisions**⁶⁵
- **Task automation and workforce “optimization”**⁶⁶

These systems are often introduced without collective bargaining, meaningful transparency, or worker consent.⁶⁷ Employees are essentially asked to trust algorithms they cannot inspect, challenge, or meaningfully appeal. The result is a profound shift in workplace power. Decisions are being moved away from human judgment and toward opaque automated control.

Without guardrails, AI-driven management systems can suppress wages, accelerate burnout, intensify monitoring, and undermine organizing rights.⁶⁸ And when displacement occurs, workers are often offered vague assurances of “reskilling” that do not match the scale or speed of job loss.

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² *Id.*

⁶³ See *supra* note 5.

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ *Id.*

“Reskilling” initiatives are often highlighted as a solution to workplace automation.⁶⁹ While retraining is important, history counsels caution. Often automation produces far fewer high-quality replacement jobs than were promised and, if created, those jobs are less visible and difficult to find.⁷⁰ Further, AI-driven displacement is unfolding at a speed that makes traditional retraining pipelines inadequate by comparison.⁷¹ Many of the jobs being automated are entry-level and mid-skill positions that historically served as rungs on the economic ladder.⁷² When those rungs disappear, the ladder itself ceases to exist.

A workforce policy built on aspirational retraining slogans is not a workforce policy at all. It is an abdication of responsibility that fits squarely within a broader political tradition of weakening labor protections and undermining unions in the name of “flexibility” and corporate efficiency.

If AI is to strengthen the middle class rather than hollow it out, Congress must intervene now—before infrastructure lock-in and automated management systems become permanent features of the economic landscape. The AI industry’s strategy follows the same political logic that has weakened labor standards and targeted unions for decades: move fast for corporations, move slow for workers. Now it’s been rebranded as ‘AI transition policy’—same script, same winners, same losers. **Public Citizen’s believes AI must not become another chapter in the long American history of privatized gains and socialized losses.**

⁶⁹ Jorge Tamayo et. al., *Reskilling in the Age of AI*, Harvard Business Review, September–October 2023, https://hbr.org/2023/09/reskilling-in-the-age-of-ai?utm_medium=paidsearch&utm_source=google&utm_campaign=domcontent&utm_term=Non-Brand&tpcc=paidsearch.google.dscontent&gad_source=1&gad_campaignid=20553599500&gbraid=0AAAD9b3uRf6T8iE3uqi0-sm_UAx65Uk&gclid=Cj0KCQiA6NTJBhDEARIsAB7QHD1sVmbOBnqOoPgcZZcJJdzBmygO4-VBioWB2UCGkLrjHOKspbK2K_IaAsv2EALw_wcB

⁷⁰ James Manyika et. al., *Jobs Lost, Jobs Gained: What the Future of Work will Mean for Jobs, Skills, and Wages*, McKinsey & Company, November 28, 2017, <https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages>

⁷¹ Samantha Subin, *AI is Already Taking White-Collar Jobs. Economists Warn there’s ‘much more in the tank’*, CNBC, October 22, 2025, <https://www.cnbc.com/2025/10/22/ai-taking-white-collar-jobs-economists-warn-much-more-in-the-tank.html>

⁷² Till Leopold, *How AI is Reshaping the Career Ladder, and Other Trends in Jobs and Skills on Labour Day*, World Economic Forum, April 30, 2025, <https://www.weforum.org/stories/2025/04/ai-jobs-international-workers-day/>

V. The Growing Risks Posed by AI in the Financial Sector

The financial sector has long been a proving ground for automation, and complex algorithmic systems. Artificial intelligence now threatens to amplify the sector's long-standing vulnerabilities—opacity, concentration, leverage, and misaligned incentives—while introducing new risks that regulators are only beginning to confront. In finance, small modeling errors, biased decision-making, or runaway automation can rapidly metastasize into systemic instability.⁷³

This makes the finance industry's adoption of AI more concerning. In finance, AI systems are no longer peripheral tools. They are increasingly embedded in core functions including⁷⁴ but not limited to:

- **Credit underwriting and loan pricing**
- **Fraud detection and transaction monitoring**
- **High-frequency and algorithmic trading**
- **Insurance underwriting and claims processing**
- **Consumer service, collections, and financial advising**
- **Market surveillance and risk management**

These systems shape who gets access to credit, at what price, under what terms, and how adverse decisions may be contested.⁷⁵ In short, AI is rapidly becoming a gatekeeper to economic opportunity. Yet many of these systems operate as black boxes, shielded from public scrutiny by trade secrecy, proprietary claims, and technical opacity.⁷⁶ That dangerous combination threatens transparency, which is the bedrock of trust.

Indeed, the financial industry's enthusiasm for opaque AI systems should raise alarms. This skepticism is well justified by the industry's own historical conduct. This is an industry whose history of redlining, discriminatory lending, and predatory financial products required repeated federal intervention.⁷⁷ AI does not erase that history. It threatens to replicate it by operating at an unprecedented scale, speed, and invisibility. AI systems trained on historical data can replicate and intensify past discrimination in credit, insurance, housing finance, and small-business lending.⁷⁸ Automated decision systems can deny

⁷³ Hilary J. Allen, *Driverless Finance*, Harvard Business Law Review, https://journals.law.harvard.edu/hblr/wp-content/uploads/sites/87/2020/03/HLB101_crop.pdf

⁷⁴ *Id.*; See also Gary Gensler, *Chapter 7, Artificial Intelligence Development and Policy Landscape*, December 2, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5842702; See also Todd Phillips, *The Risks of Generative AI Agents to Financial Services*, Roosevelt Institute, September 26, 2024, <https://rooseveltinstitute.org/publications/the-risks-of-generative-ai-agents-to-financial-services/>

⁷⁵ See *Id.*

⁷⁶ *Id.*

⁷⁷ Amalie Zinn et. al., *Building Trust in the Financial System is Key to Closing the Racial Wealth Gap*, Urban Institute, June 15, 2023, <https://www.urban.org/urban-wire/building-trust-financial-system-key-closing-racial-wealth-gap>

⁷⁸ See *supra* note 74.

thousands of applicants in seconds with no clear explanation, no meaningful appeal, and no accountability pathway.⁷⁹ Consumers are left with adverse outcomes while firms may claim there is no human decision-maker to confront.⁸⁰

Regulators and researchers have repeatedly documented biased outcomes in automated credit and insurance systems.⁸¹ When discrimination becomes automated, civil rights enforcement must become more robust. Yet the current administration's sustained attacks on civil rights protections threaten to make enforcement nearly impossible precisely when it is most needed.⁸²

Beyond consumer harm, AI poses macro-level risks to financial stability. In trading and market-making contexts, machine learning systems react to the same data at the same time, often using similar optimization strategies.⁸³ That creates the conditions for herding behavior, where large volumes of capital move in lockstep based on similar investor behavior.⁸⁴

History shows how dangerous this can be. High-frequency trading has already contributed to flash crashes and sudden evaporation of liquidity.⁸⁵ AI systems, which adapt dynamically and operate at light speed, magnify that instability.⁸⁶ When things go wrong, they go wrong faster and at a scale no human intervention can immediately arrest. The central danger therefore is not simply automation. It is automation without explainability, without oversight, and without enforceable guardrails.

AI also introduces a new and underappreciated form of systemic risk: technological concentration. A small number of cloud providers, chip manufacturers, and AI vendors now underpin vast portions of the financial system's digital infrastructure.⁸⁷ When those

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ Michael Akinwumi et. al., *AN AI Fair Lending Policy Agenda for the Federal Financial Regulators*, Brookings Institute, December 2, 2021, <https://www.brookings.edu/articles/an-ai-fair-lending-policy-agenda-for-the-federal-financial-regulators/>

⁸² The Leadership Conference on Civil and Human Rights, *Trump Administration Civil and Human Rights Rollbacks*, <https://civilrights.org/trump-rollbacks/>

⁸³ See *supra* note 74.

⁸⁴ *Id.*

⁸⁵ Andrei Kirilenko et. al., *The Flash Crash: The Impact of High Frequency Trading on an Electronic Market*, Commodity Futures Trading Commission, May 5, 2014, https://www.cftc.gov/sites/default/files/idc/groups/public/@economics/analysis/documents/file/occe_flashcrash0314.pdf

⁸⁶ Kevin Frazier, *Selling Spirals: Avoiding an AI Flash Crash*, Lawfare, November 8, 2024, <https://www.lawfaremedia.org/article/selling-spirals--avoiding-an-ai-flash-crash>

⁸⁷ Asad Ramzanali, *How to Regulate the Cloud: A Blueprint to Address the Market Failures and National Security Risks of Cloud Computing*, Vanderbilt Policy Accelerator, September 2025, <https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2025/09/18140135/How-to-Regulate-the-Cloud.pdf>

same firms simultaneously supply compute power, AI models, and financial services platforms, single points of failure multiply across markets.⁸⁸

A rising wave of internet provider outages has made clear how deeply market stability now depends on a handful of infrastructure vendors.⁸⁹ As AI deepens this dependence, the resilience of the financial system becomes inseparable from the business incentives of a handful of Big Tech monopolists. This is both a cybersecurity issue and a structural market risk.

The financial system is not just another industry—it is the circulatory system of the economy. When AI distorts that system, the harm does not remain confined to trading floors or balance sheets. It infects households, small businesses, municipalities, and even national and global economies. In finance, experimentation without guardrails historically cost Americans dearly. Chaotic securitization of mortgages, unchecked, led to the housing bubble whose rupture cost millions their jobs, savings, and homes spiraling the nation into the Great Recession.

However, if Congress allows AI to reshape financial markets behind closed doors, without transparency, civil rights enforcement, and systemic risk controls, the price will not be paid only by individual consumers. It will be paid by the stability of the U.S. economy itself. **Public Citizen rejects the notion that Wall Street should be allowed to experiment on the public with diminished accountability. Congress must act with urgency and clarity to prove that democratic governance still has the power to discipline the most powerful sectors of the economy.**

⁸⁸ *Id.*

⁸⁹ Kevin Collier, *Severe Internet Outages Keep Happening—and They Might Get Worse*, NBC News, November 23, 2025, <https://www.nbcnews.com/tech/internet/internet-outages-aws-microsoft-cloudflare-rcna245043>

VI. The Mounting Evidence That the United States May Be Entering an AI Investment Bubble

Alongside the rapid deployment of AI across the economy, the United States is witnessing an unprecedented surge of speculative capital flowing into AI infrastructure, startups, and compute supply chains.⁹⁰ The sheer scale, speed, and structure of this investment raise a serious and unavoidable question for policymakers: **are we witnessing the early stages of a destabilizing AI investment bubble?**

This is a risk increasingly flagged by economists,⁹¹ market analysts,⁹² and even some of the industry's most enthusiastic participants.⁹³ An economic bubble occurs when asset prices rise far beyond what underlying economic fundamentals can reasonably support. Bubbles are rarely obvious in real time. They are typically characterized by:

- **Unsustainable price growth**
- **Circular financing that inflates apparent demand**
- **Heavy reliance on debt and leverage**
- **Narratives of “this time is different”⁹⁴**

Each of these warning signs is now visible in the AI sector. Unlike traditional public companies, many of the largest AI firms operate behind a veil of limited financial disclosure.⁹⁵ As a result, standard valuation metrics, such as price-to-earnings ratios, are often impossible to apply.⁹⁶ What is clear, however, is that current AI valuations dramatically exceed what existing revenue, let alone profit, can plausibly justify.⁹⁷

Private market valuations for leading AI firms have reached levels that imply decades of near-perfect execution, exponential productivity gains, and extraordinary profit not

⁹⁰ Paulo Carvao, *Is AI a Boom or a Bubble?* October 16, 2025, Harvard Business Review, <https://hbr.org/2025/10/is-ai-a-boom-or-a-bubble>; See also Jessica Wong, *Wall Street is Driving the AI Surge. But Millions of Americans Could be in the Blast Zone if the Bubble Bursts*, YahooNews, December 4, 2025, <https://finance.yahoo.com/news/wall-street-driving-ai-surge-210000413.html>

⁹¹ Thibault Sprilet, *The AI Boom has all 4 Classic Bubble Signs—and it could pop in 2026 if Interest Rates Rise, a Top Economist Says*, Business Insider, December 2, 2025, <https://www.businessinsider.com/ai-boom-has-4-bubble-signs-could-burst-2026-economist-2025-12>

⁹² Eduardo Porter, *The Question isn't Whether the AI Bubble will Burst—But what the Fallout will be*, The Guardian, December 1, 2025, <https://www.theguardian.com/technology/2025/dec/01/ai-bubble-us-economy>

⁹³ Dylan Butts, *OpenAI's Sam Altman Sees AI Bubble Forming as Industry Spending Surges*, CNBC News, August 18, 2025, <https://www.cnbc.com/2025/08/18/openai-sam-altman-warns-ai-market-is-in-a-bubble.html>

⁹⁴ See *supra* note 91.

⁹⁵ Jacqueline Gu and Cade Metz, *How OpenAI Uses Complex and Circular Deals to Fuel its Multibillion-Dollar Rise*, The New York Times, October 31, 2025,

<https://www.nytimes.com/interactive/2025/10/31/technology/openai-fundraising-deals.html>

⁹⁶ Daron Acemoglu, *The Simple Macroeconomics of AI*, MIT, April 5, 2024,

<https://economics.mit.edu/sites/default/files/2024-04/The%20Simple%20Macroeconomics%20of%20AI.pdf>

⁹⁷ *Id.*

experienced by any other sector. Yet, as multiple independent studies have shown, the real-world productivity impact of generative AI remains modest, inconsistent, and in many sectors statistically indistinguishable from zero.⁹⁸ When valuation growth runs far ahead of demonstrated economic returns, downside risk increases.⁹⁹

Perhaps the most troubling structural feature of today's AI economy is the extent of circular financing. In multiple high-profile cases, capital flows from large technology firms and financial conglomerates into AI developers, only to return to those same firms as cloud computing payments, chip purchases, or infrastructure contracts.¹⁰⁰ This creates the illusion of booming external demand when much of the apparent revenue is recycled funding.¹⁰¹ Circular financing can inflate valuations, obscure underlying market weakness, and mask the extent to which AI firms remain dependent on a narrow set of capital providers.¹⁰² Neighbors who do each other's washing isn't a viable economy. It is a classic ingredient in systemic economic fragility.¹⁰³

Despite extraordinary capital expenditure, leading macroeconomic research suggests that AI's contribution to near-term economic growth is likely to be modest, not revolutionary.¹⁰⁴ Even optimistic estimates project only fractional increases in total factor productivity over the next decade.¹⁰⁵ At the same time, AI-driven gains are expected to flow disproportionately to capital owners, widening inequality between labor and investors.¹⁰⁶ This mismatch between speculative investment and measured productivity is one of the clearest signals of bubble dynamics. Put bluntly: we are spending like a revolution is guaranteed, while the data says it is far from assured.

Another classic bubble indicator now flashing in the AI sector is leverage. Major AI investors have taken on substantial margin loans and bridge financing to sustain their

⁹⁸ *Id.*; See also *supra* note 94; See also Kate Niederhoffer et. al., *AI-Generated "Workshop" is Destroying Productivity*, Harvard Business Review, September 22, 2025, <https://hbr.org/2025/09/ai-generated-workshop-is-destroying-productivity>; Dritjon Gruda and Brad Aeon, *Seven Myths about AI and Productivity: What the Evidence Really Says*, California Management Review, October 16, 2025, <https://cmr.berkeley.edu/2025/10/seven-myths-about-ai-and-productivity-what-the-evidence-really-says/>

⁹⁹ See *supra* note 96.

¹⁰⁰ See *supra* note 95.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ See *supra* note 94.

¹⁰⁴ See *supra* note 99.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

capital commitments.¹⁰⁷ When asset prices rise, leverage magnifies gains.¹⁰⁸ When sentiment turns, it magnifies losses and accelerates forced liquidation.¹⁰⁹ This is precisely how localized speculative manias metastasize into broader financial and economic crises. AI's infrastructure buildout is now so large that a sharp contraction would no longer be a niche tech-sector event. It would be macroeconomically meaningful.

The most common historical comparison is the late-1990s dot-com bubble. The parallels include: euphoric narratives, explosive valuations, infrastructure overbuild, and the promise of a productivity revolution just over the horizon.¹¹⁰ But there is one crucial difference. During the dot-com era, speculative excess was largely concentrated in Silicon Valley equity markets.¹¹¹ Today's AI boom is also deeply embedded in physical infrastructure, energy grids, private credit markets, and global supply chains.¹¹² That suggests that the economic footprint of a potential AI crash could be broader and more painful. Not only would the share price of major public companies spending on AI decline, which could harm worker pension plans, but municipalities helping with data centers or associated power plants might suffer,

It may be tempting for many in Congress to believe in the AI hype. The persistent attempts to pursue federal preemption of state AI regulations suggest that many on Capitol Hill are fully invested. However, one of the most dangerous responses to speculative excess is denial. When governments treat bubble warnings as hostile to "innovation," they amplify the eventual fallout. Smart economic governance does not assume that every boom ends in catastrophe. But it also does not ignore warning signs until markets collapse.

Congress must not regulate AI as if the upside is guaranteed, and the downside is negligible. The downside risks are already visible, and pretending otherwise will only magnify the economic harm. **As speculative risk in the AI sector accelerates, Public Citizen is unequivocal: there must be no AI industry bailout.** Taxpayers must not be turned into the insurer of last resort for reckless corporate overreach. If AI companies truly believe their technology is revolutionary, they should be prepared to bear the full market risk of that claim. **Congress must make this principle explicit now, before instability sets in, not after another crisis forces emergency action. There should be no implicit**

¹⁰⁷ Chris Morahan et. al., *AI Funding: The Bull and Bear Investment Case*, Morgan Stanley, December 1, 2025, <https://www.morganstanley.com/im/en-us/individual-investor/insights/articles/bull-and-bear-investment-cases.html>; Caleb Mutua and Paula Seligson, *Wall Street Races to Cut its Risk from AI's Borrowing Binge*, Bloomberg, December 5, 2025, <https://finance.yahoo.com/news/wall-street-races-cut-risk-113000304.html>; Nick Lichtenberg, *OpenAI Won't Make Money by 2030 and Still Needs to Come Up with Another \$207 Billion to Power its Growth Plans*, HSBC Estimates, Fortune, November 26, 2025, <https://fortune.com/2025/11/26/is-openai-profitable-forecast-data-center-200-billion-shortfall-hsbc/>.

¹⁰⁸ See *supra* note 94.

¹⁰⁹ *Id.*

¹¹⁰ Jeffrey A. Sonnefeld and Stephen Henriques, *This is How the AI Bubble Bursts*, Yale Insights, October 8, 2025, <https://insights.som.yale.edu/insights/this-is-how-the-ai-bubble-bursts>

¹¹¹ *Id.*

¹¹² See *supra* notes 94-99.

guarantees, no quiet backstopping of private credit, and no federal assumption of stranded AI infrastructure debt. Losses should remain where they belong: with the investors and executives who chose to take the risk. The American public is not an insurance policy for speculative AI finance.

VII. The “Sandbox” Misnomer and the Broader Deregulatory Strategy

The Senate’s SANDBOX Act and Chairman Hill’s Unleashing AI Innovation in Financial Services Act are foundational misrepresentations of the term “sandbox.” Neither proposal meaningfully resembles a regulatory sandbox. **True sandboxes are narrow, temporary, and tightly supervised environments designed to generate evidence before broader deployment.**¹¹³ These bills do the opposite. They use the language of experimentation to justify sweeping, long-term exemptions from existing law, with diminished oversight and heightened risk to the public. This is not controlled testing. It is preemptive deregulation.

At their core, both bills invert the basic logic of public-interest governance. Instead of requiring companies to demonstrate safety before deployment, they assume safety and force the public to absorb the consequences if that assumption is proven wrong. Instead of strengthening regulatory capacity to meet the scale of emerging risk, they convert regulatory delays and agency under-resourcing into automatic approvals. In both cases, “innovation” becomes the rationale for stripping away the very guardrails that make innovation legitimate. This fits the pattern of Republican’s AI deregulatory efforts seen since this summer.

The Senate SANDBOX Act is being marketed as a narrow, innovation-friendly pilot.¹¹⁴ However, it represents one of the most aggressive deregulatory maneuvers in federal AI policy to date. It would authorize sweeping waivers of federal law for companies deploying AI systems, while simultaneously preempting state protections and sidelining expert regulators.¹¹⁵ Approval authority would be centralized in an office without enforcement powers, and if agencies fail to act within rigid timelines, approvals would be granted by default.¹¹⁶ Delay becomes rubber stamped government approval for corporate immunity.

This is not how genuine sandboxes function. Real sandboxes are narrowly scoped, time-limited, regulator-controlled, and designed to inform future safety standards.¹¹⁷ The SANDBOX Act meets none of those conditions. Its waivers are broad, its duration is long,

¹¹³ Lauren Saunders, *Are Fintech Sandboxes a Consumer Protection Desert?* The Hill, November 29, 2018, <https://thehill.com/blogs/congress-blog/economy-budget/418770-Are-fintech-sandboxes-a-consumer-protection-desert%3F/>

¹¹⁴ U.S. Senate, *Sen. Cruz Unveils AI Policy Framework to Strengthen American AI Leadership*, Press Release, September 10, 2025, <https://www.commerce.senate.gov/2025/9/sen-cruz-unveils-ai-policy-framework-to-strengthen-american-ai-leadership>

¹¹⁵ Senator Ted Cruz, S.B. 2750, <https://www.congress.gov/bills/119th-congress/senate-bill/2750/text>

¹¹⁶ *Id.*

¹¹⁷ See *supra* note 114.

its oversight is diluted, and its regulatory consequences are permanent. It does not test whether systems are safe. It assumes safety and tests the public instead.

The resulting public interest failures are profound. The SANDBOX Act would weaken civil rights and consumer protections, treat people as involuntary test subjects in live-market AI experiments, sideline expert regulators, normalize exemption as the regulatory baseline, and wipe out stronger state protections enacted precisely because Congress has not acted. In short, the SANDBOX Act does not modernize regulations. It obliterates them.

The House bill Unleashing AI Innovation in Financial Services Act follows the same deregulatory blueprint, but confines its experiment to the most systemically sensitive sector of the economy. Under the Act, financial institutions may propose “AI test projects” and seek waivers or modifications of existing rules through “alternative compliance strategies,” including rules governing consumer protection, market integrity, and risk management.¹¹⁸ Once approved, the primary regulator may enforce the waived regulation only through the firm’s alternative strategy, and all other financial regulators are explicitly barred from enforcing those same rules.¹¹⁹ In other words, the supervised entity helps write the terms of its own supervision and then receives statutory protection from the rest of the regulatory system.

The bill hardwires automatic approvals into law. If a regulator fails to act within 120 days, it may extend review once, but after that, inaction becomes approval by operation of law.¹²⁰ In an AI landscape defined by opacity and technical complexity, this structure weaponizes regulatory understaffing—particularly in the wake of the Trump administration’s mass layoffs—into a built-in deregulatory signoff.

Transparency is also sharply curtailed. Annual reports to Congress may present only *aggregated results* and may not name participating firms.¹²¹ Lawmakers, market participants, and the public will have no way to know which entities were permitted to experiment with high-risk AI systems under relaxed rules or how those experiments affected real consumers and investors. In a sector where trust and stability are paramount, anonymizing experimentation with core financial infrastructure is not responsible governance. It is concealment.

The financial industry’s history makes one thing unmistakable: waiting for fraud cases to ripen is regulatory malpractice. Complex AI-driven trading, underwriting, and customer-interaction systems can quietly shift risk, hardwire discrimination, and destabilize markets long before conduct ever meets the narrow legal threshold for emergency intervention. By the time fraud is provable in court, the damage is already done.

These two separate bills represent key aspects of the same deregulatory playbook. This unified deregulatory scheme has appeared repeatedly across legislative vehicles, both

¹¹⁸ Rep. French Hill, H.R. 4801 the Unleashing AI Innovation in Financial Services Act, https://financialservices.house.gov/uploadedfiles/ai_bill.pdf

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *Id.*

chambers of Congress, and policy proposals raised by President Trump. Key overlapping concepts include:

- **Strip state authority through preemption.**
- **Fast-track deployment of untested systems.**
- **Centralize power to federal agencies whose leadership has eschewed oversight powers and whose staff have been depleted to create automatic approvals of industry favored laws.**
- **Shift risk downward onto workers, consumers, and communities.**

Under these policy proposals, the public bears the downside while corporations retain the upside. When Congress allows industries to help write their own compliance rules, shields them from scrutiny, anonymizes experimentation on the public, and blocks state governments from responding to local harms, democratic oversight itself becomes collateral damage. **Sandboxes are supposed to be places to experiment while minimizing harm to the public at large.¹²² Both the SANDBOX and the Unleashing AI Innovation in Financial Services Act break the very guardrails that make innovation worthy of public trust. They are not experimentation but rather blanket corporate immunity.**

VIII. Guiding Principles for Democratic AI Governance

The choice before Congress is not between innovation and regulation. **It is between unchecked, high-risk deployment that serves a narrow set of corporate interests and responsible, rights-respecting innovation that strengthens the middle class, protects democracy, and preserves financial stability.** The United States can and should lead on AI. But that leadership must be defined by enforceable guardrails that allow the economy to flourish for everyone.

¹²² Venkatarangan Thirumalai, *Understanding the Power of AI Sandboxes: A Guide for Beginners*, Founder Catalyst, April 29, 2024, <https://thefoundercatalyst.com/2024/04/29/power-of-ai-sandboxes/>

A genuinely pro-American AI policy should be grounded in a small set of clear principles:

1. **Human and civil rights are non-negotiable.** AI systems must not be used to discriminate, suppress rights, or evade longstanding civil rights protections. If they do, enforcement mechanisms must be pursued to hold companies accountable.
2. **Accountability follows power.** The more powerful and impactful an AI system is, the stronger and more enforceable its oversight must be. Otherwise, the American public will be vulnerable to one of the most powerful technologies to date and beholden to the interests of a few tech monopolists. Further, corporations cannot be allowed to hide behind machine decisions. If an AI product produces discriminatory, dangerous, or simply injurious results, then the corporations behind that product must bear responsibility.
3. **States remain essential partners.** Federal law should establish a floor of protection, not a ceiling. States must remain free to respond to evolving harms and innovate in the public interest. This represents the will of the American people as shown by consistent polling.
4. **Workers and communities are not collateral damage.** AI policy must prioritize job quality, workplace dignity, and community stability. The American economy was built upon a strong middle class, and Congressional policies must seek to encourage middle class growth.
5. **Financial stability and economic realism matter.** AI cannot be regulated as if its upside is guaranteed, and its downside is someone else's problem. Speculation is not a regulatory strategy, and taxpayers must never be forced to underwrite the consequences of reckless AI finance.
6. **Transparency is the price of public power.** Systems that make or influence decisions about people's rights, livelihoods, or safety must be explainable, contestable, and auditable. This is the bedrock of democratic governance.

These principles are concrete governing standards that must shape legislative text, oversight mandates, and agency rulemaking. They also reflect the core values that have historically allowed the United States to prosper: accountability, fairness, shared prosperity, and democratic control over concentrated power.

Conclusion

Each month that passes without meaningful federal guardrails is another month in which AI systems deepen their footprint in finance, employment, policing, infrastructure, and politics—often under weaker oversight than the industries they are displacing. AI is shaping our society in real time. **The question before Congress is who this technology will serve and who will bear its risks.**

In past eras—whether with tobacco, opioids, financial derivatives, or social media—Congress was told repeatedly to move fast, trust industry, and regulate later. Each time, the public paid the price in lives, livelihoods, and lost trust. AI is moving faster, operating at a greater scale, and concentrating more power than any of those industries ever did. The cost of getting this wrong will be higher.

The United States does not have to choose between leading in AI and leading with values. The only way to do both is through enforceable public-interest guardrails. Congress now has a once-in-a-generation opportunity to decide whether AI becomes another chapter in the story of unchecked corporate power or a model for how democratic societies govern world-changing technologies responsibly.

Public Citizen respectfully submits that the better path forward is not a mystery:

- Reject blanket preemption and deregulatory sandboxes.
- Build enforceable, sector-specific guardrails.
- Invest in regulators' technical capacity.
- Protect workers, children, and communities.
- And refuse to make taxpayers the backstop for speculative AI finance.

This is pro-democracy, pro-worker, pro-consumer, and pro-market stability. It is what serious AI governance looks like. America's leadership in AI will ultimately be measured by whether working families are more secure, markets are more stable, civil rights are protected, and democracy emerges stronger on the other side of this transformation.

That is the standard the public expects. And it is the standard Congress must now meet.

Chairman HILL. I thank our panel very much.

I now recognize our members for questioning, and I recognize myself for 5 minutes.

The Trump Administration's AI Action Plan prioritized the acceleration of AI adoption in government and outlined several policy actions that agencies can take to further U.S. government's use of AI to, as it says in his plan, "deliver the highly responsive government American people expect and deserve." I am pleased to see this mentality at the highest levels of government.

Ms. Manfra, how does the AI Action Plan align with industry best practices and the recent advancements in AI, and what can the government learn from market participants to close the AI adoption gap, and promote responsible use by our government agencies? Emphasis on "responsible."

Ms. MANFRA. Thank you for the question, sir.

The administration's approach to ensuring that AI and other technologies are used to better deliver services to the American people is very welcome and combined with that, the approach to ensuring that responsible use with safeguards, and the experience that agencies are having in implementing their own AI governance has also been welcome. So being thoughtful about how these AI tools are being used in different risk scenarios is something that we see every day with our customers and partners in the government and we welcome that.

We also appreciate the approach of experimentation, and being able to create spaces where an agency or an organization can explore a use case for AI and work out responsibly what those issues might be before—

Chairman HILL. I think that is a—I think that is an important point because over the years, we have had bipartisan support for regulatory sandboxes for a variety of things, block chain and other aspects of it. That is something that technology providers and banks have tried to work out. It is important in financial technology (fintech) partnerships. It is not deregulatory per se if one has a sandbox, and in an offline capacity tries to perfect the use, in this case, of AI and then the responsible compliance procedures for it. Is that not a fair way to describe it?

Ms. MANFRA. Yes, sir.

Chairman HILL. You do not consider that, per se, deregulation, do you?

Ms. MANFRA. I do not, sir. I think it allows organizations to have a safe space where they can experiment and work out any potential issues before they would then—

Chairman HILL. Yes—

Ms. MANFRA [continuing]. employ it.

Chairman HILL. I kind of share that—I share that view as a general statement, subject to the details, obviously.

While machine learning is not new, Generative AI and agentic AI have recently been paradigm shifts for this technology, particularly in the private sector. Such tools may hold enormous potential for our financial institutions and our financial regulators to change how they work.

Mr. Cohen, let me turn to you. At Nasdaq, you moved trading markets to the cloud. You were one of the first exchanges to release

an AI-powered order type. Can you describe the efficiency gains that you achieved through this transition and what lessons you think that taught Nasdaq as you look at other AI adaptations?

Mr. COHEN. Thank you for the question.

In terms of the order type you are referring to, it was—it is called Dynamic Midpoint Extended Life Order (M-ELO). It is the first SEC AI-enabled order type, and the SEC had to get comfortable with exactly how we designed it, the explainability of it, how we are testing it, and then how we are deploying it into the market.

We designed it for large institutions—the Fidelity's, the Wellingtons of the world—so that they can execute inner markets with confidence and get the execution quality they need as they are serving, we tell investors, everyday investors sit behind the money that they put to work every day at our markets.

So we wanted to democratize good execution quality, and we did it through this order type, through, initially, a static delay mechanism that allowed them to void fast money in the market, which meant that at the end of the day, they could look at their executions and the price movement after they executed and see that there was quality in those executions.

What we did with AI is we incorporated 140 data points every 30 seconds to determine what that delay should be to optimize the execution quality that those large institutions get.

Chairman HILL. Appreciate that. My time is short, so Ms. Whitmore, if I could ask you to respond in writing—of course, good people and bad people can use AI, so countering threats, I think, is very important, and I think cyber risks are a big challenge for the private sector and the government sector. Can you follow up in writing with me and talk about how we should counter those cyber risks to counter bad actors in this space using AI? Thank you.

Ms. WHITMORE. Yes, sir.

Chairman HILL. Thank you very much. If you do that in writing, please.

I recognize the gentleman from Georgia, the distinguished Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you very much, Chairman.

You know, concerning this AI business, I am very fearful that we are rapidly becoming servants of the machine that we created to serve us. I want that thought to register with you and that is why I am working on a bill to expand wage insurance protections, guaranteeing temporary wage replacement for workers who are forced into lower paying jobs by AI. This is dramatically important.

Mr. Branch, let me ask you. You said something very important in your statement. You said in your statement, and I quote, Workforce policy built on aspiration and retraining slogans is not a real A-1 workforce policy.

So let me ask you a couple of questions. Have you talked with our labor unions about this? What are they saying, if you have or have not?

Mr. BRANCH. Thank you for the question, Representative.

Yes, we have spoken with union representatives, and they are concerned about the potential for replacement and lost jobs. The problem with some of these reskilling programs is that oftentimes

the jobs are not available in the communities where the jobs are lost. So you lose a job in rural America, but the job is actually based in Silicon Valley that you are being retrained for. A lot of times, the reskilling jobs do not even come at the rate of the jobs that end up being lost. So you end up having a variety of folks who lose jobs but then cannot be employed afterwards.

Mr. SCOTT. Spell out for us, how can unregulated A-1 jobs lead to widespread job displacement?

Mr. BRANCH. Well, thank you again. Currently, a variety of tech companies are really moving forward with trying to replace a variety of their employers—employees. We are seeing this in the tech force right now where you have whole slews of coders who are losing their jobs. So that is why it is important for Congress to address this issue head-on to work with unions to ensure that when these jobs are lost, that there are actually going to be jobs available for these folks.

Mr. SCOTT. That is why I keep saying we are rapidly becoming servants of this machine we created to serve us and I hope, Chairman Hill, that this very timely hearing will wake our Nation up to realize. I am working on a bill, as I mentioned, to expand wage insurance protection, guaranteeing that our workers are taken care of here.

Let me ask you one more question, Mr. Branch. The unemployment rate for recent college graduates has risen recently. Why is it important to modernize workforce protections to reflect today's AI driven economy?

Mr. BRANCH. Thank you again for the question—

Mr. SCOTT. Because the AI is driving it, man.

Mr. BRANCH. Thank you again for the question.

Again, to sort of boost efficiencies that some of these companies are talking about, they are really targeting lower-level employees and lower-level jobs and so you are seeing waves of college graduates who do not have those lower-level jobs available for them. They are oftentimes requiring additional job experience that they might not have because they have not had the opportunity because efficiencies have made those jobs essentially redundant.

So it is important to ensure that there are opportunities for these young kids to get into because if you are removing those jobs, you are essentially removing the ladders to success that the middle class was built on.

Mr. SCOTT. In my last 7 seconds we got to guarantee that our workforce is protected with this advance of AI. Mr. Chairman, thank you.

Chairman HILL. I thank the gentleman from Georgia.

I recognize the vice chairman of our full committee, the gentleman from Michigan, Mr. Huizenga. You are recognized for 5 minutes.

Mr. HUIZENGA. Thank you, Mr. Chairman.

It is interesting, the conversation that we are having here. Some seem to be suggesting we should not innovate because of potential job loss. I cannot imagine where America would be today if that was our guiding principle. We also seem to be having some folks who lump in AI generally into one big category. It seems to me an AI system dispensing "life advice" about whether I should take this

job or, more tragically, and is a huge problem, where we have seen systems tell kids to go do things to themselves that they should not—it should not even come across their screen but that is very different than an application to seek facts. What was the gross domestic product (GDP) of the United States in 1904 is a fact and because of AI and because of some of these systems, we are able to—we are able to sort through those things but both of those are very different than an application to introduce efficiency into a simple process, or even a complex process. We have got two great examples here with Nasdaq and Zillow, and others.

I am going to start there. Someone suggested that there are not the same protections against discrimination with the application of AI to various transactions. Mr. Cohen and Mr. Stevens, I would like you both to quickly address this. What have you done to ensure that does not happen in your respective industries? Housing and investing are two of those areas that we talk about often here in the committee. Is there any evidence that what your efforts have done is not working, and is not mitigating that concern, and have you had to make any adjustments? Mr. Cohen.

Mr. COHEN. Thank you for the question. So we do not serve retail directly. We serve institutions. We serve financial markets—

Mr. HUIZENGA. Sure.

Mr. COHEN. The way that we think about it and the way that we employ it into our solutions, whether it is our anti-financial crime solution, our surveillance solution, or regulatory solutions, it goes through the same PBLC process that we have for anything that we would deploy. What is really important about that is the rigorous testing that we do, the understanding of explainability and transparency—can we reproduce it and do we understand what the models are providing? There is always a human in loop. Really important you keep that human in the loop.

Mr. HUIZENGA. Obviously, you are not quite as forward facing as a real estate transaction?

Mr. STEVENS. Yes. Similar answer. I will talk about fair housing and then back to the first part of your question, how important advice from a human really is in housing. For fair housing, we built the classifiers—

Mr. HUIZENGA. By the way, as a former realtor, I fully subscribe to that.

Mr. STEVENS. Yes. Our research shows—it might be counterintuitive for a leader of AI to say it, but our research shows that humans making a buy, sell, rent decision want to sit across a kitchen table and get real human advice from someone who lives in their market. So, our AI is built to really target the processes that are keeping real estate agents, like your former self, away from those important conversations. Then along the way, we built classifiers like the Fair Housing Classifier, AI should be held to the same standards as any human. We want to make sure the facts that are presented to people as they prepare are meeting those same fair housing standards.

Mr. HUIZENGA. Real quickly, in my last minute and a half here. Mr. Cohen, how is Nasdaq leveraging artificial intelligence to create markets that are not only more efficient, but more transparent

and fair? You touched on that a little bit. Do you care to elaborate or—or—how you have to deal with that—through that?

Mr. COHEN. A really great example of that I did not talk about in my opening remarks—we have a market intelligence desk where our listing clients, our corporate clients will contact us and ask us about sentiment, will ask us about, what is the intelligence and what are you seeing in the markets? What we are doing is using AI to essentially group different parts of data or different pieces of data, which is what we see in social media, what we see in the news, and what we see in the markets, and the confluence and the aggregation of that allows us to use AI, develop patterns, develop insights and intelligence. We can provide business leaders so they can make real-time decisions. Now, again, there is a human in the loop.

Mr. HUIZENGA. Yes.

Mr. COHEN [continuing]. We ensure that, to the extent that there is news out there that is not real or fake, we are taking that out before we provide—

Mr. HUIZENGA. So you are stitching that altogether.

Ms. Whitmore, I am sorry. You seem to be—you are going to be answering a lot of our questions in writing, but I want to touch on the anti-money laundering (AML), Know Your Customer (KYC), and how AI has the potential to enhance compliance efforts. So 10 seconds.

Ms. WHITMORE. Okay. We will follow up in writing on that. Thank you.

Mr. HUIZENGA. With that, I get to yield back with 2 seconds. So sorry about that.

Chairman HILL. I thank the vice chairman.

I call on the gentleman from Massachusetts, Mr. Lynch, who is the ranking member of our Digital Assets, Fintech, and AI subcommittee.

Mr. LYNCH. Thank you, my friend.

I have got a couple of things here. So we are talking about a quasi-sandbox process here to try to test some of these AI applications and financial services. As a member of this committee in the past, we have done oversight on the whole sandbox process. One of our more instructive experiences was in Singapore where we went in there and they had a financial services tech—a fintech sandbox where they invited companies to come in and participate.

The difference here is that when they did that in Singapore, they had their regulations in place already and here we are—we are doing it backward. We are inviting—we are inviting financial services companies as they deploy AI to choose which—which consumer investor protections, which soundness—safety and soundness regulations that they might want to avoid.

Mr. Branch, is that a proper way to introduce a new technology? Where you are asking the private sector to identify regulations that are in place to protect consumers, investors, depositors—because this applies to banks as well—and you are asking them what would you like to do to avoid a compliance with some of the current existing financial services regulations?

Mr. BRANCH. Thank you for the question, Representative.

No, I do not think that is a responsible way of moving about this. The sandboxes that are being proposed often are completely deregulatory. That is entirely different from the Singapore model, which was actually hailed in this committee just a few months ago. They had regulators in place. It was time limited. Consumers were warned if they are a part of that sandbox. None of that is present here.

Mr. LYNCH. Right. So the idea of the sandboxes, you have a contained area. Matter of fact, Mr. Chairman, I would like to ask unanimous consent to introduce the Fintech Regulatory Sandbox Guidelines, dated November 2016. This was in advance of the Singapore sandbox.

Chairman HILL. Without objection.

[Information referred to can be found in the appendix on page 126.]

Mr. LYNCH. So a few of the things that they point out here that are essential to—essential to a successful sandbox, and that is to manage risks, to contain the possibility that individuals might be injured, or financially damages. The consequences of failure for that technology need to be contained and people need to have advanced knowledge of the risks that they are embracing by participating in adopting that technology. It cannot—it says here it cannot be used as a means to circumvent legal and regulatory requirements, which is exactly what this bill is suggesting, that—that in adopting AI, they are allowing, or encouraging, ways of circumventing existing regulation in what are supposed to be a technology-neutral approach.

There are also cautions here where applicants have not demonstrated that they have done due diligence, including testing the proposed financial services technologies in a laboratory environment beforehand and knowing the legal and regulatory requirements for deploying the proposed financial service technology.

So what—so, Mr. Branch, what is wrong with that whole approach in terms of protecting consumers, investors, depositors, and others who rely on the benefits of this financial services industry?

Mr. BRANCH. Well, I think the main thing that is wrong with that approach is that there is everything to gain for large corporations, and the harm is just going to be entirely brought on by the American consumer. If anything, if things go wrong, the government is going to be expected to either bail out or help out the corporations that have put the consumers in harm's way.

Mr. LYNCH. Thank you very much. Mr. Chairman, I believe my time has expired. I yield back.

Chairman HILL. The gentleman yields back.

I am pleased to recognize the gentleman from Oklahoma, Mr. Lucas, who chairs our task force on Monetary Policy and Treasury Market Structure.

Mr. LUCAS. Thank you, Mr. Chairman and thank you to our witnesses for being here today.

Our whole economy benefits when United States companies lead the world in innovative financial services. I think we all agree on that, and our regulations should allow for that responsible growth and expansion when it comes to AI, too.

Mr. Cohen, would you expand a little bit, what are the best-use cases, as you see them, for AI to be further deployed in capital markets?

Mr. COHEN. Thank you for the question.

We, at Nasdaq, deploy AI in two ways: in our products and then on the business and the way that we think about in the products. We are trying to generate greater productivity, better outcomes for our clients, and lead to better client experience with the types of solutions we provide and I mentioned this before. We see the possibility of improving how—how jurisdictions put out regulation, the complexity associated with regulations, and then what clients need to do to comply with those ever-changing regulations. AI can go from reg to code and really allow them to ensure with confidence they are complying with regulation. So that is a great use case for us.

In fighting financial crime—I mentioned it earlier. We must use AI in the data that we have at our disposal to make sure that we are staying ahead of the bad guys. In terms of what I talked about with human trafficking, financing terrorism, we need to make sure that our solutions are protecting the reputation, the brand, and the consumer behind those institutions. So that is really, really important.

Then in our markets, we are using AI—and this is our north star—to make sure that we are democratizing the types of—the types of capabilities that otherwise small broker dealers do not have the R&D and engineering talent to develop on their own and they would be left behind if not for Nasdaq and others developing it on their behalf.

Mr. LUCAS. On that same thought, throughout the committee's work on combating fraud and scams in financial services system, we have discussed the sophistication and technological assets that bad actors use against consumers. So giving you prime time, opportunity to answer, Ms. Whitmore, how is AI being used right now to detect and stop fraud and scams, and how will those services improve and expand in the future?

Ms. WHITMORE. Well, I am thankful for the question.

So what we are seeing in terms of the threat landscape relative to AI—two areas.

The first is attackers using AI to fuel traditional cybercrime. We are largely seeing that impacts the speed and the scale with which they operate.

The second part that is not being talked about as much is how attackers are targeting AI, so creating the ability to make agents inside of our environments into rogue insiders that cannot be trusted.

What we see with that is the need for security to be closely coupled with AI innovation, the need to make sure that we are protecting the build, the run, and the access—so, particular to the run time, making sure that agents do not have the capability to go rogue and that those protections are in place so that organizations can successfully innovate without that being hijacked by attackers.

Mr. LUCAS. Ms. Manfra, can you discuss how smaller financial institutions like community banks can utilize this technology? Why

is it important for financial institutions of all sizes to have access to the latest technology, please?

Ms. MANFRA. Absolutely. Thank you for the question.

One of the great benefits of what we are seeing in AI is the democratization of access to data that, historically, only large, well-funded institutions might have and the additional productivity gains that smaller institutions that are more resource-constrained now have access to larger data sets in more real-time and are able to put in place improved customer service experiences, improved productivity, are better able to detect fraud and reduce the amount of false positives so that their employees do not have to spend time chasing down potential dead ends.

So we see a lot of opportunities in the small and medium-size financial institution space.

Mr. LUCAS. Mr. Cohen, I will ask you to respond in writing. Are existing regulations appropriate to encourage innovation while maintaining appropriate consumer and financial stability protections and what are the regulations/statutes, if any, that would use modernization? You can respond in writing.

Mr. LUCAS. I yield back, Mr. Chairman.

Chairman HILL. I thank the gentleman.

The chair recognizes the gentleman from California, Mr. Vargas, who is the ranking member on our Task Force on Monetary Policy. You are recognized for 5 minutes.

Mr. VARGAS. Well, thank you very much, Mr. Chairman. I appreciate it, you and the ranking member putting this together. I think it is a very important hearing.

I do not believe that you can unring a bell or put the genie back in the bottle or do anything like that. So the reality is that science moves forward and our knowledge moves forward; you cannot reverse it. So I think AI is here. It is now, how do you manage it?

A few years back, I had the opportunity to go with some of my colleagues here to the World Economic Forum, and somehow I got assigned to go to dinner with the young tech entrepreneurs to listen to Sam Altman. I thought I was not going to understand a thing because I am not young and I am not a techie. So I thought, this is going to be interesting, but I am not going to understand anything.

It turned out I understood everything, because they really did not talk about technology; they really talked more about philosophy. It really was more the philosophy of the machine, you heard earlier, versus human being, the data that you put in and what comes out and whether that data is positive or negative.

You could see some of the results—I have seen them in the following years—where, yes, AI, you will ask it a question and it will come back with what we would think is a pretty absurd answer or horrific answer for some young people, but you could see why the data that you put in, it would ultimately reach that conclusion. Because not all data is positive; you also have data that is in there that is negative.

So I appreciate, then, also, we have heard today really the competition between the good and the bad in AI, because, I mean, the bad guys use AI also, for fraud and other things.

With all that being said, Mr. Cohen, you have a very transparent company. In fact, when we talk to your staff, they get back to us right away. So I will ask you, who is winning here? I mean, are the bad guys winning in the attacks or not?

Mr. COHEN. Yes and thank you for the question.

What is interesting about this technology is, the rate of advancement of this technology is faster than the rate of adoption and you do not often see that with technology.

The second thing is, we need to, as an organization, all of us, within our four walls, talk out loud about the negative scenarios that might occur with AI so that we prevent them. If we do not talk out loud and we do not have conversations internally about that, then we are missing an opportunity.

To your more specific question, we are seeing in our markets bad guys, if you will, using AI to come up with more sophisticated market manipulation schemes. If we are not using the data and the technology to stay one step ahead, then we risk the integrity and the investor confidence around our markets.

For banks, fraud is a massive, massive problem and fraud is becoming more sophisticated. It is more difficult to detect, and you cannot do it on your own; you need a public-private partnership, and you need a massive amount of data to really stay ahead of it.

So, unless we arm our community to be able to do that, then we are going to be a step behind, banks are going to be subject to fraud, markets will be subject to market manipulation.

Mr. VARGAS. So I understand that part. You have to—they are going to use it, so you have to prepare. I mean, it is one of these things that has to happen.

You also said something that is very interesting because it is also a philosophical point. And I do have a master's in philosophy. That is why I am so confused normally but it was more based on religion. I studied to be a priest for a long time. The notion of keeping the person in this process becomes harder and harder as it advances, because the decisions it makes—it takes all this data, and it uses it so quickly.

How do you figure to keep the person, a human being, in this process—as you would call it, in the loop—when AI can make decisions so quickly?

Mr. COHEN. It is an excellent question and the human in the loop is really, really important. Building those critical-thinking skills and those judgment skills are exactly what we are training our people to do.

So, one, we are putting the tool in our hands. Two is we are providing them with training and education and three is we are putting good governance around them and providing them with policies that they can follow and understand. So the humans are armed with enough so they can make the right decisions at the right time and understand their roles and their roles are not decreasing or becoming marginalized. It is actually more important than ever to have that human in loop and provide that judgment, as you noted, because AI is designed to provide you with an answer. It is our responsibility to determine if that answer is correct and if that is the answer that we want to provide our investors and, if you will, institutions that we serve around the globe.

Mr. VARGAS. Well, I apologize, I asked you all the questions. I apologize to the others I was not able to, but I have 10 seconds left. With that, I will just thank all of you and I will thank the chair. Appreciate it very much.

Thank you, Chair.

Mr. BARR [presiding]. The gentleman yields back.

The gentlewoman from Missouri, Mrs. Wagner, is now recognized for 5 minutes.

Mrs. WAGNER. I thank the chair.

I say welcome to our witnesses.

Mr. Cohen, in your testimony, you highlighted how Nasdaq has been at the forefront of technological innovation in our capital markets since the exchange was founded in 1971.

Nasdaq was an important player in the creation of electronic trading. While rapid growth over the last few years in generative artificial intelligence, or AI, has brought this technology center-stage for the general public, Nasdaq has been quietly using AI for years and years to fight fraud and increase market efficiency, liquidity, and transparency.

Mr. Cohen, can you describe some of the ways that Nasdaq currently uses AI and the extent to which generative AI either has or might have a role to play in our capital markets and how do you manage the risks associated with this technology, sir?

Mr. COHEN. Thank you for the question.

It is in our ethos, if you will, to adopt and integrate emerging and advanced technology early. We see it as a competitive advantage and one that we have embraced since our founding in 1971.

With respect to the use of AI, what is important for this committee to understand is, you cannot harness the power of AI unless you make the foundational investments to do that. We have done that over the past decade, whether it is embracing the cloud, putting good governance in place, having a mature posture over information security, training and upskilling our employees, and making sure we have good governance; good governance is the lubricant for innovation. That is the way we see it.

Then you have to be really clear to make sure that it is centralized so you do not have the AI sprawl happening within your organization and shadow AI, where you cannot control it, you do not know about it.

So all of those things have been what we have been focused on over the past decade, which has now enabled us to put them in our products. As you mentioned, we use it for market abuse. We use it to fight crime. We use it to democratize access. We use it to provide more transparency, more information to end investors so they understand the risks that they are taking when they invest in our markets.

We are always trying to stay one step ahead of the bad guys, one, and two, one step ahead of ensuring that our markets continue to be the best in the world. We have the pride in making sure that the U.S. markets are the most robust, most vibrant, if you will, highest moral ground in terms of the way that we operate and we protect the U.S. markets every day in the way that we use that—

Mrs. WAGNER. You are absolutely right; we have the most extraordinary markets in the entire world, and we are going to put

a fine point on that this week with the Incentivizing New Ventures and Economic Strength Through Capital Formation (INVEST) Act that will be moving forward. So we are very excited about that.

You are right; other companies and industries need to look at that AI sprawl, shadow AI, some of the things that—I do not know that they are entirely discerning, but those are key.

Mr. Cohen, do existing technological-neutral regulations provide sufficient guardrails for the responsible use of AI in our capital markets, or are new AI-specific updates and clarifications required? If updates are in order, what should they look like, and how can they be implemented without stifling innovation?

Mr. COHEN. That is a great question. It is one that we actually think about quite a bit, especially as the technology is evolving.

What I would say is, we have a great foundation. We have securities laws. We have NIST that we follow. We have Reg Systems Compliance and Integrity (SCI) and we have worked hard as an industry to put more rules in place around technology. So the foundation is there.

I think the key to that question is, because the technology is advancing at such a rapid pace, information-sharing or private-public partnership, where we can share information about the advancements of this technology to identify gaps, was—we do not know what those gaps might be today, because the advancement of that technology is such that it is not linear. It is exponential and we tend to plan very linearly as humans.

So we are just going to have to make sure we stay in touch, we share information, we use the foundation that we have that I mentioned, with NIST and Reg SCI and the securities law, to ensure, when a gap comes up or when there is a risk that we have identified, we work together to address that quickly.

Mrs. WAGNER. Well, I may not—you may have to respond in writing here, but I am interested in knowing if there are any existing rules or ambiguities or proposals that are limiting AI innovation from reaching its full potential in U.S. capital markets—obviously, a focus of mine.

So I will look for your answer in writing.

Mrs. WAGNER. I thank you for your testimony.

I yield back to the chair.

Mr. BARR. The gentlelady yields back.

The gentleman from New York, Mr. Meeks, is now recognized.

Mr. MEEKS. Thank you, Mr. Chairman.

Let me go directly to Ms. Whitmore.

Ms. Whitmore, the nexus of AI and cybersecurity is particularly important and can be particularly concerning as well. Last year, the Salt Typhoon hack against the United States companies and high-profile leaders was called the largest cyber breach in United States history.

Can you just give me a very brief summary of what happened?

Ms. WHITMORE. Yes. Thank you for your question.

So you are referring to an attack by a nation-State actor, in this case China, that targeted our telecommunications and critical-infrastructure industries across the board, with the intent to steal data to then use it to meet political objectives at some point.

Unique to critical infrastructure, the component there is the fact that the Chinese nation-State may be intentionally looking to embed themselves within critical infrastructure, with the intent to take some sort of action at a later date.

Mr. MEEKS. Thank you.

Mr. Chairman, I want to, for the record, enter this article entitled “U.S. Halted Plans to Sanction Chinese Spy Agency to Maintain Trade Truce.”

Mr. BARR. Without objection.

[The information referred to can be found in the appendix on page 146.]

Mr. MEEKS. Then, a few days after the report, more news came out of Department of Commerce, which I cannot believe that they intend to allow Nvidia to sell one of the most advanced AI chips to China that had been previously banned for export.

In fact, the Justice Department was just about to go after someone who was trying to sneak them into China. Yet—this is unbelievable to me—the President started a trade war that we are losing, and he is now afraid to punish the People’s Republic of China (PRC) and its entities that hacked our most innovative companies to access the private communications of the American people.

Further, by allowing advanced Graphics Processing Units (GPUs) to go to the PRC, he is throwing away our biggest and most important advantage in the AI race with China.

That is innovation? This is not innovation. This is not winning. This is, indeed, weakness. Unfortunately, it is going to cost our country.

Let me go to another matter. In America today, rising housing prices and stagnant wages have put home ownership out of reach for millions of Americans. Median home prices remain near historic highs, and too many working families are nowhere near achieving their American Dream of owning a home.

A major part of the problem is that we simply are not building enough homes. Whether it is because of zoning barriers, permitting delays, outdated systems, and rising construction costs because of—you got it—Trump’s tariffs on materials like lumber and others, you have what is becoming a perfect storm.

So, Mr. Stevens, in your testimony, you mentioned that AI can help address some of these challenges. You said it could help with clearing permitting and zoning backlogs, reduce loan origination and compliance costs, and speed up the development process. That would be good news.

My question to you, sir, is: Aside from boosting efficiency, how can AI be leveraged to enhance housing affordability and increase the supply of homes? The President says this is a hoax, affordability, but let us go. How can that happen?

Mr. STEVENS. Yes. Thank you, Congressman, for the question.

I very much agree, we are facing a housing affordability crisis, and there is no silver bullet. I think you mentioned one of the biggest drivers is that we are 4 million homes short in terms of supply.

We are very excited about the efficiency gains that you mentioned—zoning laws, really understanding how we can make more efficient the mortgage and real estate processes.

I would say, beyond that, bringing more information to consumers. Four million families will buy a home this calendar year, 2 million for the first time, and understanding what is available to them, what they can afford, what they should explore, helps actually reduce some of the affordability problems we are facing today.

Mr. MEEKS. There should be some public-private partnering so that we can ensure that AI is being used safely and effectively? Is that not correct? Do you—

Mr. STEVENS. Yes.

Mr. MEEKS [continuing]. agree with that?

Mr. STEVENS. Exactly.

Mr. MEEKS. Thank you.

I yield back.

Mr. BARR. The gentleman's time has expired.

I now recognize myself for 5 minutes of questioning.

In President Trump's July AI data action plan, he notes that we must develop a grid to match the pace of AI innovation. Unfortunately, our grid is currently unable to keep pace with our energy demands.

The Department of Energy projects that blackouts could increase a hundredfold by 2030, with one study saying that the Mid-Atlantic and Great Plains regions could face 400 hours of power outages annually.

The growing demand for power, with AI, is increasingly a major strategic challenge for the United States.

Ms. Manfra or Ms. Whitmore, what is the threat to U.S. national security and global leadership in the AI space if we cannot meet the supply of energy needed to power AI data centers in the United States?

Ms. MANFRA. Thank you, sir, for the question and raising this important topic and I am happy to go and continue with you and your staff in more discussion on this.

Yes, overall, we need to ensure that we are able to keep pace with the demand for energy in order to support American competitiveness in this space. We also need to ensure that we are doing that responsibly and in partnerships with those companies that are involved in the distribution and provision of electricity.

Mr. BARR. Well, what considerations go into a firm's power strategy, your firm's strategy, when it comes to training and developing frontier AI models?

Ms. MANFRA. We are heavily invested in optimizing our infrastructure, so our technical infrastructure, and the way that we run and power the machines that power AI for energy efficiency. So we spend a lot of time, and that is a key principle of ours, is to optimize for energy efficiency.

I hope that answers your question.

Mr. BARR. Well, let me ask the question a different way.

Our self-inflicted energy crisis is a direct result of bad policy—Green New Deal, Paris climate accord, Network for Greening the Financial System, the SEC's climate disclosure rule, the regulators' "Principles for Climate-Related Financial Risk Management," chokepoint, the push for the greening of the financial system.

Mr. Cohen, can you talk about the importance of traditional financing of the most reliable and affordable, dispatchable sources of

power—that is, fossil energy and nuclear? Why is that important for us to win the global race for AI leadership?

Mr. COHEN. I think, at the end of the day, it is important to note that Nasdaq does not operate its own data centers and so, when we think about power—and we operate our markets, for instance, out of New Jersey, a data center we have been in for a very, very long time—we are working hand-in-hand with our data-center providers on the power strategy.

As you just heard, we, as a public company, a for-profit company we want to be as cost-effective as we can, making use of all sources of power, and ensuring that we have the portability—

Mr. BARR. Well—

Mr. COHEN [continuing]. and mobility to move should we—

Mr. BARR. I am going to reclaim my time and make an editorial comment.

China has 33 nuclear power plants under construction, with an additional 200 in planning. Coal has been the largest source of global electricity for 125 years, and it will be for decades more in the future. It is by far the largest source of electricity in China. They built 100 coal plants last year.

Now, we need diversified energy sources. I am not advocating for exclusively fossil energy or exclusively nuclear, but we have to get with the program. If we are going to win the race for AI, we have to look at what our competitor is doing, and we cannot put our heads in the sand and continue to regulate our energy sources into oblivion, if we want to win the AI race.

Final question: We all acknowledge the risks of AI that Mr. Branch talked about—AI-generated fraud, deepfake abuse, consumer deception, et cetera but he criticizes this proposed AI preemption language as an effort, quote, to undermine State AI protections. There are more than 160 State-level laws and AI, by its very nature, is interstate commerce.

Mr. Cohen, can you talk about the importance of Federal preemption to avoid a patchwork of conflicting and inconsistent AI regulations that would stifle innovation?

Mr. COHEN. We think Federal preemption is extremely important, and we think it needs to be principles-based as well. We do not think we need a new central regulator while we consider that. I think the reasons for that are: If you cause confusion, if you raise the cost of doing business, it will simply just go overseas.

Mr. BARR. Well, I agree, we do not need a new central regulator, but we do need Federal preemption so that AI innovation can fight crime, detect and stop fraud, democratize finance, promote financial inclusion, and protect our markets.

I yield back.

Now we recognize the gentleman from Illinois, Dr. Foster, for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chair, and thank you, witnesses, for your really excellent testimony.

You know, Congress is currently stuck in this issue with federalism and Federal preemption. You know, we are struggling between the nightmare of having 50 independent standards for AI regulation and the fact that we have a do-nothing Congress that is so paralyzed by the thing that—even straightforward things that

we ought to be able to agree on, nothing is happening. We are seeing consumers suffer greatly already, and it is not going to get easier.

There is a middle ground on this, which is something that we are going to be circulating draft legislation on and I would like to comment on, which is simply a proposal to let coalitions of States form their own standard, so that any coalition would have to have, for example, 20 or 25 percent of the population, and so there would be significant coalitions, and companies would only face at most two or three sets of AI standards.

This sort of cooperative federalism, if you will, I think, is the thing that we may be able to agree on in this and so I just—I am tossing that out. There will be more detailed legislation, but it is a pretty simple concept.

Most of you who work internationally already deal with a dozen different countries and their regulations, so if the U.S. had two or three standard markets for things like—you know, for everything AI—privacy, all this sort of stuff—I think it would actually work well and we would preserve the laboratory of democracy of the States on this.

Also the big thing that is coming at us is agentic AI. This is—you know, it is the future, not only of financial services but everything consumer-facing and Business-to-Business (B2B) transactions.

In the near future, most businesses are going to be facing not their customers but their customers' agent, and that is going to change everything. Customers' AI agent will not care if you have a pretty website or an easy-to-use customer interface or a friendly smile, you know? Most consumer agents are just going to be given instructions to get the best price. Customer loyalty will go to zero and this could destabilize our banking system—for example, with AI-driven bank runs. Agents are going to squeeze the margins out of all consumer-facing businesses, and that will be extremely disruptive. You know, for example, to pick an unsympathetic example, used-car dealers will no longer have an infinite supply of clueless customers to take advantage of.

However, it may also really simplify consumer protection law, because so much of consumer protection law is to protect unsophisticated customers. If there are no unsophisticated customers because you are dealing with their AI, it will change everything.

All right. So what can Congress realistically do about this?

First off, preventing identity fraud by enhancing the deployment of digital driver's licenses and mobile ID. This is being done by most of the States right now. The EU, the U.K., Asia, everyone has—almost every country has the ability to get out your cell phone, to deploy a federally issued real ID, a driver's license or a passport or equivalent, and prove they are who they say they are in an online transaction. We have to do everything we can to get this adopted.

What we need here are not—you know, one of the legislation is to study best practices for sandboxes that we are not yet going to build. What we actually need is a pilot program for KYC customers using a REAL ID digital driver's license, which would just simplify all kinds of things and prevent a lot of the identity fraud.

Second, I think, if we were able to define United States standards for agent-to-agent communication.

You know, right now, there are multiple competing standards. There is the Model Context Protocol from Anthropic. There is an Agent-to-Agent (A2A) coming out of Google. Actually, Google has two. You just in your testimony referenced AP2, where I spent a while on the website last night. It is actually, I think, a much better step in the direction of—because what we need is a well-defined, legally precise language to communicate things like what is the privacy, what is the data retention, what is the logging of the interaction, and all the legally things in order to have reliable transactions between agents.

There are policy decisions there that we can defer. What we should do is have NIST or—you know, probably NIST and a number of partners in industry come together and define those standards. The White House is correctly appointed to the advantage of having the U.S. lead that. What I would like to see is to have NIST and the United States lead the world in defining agentic communication standards the same way we led the world in defining the personal ID standards, digital ID standards, that are now at Android and IOS and everything else.

Anyway. So these are—there are lots of things to talk about here.

I just want to thank you. You had really high-quality testimony, and I learned a lot reading it.

Thank you.

Mr. DAVIDSON [presiding]. I thank the gentleman.

I now recognize myself for 5 minutes.

Artificial intelligence does not change our fundamental regulatory framework which allows innovation while protecting consumers from abuse or fraud. As AI becomes more deeply integrated into our financial services and housing markets, it is essential that existing consumer protection laws covering privacy, fair lending, data security, fraud, et cetera, continue to apply fully regardless of the technology used. The principles should remain simple. If a practice violates the law without AI, it should not be permissible with AI.

At the same time, AI's increasing reliance on large, sensitive data sets raises important questions about whether our current data protection frameworks are sufficiently clear and durable for the modern economy. In my view, privacy is the base layer for ethical AI, and we need to update our privacy laws. We need it to do a much more robust job of that. Congress should reassess how consumer data is collected, used, shared, and safeguarded, without imposing rules that freeze innovation.

Finally, we should also know that a fragmented patchwork of State AI mandates risks undermining both innovation and privacy. A harmonized Federal framework can protect consumers while giving innovators the clarity and certainty they need.

This needs to be a more thoughtful approach, though, and Congress should have the debate and make the decision, not something that can be done with a two-sentence addition to some bigger bill on another topic that basically says, "We can do whatever we want." It does require a more thoughtful approach, in my opinion.

Mr. Stevens, what specific categories of consumer data are being used to train and operate AI systems today?

Mr. STEVENS. Many. Thank you for the question.

I totally agree, especially in housing, how important privacy is. This is the biggest financial transaction of your life; there are many factors that go into it. All our consumers report to us that they want to really make sure their personal data is theirs.

We use basically things like signals on what preferences they have, financial data they give to us when they are thinking about what they can afford. They work with real estate agents who use some of our tools and tell us about their hopes and dreams. We make sure that all of the above is meeting the Federal standards and laws.

When we work with other companies, as an example I gave during verbal with OpenAI, we continue to make sure that is still the case. So, when ChatGPT might want to violate fair housing, our classifier makes sure that does not happen and that all of the consumer's information is kept as theirs.

Mr. DAVIDSON. How do you ensure that you protect personally identifiable information (PII)? What kind of transparency is there? What kind of recourse do consumers have?

Mr. STEVENS. Yes. The easiest way is to not—or, is to first keep it safe, so keep it on our systems that are protected. Only certain humans have legal ability to view that data or work with that data. With third-party partnerships, we usually do not share that information. If we do, under limited license, that is then deleted upon completion of the transaction.

Mr. DAVIDSON. Thank you.

Mr. Cohen, there is a lot of discussion about the importance of winning the AI race against China. Frankly, I am concerned—to beat China, we should not try to be more like China. I do not want to be like China. I want to be like America but yes, on the technology end, we want to win the AI race.

Can you give us a sense of how you view this discussion through the lens of our capital markets and give us your perspective on the level of AI adoption Nasdaq is seeing from the broader market and China in particular?

Mr. COHEN. Thank you for the question.

Our focus continues to be, as an operator of markets here in the U.S., to make sure that the markets here are the most robust, vibrant, most attractive in the world and we will use AI to continue to ensure that we do that.

We do it—and I spoke about this before—by introducing whether it is order types of functionality that democratize access, that allow smaller broker-dealers to participate in our markets so we have a healthy ecosystem, or we root out financial crime to make sure that there is investor confidence and market integrity, or we use surveillance to detect increasing sophistication in market abuse.

All of those require us to use AI, to invest in AI, to make sure that we are partnering with folks around here, the colleagues that I have here on this panel and others, to ensure that we ensure that the U.S. capital markets remain the most robust in the world.

Mr. DAVIDSON. Yes. I mean, in the private sector, of course, there is a lot of incentive to keep up with this arms race. On the other

side, you are dealing with regulators that sometimes have not kept up with a lot of the technology.

So, when we think about it here in Congress, what are the most important things we could do to make sure that America is the most competitive place for capital to be deployed?

Mr. COHEN. We talked a little bit about it before. The need for sandboxes, the need for the ability to continue to innovate in a safe and responsible manner, I think, is extremely, extremely important and not having overly complex regulation that we have to patch together is also very important.

Now——

Mr. DAVIDSON. My apologies. I did not give you much time to answer that. If you want to provide a longer answer——

Mr. COHEN. I can certainly do that.

Mr. DAVIDSON. My time has expired, and I respect everyone else's time.

I now recognize the gentleman from California, Mr. Sherman, who is also the ranking member of our Capital Markets Subcommittee.

Mr. SHERMAN. I want to commend Mr. Foster for his digital ID bill. I know it is running into some opposition, but, ultimately, if we cannot identify ourselves in this new digital age, this will be a problem.

I also commend him for leading a letter asking that the Financial Stability Oversight Council (FSOC) to look at the financial risks of an AI bubble.

Ms. Manfra, do you see signs of an AI bubble out there?

Ms. MANFRA. Sir, respectfully, I am not a market analyst.

Mr. SHERMAN. Okay.

Ms. MANFRA. I am responsible for risk and compliance, like——

Mr. SHERMAN. Thank you.

Ms. MANFRA. So I will yield.

Mr. SHERMAN. But you are from Google and there is someone else who works at Google, Ray Kurzweil. I think he was once your chief technology officer, and he was before the Science Committee some 22 years ago. I asked him how long it will take for non-biological intelligence to surpass human intelligence, and his estimate then was 26 years. So we are almost there.

First of all, you hire very smart people, because to predict something and to be that close—we are spending trillions of dollars, as a species, to make AI more powerful. I cannot find a program anywhere in the world—and I would support it if I could find it—designed to monitor and prevent self-awareness and ambition, to determine what can be done to prevent AI from developing its own objectives, which I think would be hostile to ours.

There is a book—you may not have to read the book—great new book coming out—it just came out. It says, if anyone builds it, everyone dies.

Is Google—do you have a department, do you have a budget, for monitoring, for preventing self-awareness, ambition, or AI creating its own goals?

Ms. MANFRA. We invest a great deal in ensuring that the AI capabilities we are developing is in line with human values——

Mr. SHERMAN. I have always heard that, but I cannot find a single scientist who is looking for self-awareness and ambition. Obviously, you do not want criminals stealing our data or our money, and what you describe fits into that category.

Can you name one person whose job it is at Google to prevent AI from becoming a creature rather than a tool?

Ms. MANFRA. So let me get back to you. We do have researchers that are heavily invested in this topic. So, if I can, I will get back to you. It is not my area.

Mr. SHERMAN. Please. Please get back to me because I have not been able to find anyone. Then you ask about these issues, and you get this vague “align with our goals,” and the goal usually is, “Well, look, we can make trillions of dollars by making AI more powerful,” and there is no money in preventing AI from taking over the world. That is the next generation’s problem.

One problem we have—and I will feed you one more question—is AI doing its analysis and then reflecting the discrimination that has existed in our society for many centuries. For example, you could say, if somebody grew up in a particular ZIP code, they are more likely to default on their rent.

What do you do at Google to make sure—and I think there was another study that says, if you want to analyze who is going to be successful at Yale, it turns out the best predictor is being named, I think, “Jared” or some other name associated with the elites in our society.

What do you do to make sure that the prejudices of the past are not built into the computers that will control the world in the future?

Ms. MANFRA. Thank you for the question. This is something we care deeply about and issued our responsible AI ethics principles nearly a decade ago.

So our approach, first, is to ensure that humans are involved in the setting of the parameters, if you will. We are constantly designing, redesigning, and then monitoring to ensure that we have an unbiased approach and we are always iterating. It is not—

Mr. SHERMAN. Do you have a program that—

Ms. MANFRA. Yes.

Mr. SHERMAN [continuing]. prevents the ZIP code that you were born in from influencing the decision that is made?

Ms. MANFRA. I know we look at those things to ensure that we do not have—I will get back to you on a specific program.

Mr. SHERMAN. I will ask everyone to get back to me on whether you are focusing on preventing AI from becoming a creature.

I will yield back.

Mr. STEIL [presiding]. The gentleman yields back.

The gentlemen from Tennessee, Mr. Ogles, is recognized for 5 minutes.

Mr. OGLES. Thank you, Mr. Chairman.

Thank you to the witnesses.

You know, obviously I serve on Financial Services. I also serve on Homeland Security, where I am the chairman of Cyber, which would obviously overlap with AI. This obviously, when you look—and, quite frankly, Mr. Chairman, when you look at AI, what really

got my interest in this topic was the national security side of the financial services conversation.

As we look at artificial intelligence in the context of financial services, I think it is important we recognize that we are dealing with a technology that does not fit neatly into traditional policy frameworks. AI is not a product or a single system; it is a capability layer that will influence everything from market structure to fraud prevention to consumer decisionmaking.

That means the questions in front of this committee are not simply about regulating a new tool. They are about whether our existing financial architecture, our risk models, our supervisory expectations, disclosure rules, or even our assumptions about human judgment are prepared for a world where some of our core analytic work is done by systems that learn and adapt at scale.

At the same time, AI gives institutions the ability to detect threats faster than humans ever could, analyze complex data sets that were previously unusable, and offer consumers services that are more personalized and more efficient.

The challenge for Congress is understanding where AI is simply accelerating what firms already do and where it fundamentally changes the nature of a financial decision, a compliance obligation, or a market signal.

My goal today is not to choose a side between regulation and restraint. It is to ensure that, as AI becomes more embedded in our financial system—and, as said previously, it is here, it is not going away—that we understand the concrete risks, the real opportunities, and the limits of the technology and, I might argue, the unlimited potential of the technology. We need clarity where clarity is necessary, flexibility where innovation requires it, and a realistic view of how these systems operate in practice.

Ms. Manfra, you mentioned grounding and outcome-based evaluations in AI risk management. Can you give a real-world example of how grounding has corrected or improved financial AI models' output and how regulators should think about evaluating whether grounding was done properly?

Ms. MANFRA. I can get back to you on a specific example, but I would say, in general, the core to what we need to focus on is having transparency and explainability.

So, as—which we have invested a lot in and work with a lot of our financial consumers as they use AI for things like fraud detection, anti-money laundering these various decisions that have this high risk, to be able to ensure that they can go back and understand why the model made the decision or the recommendation that it did and enable the compliance with existing laws that do apply to these scenarios as well.

So that is a space that I think is very important, is ensuring that transparency and that explainability, in particular for financial services, though they are not the only industry, but to enable AI for these heavily manual but oftentimes high-risk, with a lot of false positives that put a lot of burden onto organizations.

So I believe it actually can—if organizations implement it responsibly, you can reduce your compliance obligations, better manage your risk, and get better outcomes for consumers and partners.

Mr. OGLES. I think for those who are watching at home the key here is that transparency and understanding because the financial institutions are required—there are compliance requirements. If they are using AI to achieve those requirements, to be in compliance, they need to understand how AI is helping them get there but then also understand where it may make mistakes or hallucinations, right?

Mr. Cohen, your Dynamic M-ELO AI-powered order type adapts to real-time market conditions. What specific signals or data streams do they rely on? And should investors have standardized transparency into how these AI-assisted order types behave?

Unfortunately, you have 40 seconds.

Mr. COHEN. I might come back to you with details in writing.

Mr. OGLES. Give us that overview.

Mr. COHEN. So we take in 130 different signals from the market to determine how that order type should operate. Every 30 seconds, we take that in because real-time market conditions, they give you a sense—we are processing millions of messages per second. To be able to process all of that, we need to use AI to ensure that we are staying one step ahead of the market conditions that then allow our investors to get the kind of execution they require.

Mr. OGLES. Yes, sir.

Mr. COHEN. Remember, we are highly regulated, so everything we do, we need to have the Federal Communications Commission (FCC) approve. They need to make sure there is explainability and reproducibility on what we provide.

Mr. OGLES. Mr. Chairman, I will just say that, as we look at the national security landscape, the financial landscape our adversaries are leveraging AI without any guardrails, and we have to be prepared and ready to, quite frankly, go on the offense.

Mr. Chairman, I yield back.

Mr. STEIL. The gentleman yields back.

The gentleman from Missouri, Mr. Cleaver, who is the ranking member on the Subcommittee on Housing and Insurance, is now recognized for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman.

If I could also thank Mr. Lynch for kind of leading this effort on our side.

I just have one question. My interest in AI grows daily, and I am even more concerned today than I was yesterday.

If you look at what is happening in the Federal Government, being reshaped by the President and the Supreme Court, 75 percent of fair-housing staff is gone. It is not, like, a couple people, but 75 percent has gone since January.

Because I have been around, I know that when we are talking about trying to deal with housing, which is easily the number one or number two most significant domestic issues we face, I am further—my paranoia has grown stronger because I am concerned that AI could also be an excuse—“Well obviously, this is fair.”

It goes along with something that was raised earlier. Fair housing, I mean we are—“Do not worry about it. AI is going to make sure that everything is fair. I mean, after all, AI cannot discriminate.”

It is infuriating, first of all, that this is already taking place in the government, and then we have to deal with AI possibly doing even more damage to fair housing. If everything was clear and equality was a part of everyday thought I would not even need to raise this issue but that is just not the case.

So, at a time when civil rights and fair housing are issues, growing issues instead of being subsided, somebody help me understand how—why AI will not make this worse.

Mr. STEVENS. I would be happy to, Congressman.

Working at Zillow day to day, we totally believe that fair housing is paramount. I would say, an opportunity that AI—we have already seen is, you can start describing what home you are interested in a more natural language. No one wakes up and goes, “I want three bedrooms, comma, big backyard, comma,” like a computer would standardly want. With generative AI, you can say, “Hey, I am looking for that big backyard, close commute to work,” that kind of thing.

The problem is, there are certain fair-housing questions that are not legally supposed to be answered and that is what led to our Fair Housing Classifier. It is probably one of the more complicated models we have developed at Zillow. Instead of going, “Okay, we will just keep that to our ourselves,” we felt that the right thing to do to help other researchers, other institutions, was to make that available to others. They can contribute back and, of course, use it in their own systems.

So that means every deployable AI in the housing sector can take advantage of a fair-housing-compliant method.

Mr. CLEAVER. Well—and I appreciate your response. I am wondering about the others on our esteemed panel today.

Do any of you have a suggestion?

Mr. BRANCH. Representative, may I respond to your question?

Mr. CLEAVER. Yes.

Mr. BRANCH. There is an assumption built in with a variety of companies when they discuss the positives of AI, and one of those built-in assumptions is that AI is going to remain aligned to human values or American values. What they are not acknowledging is the possibility of AI drift. That is when AI starts to drift away from what some of our values actually are. That is when you see instances of kids being encouraged to harm themselves or discrimination in banking decisions and that is why it is important to have these regulations in place to ensure that these companies are being regulated and ensured that they are making sure that their algorithms are working in place.

There are ways to do that. We have spoken a lot about China today. I do not think Americans have to choose between winning a hypothetical AI race in China or being protected from harmful AI products. I think that is a false narrative and a false binary.

Mr. CLEAVER. Thank you.

Thank you, Mr. Chair.

Mr. STEIL. The gentleman yields back.

I recognize myself for 5 minutes.

I think we have seen a real positive shift in AI policy from the previous administration to the Trump Administration. The Biden Administration’s precautionary approach was stifling innovation.

The Trump Administration's AI action plan try-first approach is the right approach, in my opinion.

I think financial services have been leading the way in applying AI in the real world for decades, so I just wanted to get a couple instances on the record.

I will start with you, if I can, Mr. Cohen. Can you just describe a couple ways that Nasdaq is utilizing and has been utilizing AI in the financial services space?

Mr. COHEN. Thank you for the question.

I will go back to my opening comments, in that we focus on three core principles when we employ AI, and I talked about liquidity, transparency, and integrity.

With regards to integrity, our anti-financial crime platform, Verafin, is allowing banks to operate with confidence when it comes to fraud management and it is allowing them to achieve goals that they otherwise could not achieve on their own when they limit fraud in the market.

Mr. STEIL. So it is essential to manage fraud, illicit trading broadly in the risk space.

Mr. COHEN. Absolutely. It does more than any single institution can do on its own, because it is cloudinated, AI-enabled, and uses consortium data.

Mr. STEIL. Let me jump to you, Ms. Manfra, if I can, a good Wisconsinite. Good to see you here.

Can I ask you to pinpoint, how are firms in particular thinking about this when they are deploying this new technology?

Ms. MANFRA. What I would say, and reiterate what you probably heard before as well, is, the financial services firm has a long history in managing model risk, and there are processes and regulations and oversight in that place.

So what we see with our financial services customers is, as you noted, very innovative uses for these set of capabilities, but also very thoughtful. So they think about things like, how do I ensure a human in the loop, how do I ensure I have proper governance in place, how do I ensure that I understand how I can meet my risk management and compliance goals and—

Mr. STEIL. So, knowing that these firms are going through this deliberative process to think through how they are balancing reward and risk in utilizing AI, I want to come back—because we discussed the sandbox concept earlier—I want to come to you, Mr. Cohen, with a short question here.

Earlier this year, Chairman Hill and I introduced the bipartisan Unleashing AI Innovation in Financial Services Act, which enables regulatory sandboxes at the Federal financial agencies that are targeted in size and scope.

These sandboxes, they have a handful of things: They have to be approved and overseen by Federal regulators; they require compliance strategies and risk management, which we were just discussing; they must not impose systemic or national security risks—obvious to make sure we are doing that.

So Federal regulators will impose appropriate limitations or conditions on them. Additionally, fraud and unsafe and unsound practices will remain prohibited under the sandbox.

So the idea that these sandboxes create a free-for-all and allow participants to flout all the rules they just do not like, it is simply not true, right?

So, rather, the sandboxes provide a more secure environment to experiment with AI, enabling innovation, with built-in guardrails, Federal oversight and so this is how I think we learn from best practices for governance while exploring the applications that will improve American financial life.

So here is the question: Would these AI sandboxes enable regulators and market participants to responsibly experiment with AI and learn best practices?

Mr. COHEN. Yes, the key qualification is what you said; it needs to be controlled, it needs to be targeted, it needs to be time-boxed, and it cannot be used to circumvent—and we have a very practical example of that.

We, as a highly regulated institution, often run pilots with the SEC, where we are really transparent about the results of that pilot, and we ensure that informs decisionmaking and allows for better outcomes for investors in the markets.

Mr. STEIL. So it is not really a free-for-all. It is a sandbox that has a regulatory structure in place. Underlying laws apply. Ms. Manfra laid out how firms are thinking about applying AI. They are going through a deliberative, thoughtful process.

In your opinion, do sandboxes help create innovation and development in the United States in a thoughtful, structured way?

Mr. COHEN. They have. They have. They have been critical to our innovation. Again, if it is controlled, time-boxed, and targeted and transparent, it yields positive results.

Mr. STEIL. I appreciate that.

Ms. Whitmore, I wanted to take my time and come to you and discuss, in particular, how AI can eliminate fraud, deepfakes, and really help us. In 10 seconds, can you add to your previous comments?

Ms. WHITMORE. We will be happy to follow up with a written response to that. Thank you.

Mr. STEIL. Thank you very much.

I yield back.

I now recognize the gentlewoman from Ohio, Mrs. Beatty, who is also the ranking member of the Subcommittee on National Security. She is now recognized for 5 minutes.

Mrs. BEATTY. Thank you, Mr. Chair and Ranking and thank you to the witnesses.

Wow. A lot of good testimony. I never thought about asking my grandchildren, when we move, what they would like to take into a new house. So you put it in a whole new perspective for us.

A lot of words today, on both sides of the aisle, and they all come together. You know, we have heard things like we need to strike the right balance, we should not discriminate with AI, we should have accountability, it should be well-defined, there should be responsible AI, we need clarity, we need legal and policy definitions. All of that is true, whether it came from the Republican or the Democratic side.

I do not know that I have heard a lot of responses that are definitive to say, “Here is how we are having responsible AI.”

I have a great concern. I serve as ranking member on the National Security Subcommittee, and I am focused on preserving the safety and the security of our financial systems and protecting consumers from fraud.

So my first question—and I am going to try to get through a series of them.

Mr. Branch, we will start on this end. How is AI used in anti-money laundering and fraud detection, and how effective is it as a tool in our illicit finance arena?

Mr. BRANCH. Representative, thank you, but I apologize, I am not an AI fraud analyst. That is outside of my expertise, but I could have my colleagues get back to you.

Mrs. BEATTY. Okay.

Anybody else want to take a stab at that?

Mr. COHEN. I can try.

So we operate a financial crime management platform called Verafin. I have spoken about it here. Again, it is cloud-native, AI-based. We have over 2,700 clients. We have 725 million accounts, just to give you a sense of how large that pool of consortium data that we dig into is.

We use that—we use that to protect small and medium-size institutions, small banks, super-regional banks from the cost of fraud so they can operate and provide everyday customers and investors and clients of theirs with the security that they deserve when they invest their money and then have transactions associated with that institution.

So that solution is really paramount to creating safety and responsibility along the traditional rails.

Now, we also are looking at nontraditional rails like crypto rails and others that consider how payments and transactions may be—may be—subject to fraud as well. So that is where we are extending it, but it is incredibly important and valuable for small and medium banks.

Mrs. BEATTY. Okay.

I will go to another question.

We talked about—or someone, on both sides, said that we should not discriminate. One of my primary concerns about the use of AI, especially in financial services, or maybe not necessarily with just financial services, is the potential for bias in algorithms and that they lead to unfair results. You can only be as good as the individuals that put the data or gather all the folks in it.

So, as we look to develop a comprehensive AI regulatory framework, how do we ensure that the use of AI does not lead to discriminatory lending or pricing or underwriting or any other area that we use algorithms?

Anybody want to take a stab at that?

Mr. STEVENS. Thank you, Congresswoman, for the question.

I will say, I was first hired by Zillow to work on the Zestimate and two answers would be: additional data and then also a national right-sized framework that we can apply across the country.

On additional data, that is the benefit of GenAI. For the Zestimate, we can now look at additional comparables maybe outside of your direct neighborhood to get a more balanced and fair evaluation. We can also look at the listing images, the listing de-

scription—all this unstructured data that was not possible to be ingested before.

At the same time, we have to do a lot of checks that is the right data and there is no inherent bias within it and that is where we use, like, the NIST Risk Management Framework (RMF) to make sure, before we deploy, that it is a fair evaluation.

Mrs. BEATTY. Thank you for adding and saying that because you—the outcome has to be that you have people from other communities and there is a diverse pool of folks at the onset. So it would help us not have discriminatory practices with that.

Thank you, because I know, for example, women have not always been included in trials, and so when you are building these algorithms, you have to have people in examples that you put in. So that is something that I am watching carefully.

My time is up. Thank you, Mr. Steil. I yield back.

Mr. STEIL. The gentlewoman yields back.

The gentleman from Florida, Mr. Haridopolos, is now recognized for 5 minutes.

Mr. HARIDOPOLOS. Thank you, Mr. Chairman.

I appreciate this thoughtful conversation. I know Congressman Liccardo and I are working across bipartisan lines and trying to find solutions of this and become a hyper-partisan issue which is, I think, all of our goal today, especially as we face this increasing threat from China. We just had a hearing in my subcommittee that I chair on the threat in space and some of those challenges you face, of course, here on Financial Services, a little bit different model.

If I could, Ms. Manfra with Google, if I could ask this question. One of the things that I have been concerned about—and this goes across the gamut as far as age groups too—are these deep fakes, this idea where AI has used—someone's reputation can be literally eliminated in a day, because there is some type of fake video. What does a huge company like yours do to try to identify these to take them either offline or to identify that these are deep fakes?

Ms. MANFRA. Well, I will say just to start—first, thank you for the question, and it is something that has been concerning for us for a long time, and we have invested a lot in technical measures to be able to better detect as well as making a lot of these measures and processes that we have learned from available to others to be able to do that and to rapidly be able to take those down, and happy to get more details if you are interested in more of the specifics on the technology that we use to be able to—

Mr. HARIDOPOLOS. I think that would be very helpful because, again, this is a reputational issue.

Ms. MANFRA. Absolutely.

Mr. HARIDOPOLOS. It takes a lifetime to generate a reputation. It can be destroyed in a minute.

Ms. MANFRA. Absolutely.

Mr. HARIDOPOLOS. I think that this is especially true not only in politics but just everyday life. We have seen how people get hazed, bullying happens, especially at the middle schools and high schools, and this could easily be done with just a basic technology. So any advice y'all have would be great.

I think the second one, I will ask with Nasdaq, if I could. There are existing rules of the road. Are those guide rails sufficient for what you do every day in the investment world and are there enough recommendations that our committee is putting out and you are, of course, producing and providing for us—where are we? Are the guardrails sufficient now? Are there a lot more guardrails needed, in your opinion, to make sure the financial markets are protected from AI in a negative way?

Mr. COHEN. Our markets, as you know, are highly regulated and have a lot of transparency to ensure that we run our markets in a way that is enduring from a trust perspective. “Trust” is not a word we have spoken about a lot, but trust is extremely important when we talk about our markets.

So the fact that we are highly regulated, run mission critical infrastructure, requires us to have certain standards outside of just thinking about AI. I think we can use that as the foundation, whether it is the securities law, it is Reg SCI, it is following this, all of that is foundational.

What I mentioned earlier, and I think is incredibly important, as this technology advances and maybe creates gaps, we need to make sure there is information sharing, that we have a safe space to share information with one another about what we are seeing, about what we are seeing within our own four walls and across the industry. So I think that would be what I would advocate for to make sure that we have what we need on a principle-base and from a Federal level. Those are the two things that I think we would also want to see.

Mr. HARIDOPOLOS. Thank you.

Ms. Whitmore, what keeps you up at night about AI? What is the biggest concern that is out there, in your opinion? You see this every single day. We deal with a lot of issues every single day, but you are focused on AI. What is the fear factor that you have, wondering, God, I hope they do not do this, or this is the threat that is most prevalent out there, and in both the business community and the general internet space?

Ms. WHITMORE. Thank you for the question, Congressman.

First, I think, just the challenge that attackers are leveraging AI for, which is primarily speed and scale. So now we are looking at reduced timeframes to execute a ransomware attack to 25 minutes, and that includes from initial access into an environment to the time that they encrypt or steal data in that environment.

The second is the concern that attackers are specifically targeting AI to then misuse it intentionally, right? That requires a use of some specific guardrails to put in place but in particular, one, we can—to solve these two challenges, right, we can—we need to be fighting machines with machine speed. That is the only solution that we are going to have to transform the way that we detect and respond, and to truly get to decreased numbers in both of those categories.

Second is the capability to ensure that as these systems are running within environments, that we have got the critical levels of visibility into the actions they are taking so that when an attacker does decide to change the functionality of an agent and have it go rogue, that we can detect that and stop it as quickly as possible.

Mr. HARIDOPOLOS. Well, I appreciate the thoughtful answers to those. Mr. Chairman, I yield back.

Mr. MEUSER [presiding]. The gentleman yields. The gentleman from Illinois, Mr. Casten, is now recognized for 5 minutes.

Mr. CASTEN. Thanks so much. I appreciate y'all.

I want to focus specifically on securities regulation. I am going to oversimplify, but I am going to—Mr. Cohen, I will ask you to correct me if I have got it wrong. We have got Federal securities regulation through the SEC. We have got an additional State layer with registrations and licensing laws, and then, of course, the rules that the individual stock exchange has put in. Are you generally supportive of that structure? Having those three layers of regulation?

Mr. COHEN. We are and do not forget Financial Industry Regulatory Authority (FINRA).

Mr. CASTEN. Yes.

Mr. COHEN. So we have SEC, FINRA, and then obviously we have our own, if you will, responsibilities as an exchange, highly regulated exchange, listing qualifications, for instance.

Mr. CASTEN. Fair point. I raise that only because I had some concerns about in your testimony, when you supported Federal preemption of State laws related to AI. So, I just want to pick at this point a little bit. I am concerned partly because the Trump White House has instituted massive cuts to SEC. So if this is a three-or four-legged stool, it is kind of a wobbly chair right now. I get nervous about saying let us shorten all the legs to make it work.

I also have a concern as an engineer, as a guy who built some AI models before I came here. I do not think this is as big a deal as we talk about it. I think we use words—you know, we call it intelligence, but it is just—it is a massive correlation machine. It is not intelligent, per se, but I can plug in huge amounts of data on the markets and historic trading trends, and say I want this algorithm using those historic correlations to identify relationships and optimize for profit margin. It can do that. It is really cool, right? I can plug in the entire Taylor Swift catalog and say put let us take a Tom Waits song and make it sound like a Taylor Swift song. I can do that. It is not intelligent. It is just massively correlative.

If—there is no reason why anybody using an AI tool is necessarily incentivized to say: Let me optimize this for truth. Let me optimize this for ethics; let me optimize it for legal compliance. I am going to optimize it for the thing that is valuable to me, making something that sounds like Taylor Swift, making—you know, making money on markets.

I guess I do not understand why—or maybe correct me if I am misreading you. Would it not be wise to prevent States from protecting investors from AI-enabled market manipulation, especially if the Federal Government is not doing it?

Mr. COHEN. Let me answer the first part of your question. As an exchange, we are an SRO, self-regulatory organization, and we have a public mandate. Our public mandate is to ensure that we run fair and orderly markets, and we take that responsibility very seriously. So our north star is just that. When we design solutions around our markets, we are thinking about making sure that—

Mr. CASTEN. I want to—and I do not mean to cut you off. I am just nervous about the clock here. I was in the energy industry for a long time. I remember there was a professor who did this experiment with a bunch of grad students where none of them had information, but they were basically in a simulation of California power markets, and they all independently, just based on the other students' trading strategy, figured out how to collude. It was when Enron blew up, it was this thing of, okay, you do not actually have to have information to collude, but there is an incentive to collude in the structure, and people will figure it out.

There was a University of Pennsylvania study recently that found that AI bots released into simulated markets will do—essentially do the exact same thing.

As an SRO, how do you—if we are not going to regulate—if we are going to provide liability shields for these companies—not about whether the tool is good, but if we are not going to provide liability shields, do we not still have to get to that?

Maybe, just to sort of put the punch line on it, and then you can use the rest of the time, there is a long legal history within the courts, within the SEC, of saying if there is not intent to defraud, you cannot hold somebody to account. My nervousness is that a lot of the people building these tools are saying, “Well, I want a liability shield. I want State preemption.” If the tool is not designed not to commit fraud, it can still be optimized and end up committing fraud. So as a market manager, how do you protect against that and what sorts of regulatory reforms would we need to do to it, modify some of these—this history that you need to show intent?

Mr. COHEN. Yes. Just to be clear, in terms of Federal preemption, our view is around minimizing complexity. What you just described, you can achieve all of that at the Federal level. You do not have to have it as a patchwork in each State where it is a struggle for people to figure out how to operate in that State. It is not just the exchanges; it is our members that we think about and the industry at large.

Again, being highly regulated, we do have a north star about how we want to serve and what our business interests are. So it is more about the complexity, and it is more about the patchwork that we are concerned about. We think we can solve for everything you just talked about at the Federal level—

Mr. CASTEN. I am out of time, but I would just welcome comments from all the respondents about—there is a hole in securities laws, and any ways that we can fix those holes to address this question of intent I think is important and would welcome all of your expertise. Yield back.

Mr. MEUSER. The gentleman's time has expired. The gentleman yields back. The gentlemen from Wisconsin, Mr. Fitzgerald, is now recognized for 5 minutes.

Mr. FITZGERALD. Thank you, Chair.

Regulatory technology, sometimes called “reg tech,” refers to innovation in technology deployed by companies to manage regulatory compliance. Mr. Cohen, how does Nasdaq use AI and other—any type of machine learning powered by reg tech tools to kind of enhance the regulatory compliance, such as trade surveillance or how much just efficiency in cost savings has gone on?

Mr. COHEN. So we have two reg tech solutions that we offer; one is for market abuse surveillance, and the other is actually Axiom, which is a regulatory compliance and reporting application. I have not talked as much about that today, but that is important because it is used by all the Tier 1 banks across the globe. It is the standard for regulatory reporting.

What we do, because we manage and orchestrate complex workflows through this tool, is we use AI for data discovery so they can go through complex regulations and understand and interpret how that piece of regulation needs to be implemented into the reporting obligations they have. Also, if they have any anomalies in their financial reporting, capital obligations, liquidity obligations, it may take them, a handful of individuals, hours, days, weeks, to identify anomalies. We can do that through AI very, very quickly, keep the human in the loop, make sure that they are center, in the center of any decisionmaking that can occur, but they do not have to do the heavy lifting to understand that there is an anomaly.

Also what we have done from a product development life cycle perspective, we are now taking regulations, reg all the way to code, through agents and allowing agents to hand off work to one another to take a piece of regulation that could be 4-to 500 pages long, and allow them to implement it in our tool and then deliver it more quickly to our clients. This is incredibly important in a world where the regulation is exponential in terms of the obligations that one needs to meet. They are changing. There are reforms. There is a different view in America versus where Europe and Asia are going.

So just as a Tier 1 bank or Tier 1 institution to keep up with it, it requires a lot of operational spend. We are trying to reduce your operational spend so you can do the things that you need to do, put money back into your balance sheet that you can then use for loans or for businesses that help small businesses and their customers.

Mr. FITZGERALD. Very good.

Mr. Stevens, let me ask you the question first, and I was—just maybe fill in afterwards. I am kind of switching it on the paper here. How are AI-driven underwriting models helping to safely expand access to credit for a broader range of borrowers? Because there are concerns, I know, that AI has led, maybe, to some riskier borrowers—I do not know how else to describe it—or that it has kind of changed, kind of the perspective on borrowers compared to the due diligence that—you know, the human that sits down and fills out the form and does everything that we are typically used to. So I was wondering if you could comment on that idea?

Mr. STEVENS. Yes. Thank you, Congressman, for the question.

The way AI is helping is by looking at additional data sources that, if we just left it up to humans, they might not have time to consider and that, I think, is helping particularly first-time buyers qualify.

At Zillow, we make sure the actual decisionmaking in the underwriting process, what we are prequalifying you for, for example, is completely human-driven. So we still rely on humans making that ultimate judgment.

Mr. FITZGERALD. Very good.

Ms. Manfra, the 1945 McCarran-Ferguson Act left insurance regulation largely to the States. With all the talk of freeing financial services from the onerous State regulation of AI, notwithstanding the Act, can the business of insurance benefit from being included in any national approach to AI?

Ms. MANFRA. I cannot speak to the specific regulatory framework of the insurance. It is just not an area of my expertise but absolutely there are lots of benefits for AI in the insurance industry, and I think would benefit from being a part of a national conversation and framework for standards of transparency and explainability.

Mr. FITZGERALD. Has it advanced quick enough or far enough to really be a tool, or is it something that is just kind of a sideshow right now?

Ms. MANFRA. For insurance companies?

Mr. FITZGERALD. Yes, for insurance companies.

Ms. MANFRA. I would say insurance companies are using AI tools—it is very different in terms of the customers and—but absolutely, they are using AI and innovating around that for sure.

Mr. FITZGERALD. Very good. Thank you all. I yield back.

Mr. MEUSER. The gentleman yields back.

The gentlewoman from Massachusetts, Ms. Pressley, is recognized for 5 minutes.

Ms. PRESSLEY. Thank you to our witnesses for joining us today.

AI is everywhere: our phones, our classrooms, our hospitals, our bank loans and job applications, every facet of our lives. That is why we must ensure that AI works for everyone, and that instead of deploying biased AI, which can create harm or compound existing harm, it needs to benefit everyone, all people, regardless of race, gender, income level, medical conditions, or other parts of our identity.

Mr. Stevens, should we prohibit the use of AI that discriminates on the basis of race, gender, or other factors? Just a yes or no.

Mr. STEVENS. Especially in housing, I believe yes. Fair housing, make sure that we eliminate all forms of racism, different disparate impact, that kind of thing.

Ms. PRESSLEY. Okay. I will ask the question of everyone, just for the purposes of the record. So just a yes or no. Should we prohibit the use of AI that discriminates on the basis of race, gender, or other factors? Yes or no? Ms. Manfra.

Ms. MANFRA. Yes.

Ms. PRESSLEY. Mr. Cohen?

Mr. COHEN. Again, we apply three principles. We try to promote transparency, liquidity—

Ms. PRESSLEY. Yes or no.

Mr. COHEN [continuing]. integrity in our markets and as a highly regulated institution, we are making sure that we prevent that in our algorithms.

Ms. PRESSLEY. Mr. Stevens, yes or no, again.

Mr. STEVENS. Yes.

Ms. PRESSLEY. Ms. Whitmore?

Ms. WHITMORE. Yes.

Ms. PRESSLEY. Mr. Branch.

Mr. BRANCH. Yes.

Ms. PRESSLEY. Okay. Thank you.

We need, urgently, civil rights laws for the 21st century in the age of AI, which is why I have joined with Senator Markey and also with Congresswoman Yvette Clarke to introduce the AI Civil Rights Act. It is urgent because the truth is that we are already behind. People are already being exploited and discriminated against with the use of algorithms.

Now, let us take an issue like housing, for example, which, in my opinion, is a human right. Everyone deserves more than just shelter. They deserve to have a home. It is safety, it is dignity, it is health, it is mobility. In 2025, the Trump Administration has gutted the key agencies that protect against housing discrimination: the Consumer Financial Protection Bureau (CFPB) and Housing and Urban Development (HUD) Fair Housing Enforcement Offices. They are even trying to undo consent orders that are already in place, like the Townstone discrimination case in Chicago. This gap in civil rights protections is an opening for continued discrimination. One study found that mortgage lenders are 80 percent more likely to reject Black applicants compared to White applicants with the same qualifications.

Mr. Branch, should we have additional oversight tools, such as assessments, to test the algorithms out before companies can use AI on the public? Yes or no?

Mr. BRANCH. Yes.

Ms. PRESSLEY. Do any of our witnesses, other than Mr. Branch, disagree with that? Okay. Let the record reflect that no one disagreed.

We know that bias exists in our Nation. We see the inequities all around us. I represent the Massachusetts 7th, a vibrant, diverse, dynamic district, and one of the most unequal in the country. We are in a 3-mile radius from Cambridge, home to MIT, Harvard, and AI advancement, to Roxbury, the blackest part of my district. Life expectancy drops by 30 years and median household income by \$50,000. Now, that is the result of intentional lawmaking, which is why I believe we have to be just as intentional in undoing the harms and charting an equitable path forward, because AI is trained on data that is already biased and by humans that have biases. It can replicate and exacerbate these harms unless we have oversight and prevent it. We must not allow AI innovation without AI protections. In a world of artificial intelligence, we really cannot lose sight of what is real, and that is the people, the people and their livelihoods and their lives. If Republicans are serious about protecting our elders from fraud, and consumers from discrimination, then Congress must pass the AI Civil Rights Act.

Thank you. I yield back.

Mr. MEUSER. The gentlelady yields. The gentleman from Indiana, Mr. Stutzman, is now recognized for 5 minutes.

Mr. STUTZMAN. Thank you, Mr. Chairman. Appreciate you all being here today.

Before I begin, though, I would like to address some concerns raised by my colleagues across the aisle. The Unleashing AI Innovation in Financial Services Act enables federally regulated entities to experiment with AI in secure environments, overseen, approved, and subject to the conditions of their Federal regulators, including

for compliance and risk management. Importantly, the sandboxes must not present systemic or national security risk; two, unsafe and unsound practices and fraud remain prohibited; three, the sandboxes under unleashing AI would be targeted, time limited, and subject to regulatory approval and oversight; finally, the participants' compliance strategies must be approved by the appropriate regulator, and who would retain enforcement authority subject to the terms the regulator sets.

So it has been great to have President Trump back in the White House for many reasons, but especially for the reason we are discussing here today. During the Biden Administration, AI innovation was viewed primarily as a threat to the American people. While President Trump has set the country back on track toward innovation and American AI dominance on the world stage, we cannot have Biden's allies in anti-innovation States, like California and Massachusetts, setting the trend on overregulating AI.

I will follow Ms. Pressley's format, and I will begin with each of you. Do you think that a patchwork quilt, or a patchwork of inconsistent AI laws would help encourage innovation or stifle it? Yes or no? Stifle or unstifle?

Ms. MANFRA. It would stifle innovation and add complexity and burden to—

Mr. STUTZMAN. All right. Mr. Cohen.

Mr. COHEN. Add complexity and stifle.

Mr. STEVENS. Add complexity and stifle.

Ms. WHITMORE. I think too much complexity largely benefits attackers and not the defenders of our environments who are also looking to innovate.

Mr. STUTZMAN. Mr. Branch.

Mr. BRANCH. I do not believe that this stifles innovation. There is a lot of talk about different States that have different models. However, oftentimes, these State laws overlap, and so, it is not a fragmented 50-State analysis that needs to be done. In fact, oftentimes, many of these States overlap. So, they are not competing with a variety of State laws. The language in the laws overlap, and we see that in company valuation. If this innovation is being stifled, then these companies would not be worth trillions of dollars, and America would not be leading in the AI race, which we have been since the inception of this AI race.

Mr. STUTZMAN. But you do not think that having Federal guidelines and then having States having their guidelines, that is going to create complexity and actually people just finally say, "We are out?"

Mr. BRANCH. Well, respectfully, Congressman, the States have had to step up because we do not have Federal guidelines. They are actually begging for the U.S. Federal Government to pass some form of regulation, but they have not passed that regulation. That is what the American people are waiting for Congress to do.

Mr. STUTZMAN. All right. Ms. Manfra, is it not true that many of our existing risk management frameworks and governance practices already apply to AI?

Ms. MANFRA. Yes.

Mr. STUTZMAN. So following up a little bit, can we update our guidance to be fit for AI without reinventing the wheel here?

Ms. MANFRA. Absolutely. As has been noted, the existing laws do apply. However, there are areas, such as ensuring transparency and explainability, as we have discussed, maintaining human in the loop, some of these other areas where it is important to clarify in existing rules. But we do not need new—

Mr. STUTZMAN. All right. I want to talk a little bit about the risks a bit. We have had algorithmic trading in this country for decades, and these models are increasingly incorporating AI. One concern I have heard is that AI and machine learning could exacerbate herding. This is where trading models end up encouraging the same activity across firms because firms are using the same or similar models.

Mr. Cohen, what do you make of the risk posed by model similarity?

Mr. COHEN. That risk existed before AI. So you might have individuals that work for one firm go to another firm and design models that are very similar to one another, and therefore, exacerbate volatility or have the herd effect.

Post some market events over the last 10 to 12 years, we, the SEC, and the industry have taken action to ensure that we have volatility guards. We put in Reg SCI. We put in a number of different rules to protect the marketplace but maybe most importantly, we have asked those that are introducing algorithms to test them and then monitor them throughout their lifecycle because it may be that a trading strategy is in the market for 3, 4 years, but a change in market condition then snaps the algorithm.

So we are—we are really focused not just on the testing of it when it comes into the market but also on the monitoring and the transparency we have once it is in the market. FINRA has a responsibility to go into all of these broker dealers and make sure they have written procedures that they test it, they monitor it, and they are taking care of it in a judicious manner.

Mr. STUTZMAN. Do you know, is that happening frequently, or is it just on occasion that you are seeing a herding strategy? Is it daily? Is it weekly? Monthly? I mean, does it happen—how often?

Mr. COHEN. I would not know the exact details around that. We can come back to you on that question.

Mr. STUTZMAN. All right. Thank you. Thank you, Mr. Chairman. I see my time has expired. I will yield back.

Mr. MEUSER. The gentleman yields. The gentlewoman from Texas, Ms. Garcia, is now recognized for 5 minutes.

Ms. GARCIA. Thank you, Mr. Chair, and thank you to all our witnesses here today.

AI will impact every industry, every line of work, and every type of business in the near future. I think we can all agree to that. AI has potential to save employers on labor costs and increase productivity, but it can also disrupt workplaces and lead to loss of millions of jobs. At home, in my district as a working class district, 77 percent Latino, many of my constituents are concerned—in fact, deeply concerned—about how AI will impact their jobs and their livelihood.

Mr. Branch, could you quickly discuss what the private sector, Congress, and the public sector can do to best address workforce challenges as AI becomes more widely adapted?

Mr. BRANCH. Thank you, Congresswoman.

They can speak with these workers and allow for worker input. They can speak with unions. Many unions are discussing algorithmic pricing. They are discussing wages and the necessity to ensure that there are fair wages as well. So I would encourage them to collaborate with unions and their employees.

Ms. GARCIA. Thank you.

You also mentioned in your testimony how important it is to include the States when crafting AI policy. I mean, I think you just said that you need the national framework and then the States will act, and States actually have acted because the Federal legislation has not acted.

In 2025, 38 States have adopted or enacted around 100 measures. More than that, Colorado and Texas both enabled omnibus legislation regulating AI. In fact, our Governor just signed a bill to that effect, and will go into effect in January, and it is a new regulatory framework that applies to developers and deployers of AI systems.

Many of the witnesses today spoke about the importance of cooperation between the Federal and State policymakers. Despite this, President Trump shared his intent to enact some type of AI moratorium through an executive order via social media just yesterday.

As someone responsible for Nasdaq's financial technology division, Mr. Cohen, would it be practical—what would be the practical impact of such a moratorium on consumers and investors?

Mr. COHEN. At Nasdaq, we do not serve retail investors directly. Institutions are our customers. From our perspective, again, we want to make sure that there is a balance between the types of rules and regulation that come in, more principle-based, allow us to advance the technology and innovate while making sure it is safe and responsible. We think from the perspective of the governance we have internally, the foundation of the rules that we have in the marketplace today, following this gives us that great foundation that we can build off of.

Ms. GARCIA. But what would a moratorium do?

Mr. COHEN. With respect to—

Ms. GARCIA. The impact on Nasdaq and the work that it does.

Mr. COHEN. I think we have been operating in a space with uncertainty already. So I do not think that it would have a significant impact on us if there was a moratorium.

Ms. GARCIA. The Trump Administration's AI Action Plan and recent actions pursue an aggressive deregulatory approach to AI, dismissing the role of both Republican and Democratic States. Rather than leveraging existing regulations and enacting new risk based and proportional regulation, President Trump and congressional Republicans have tried and failed twice to pass broad Federal preemption.

Mr. Branch, can you shed some light on how State AI laws have helped to fill the current Federal enforcement gap in areas like algorithmic discrimination and consumer protection?

Mr. BRANCH. Yes. Thank you for the question.

States have stepped up to the bat in response to Congress not passing Federal legislation, and they have listened directly to their

constituents. They have passed laws in terms of deep fake non-consensual images. They have passed laws with regard to pricing as well as discrimination and this would essentially be usurping the States' abilities to protect their own consumers. This is something historically in the United States has been a right reserved to the States. There has never been a previous administration that has directly assaulted the States' abilities to protect their own consumers. So this is a very unique situation.

Ms. GARCIA. Thank you.

Ms. Whitmore, I know I served on the AI task force working group that was put together from this committee and it always struck me, the final question really becomes who is auditing and who is monitoring and making sure that the AI—who is monitoring AI, and who is going to make sure that everything they are doing is safe, secure, and something that will not negatively impact everyday Americans?

Ms. WHITMORE. I think you are articulating the criticality of security being closely coupled with AI innovation so that we can answer those questions very clearly and ensure that the communications that are occurring are legitimate.

Mr. MEUSER. Thank you. The gentlelady's time has expired.

Ms. GARCIA. Thank you.

Mr. MEUSER. The gentleman from Texas, Mr. Williams, the chair of the House Small Business Committee, is now recognized for 5 minutes.

Mr. WILLIAMS of Texas. Thank you, Mr. Chairman. Thank all of you for being here today.

Artificial intelligence and the banking sector are two industries that are working together hand in hand. For financial institutions, artificial intelligence is a valuable tool that allows them to navigate risk assessments and stress test, detect and prevent fraud, assist with regulatory compliance, and several other critical operational duties.

My district back home in Texas, Fort Worth and around in the metroplex and out West, loves their community banks, who are the backbones of their communities. As artificial intelligence continues to change the landscape of banking, it is crucial that we ensure that AI is empowering rather than complicating the work of community banks. So, Ms. Manfra, what would we be thinking about to ensure that this technology can reach community bankers and allow the importance they offer to grow and flourish and help people like myself in Main Street America?

Ms. MANFRA. Thank you for the question, sir.

I think one of the opportunities, one of the greatest opportunities with AI and cloud and associated technologies is the ability to bring access to data and capabilities that historically was only reserved for people with deeper pocketbooks, as it were. So being able to empower community banks and other smaller organizations that are more resource-constrained, AI can give them access to that data in more real time. It also allows them to benefit from those efficiencies with the limited staff to be able to provide better services to their customers and maintain that trust that you noted in communities.

I think what is important is ensuring that we do not create regulatory burdens that unfairly impact organizations that have less resources to manage those, would be my final point there.

Mr. WILLIAMS of Texas. Thank you.

AI tools are reshaping how businesses grow and enter capital markets. I see that in my business. I am in the car business and tools that help companies analyze market trends and reach investors prepare for fundraising used to be available only to the largest firms with unlimited resources. Now artificial intelligence has the potential to level the playing field by giving smaller and emerging companies better insight, data, and more efficient ways to market themselves to investors.

Mr. Cohen, how is AI changing the ways smaller companies prepare for and access public markets?

Mr. COHEN. You touched on a really important point, which is if we get AI right, it will democratize the way that small businesses can access and have access to the same tools as large businesses. They do not have the engineering talent, maybe the R&D budget, and maybe the sophistication of the larger firms. So it is up to companies like us to provide capabilities, make them available to those companies, whether it is in the capital raising side of the house or in a secondary trading side of the house, to ensure that when we put these capabilities out there, it is for all investors. It is for all of the individual and corporations that we serve and that allows them, if you will, to level the playing field and then grow their businesses.

Mr. WILLIAMS of Texas. Great.

Ms. Manfra, in your testimony, you highlighted Google's use of artificial intelligence to combat money laundering, fraud, and scams. Across the world, organized fraud syndicates are stealing billions of dollars a year from hardworking Americans. One of the biggest challenges is the speed at which these schemes operate. It takes only seconds to steal personal information, drain bank accounts, or even compromise identity verification systems.

So we must give law enforcement the tools to keep up with the pace of these scams and improve the flow of information between victim to agency and across the agency. So my question here in the remaining time is could you explain how Google is using artificial intelligence to improve information sharing in the case of fraud and scams? Specifically, how does this real-time data sharing of the banks and credit card companies stop funds from flowing to these overseas scam rings faster?

Ms. MANFRA. There are two aspects to it. The work that we do internally across all of our various different platforms to stopping phishing scams, fraudulent websites, fraudulent ads, fraudulent reviews, building an ecosystem around Android that I talked about in my testimony. So we have invested a lot in the use of AI and ML to be able to prevent those for those who use Google platforms.

We have also taken those capabilities and working with partners, in particular, in financial services, to be able to do things like using AI for preventing money laundering, and we are seeing huge benefits in that. Fraud detection has been a use case for machine learning for a very long time and continues to grow. So reducing those

false positive rates so that investigators are able to spend their time on useful and productive leads.

Also just being able to—we have one customer, a banking customer, who experienced a fourfold increase in the detection of suspicious activity; at the same time, reducing by 60 percent the volume of false positives. So they are identifying more and having more productive investigations as a result.

Mr. WILLIAMS of Texas. Thank you very much. I yield my time back.

Mr. MEUSER. The gentleman yields.

The gentlewoman from Michigan, Ms. Tlaib, is now recognized for 5 minutes.

Ms. TLAIB. Thank you, Mr. Chair.

You know, one of the things that I continue to hear obviously is all the great things about some of the technology, including AI, but I think we are not realizing the way the corporate America is and is set up is very profit-driven, and the abuse is going to be very clear that everything is going to be around profit first.

No matter how much people are like, It is going to make this easy or that easy, just New York Times publishing article after article about some of the abuses we already see. I am really concerned, of course, on the cost of prices, and the fact that private information is being used to price groceries. Groceries. I am going to walk into a place, and they are going to gather my private information and use that to price it differently than the person that comes right after me. It is discriminatory. It is private data and information. It does not belong in grocery stores.

I know, Mr. Branch, you know about Stop Price Gouging in Groceries Act that I introduced. I would like for you to talk about surveillance pricing. I was with seniors and I was trying to explain to them how surveillance pricing is going to be used in a way not to reduce costs, but actually to be able to price higher on costs because they know where they work, they know what income they have, what they were searching online. So, for folks that are out there right now, can you talk about what that means right now? The use surveillance pricing by some of the big grocers?

Mr. BRANCH. Yes. Thank you for the question, Congresswoman.

In this new age of AI, the power is data driven. The largest companies on earth own all of that data and from a consumer perspective, there is a mismatch there because consumers only see the price that is in front of them, but the large companies have all the information from the consumer.

So Consumer Report actually just came out with a report just the other day that showed that grocery prices based on algorithmic pricing can increase individual consumers' grocery bills by \$1,200 over the course of a year. We are going to find ourselves in a situation where Americans are struggling and struggling to make ends meet, and these companies are arguing that it is just about everything else when, in reality, it is the algorithms that are setting the prices and manipulating them and taking advantage of the data that they have that the consumers are not privy to.

Ms. TLAIB. That is in combined to the digital pricing. You know, explain to folks—so, bye-bye, tags that they have. It is going to be digital. Explain how that is connected.

Mr. BRANCH. Right. So digital pricing can involve the price of certain goods, and those goods can differentiate between different groups of people, oftentimes based off of shopping behavior. So if you happen to like Wheat Thins, for example, Wheat Thins are going to be more expensive for you by maybe a quarter, maybe a nickel, whatever it is. But that little incremental amount—

Ms. TLAIB. Yes.

Mr. BRANCH [continuing]. ends up adding up over the course of the year and over the course of your grocery bill itself.

Ms. TLAIB. Mr. Chair, I ask unanimous consent to enter into the record an article, “Goodbye, Price Tags, Hello, Dynamic Pricing. Shopping has always been a game, and now it is being rigged against you.”

Mr. MEUSER. So ordered.

[The information referred to was not submitted prior to printing.]

Ms. TLAIB. I want to now talk about the discriminatory factors that are going to be at play, because I see this in the auto insurance industry that they already use and collect data—non-driving factors, like your marital status, your education level, your credit score—used toward auto rates right now without the kind of technology, and adding that and compiling that on to decide how much to pay—charge somebody for auto insurance in Michigan. It is mind-boggling that your son’s GPA or your child’s GPA has anything to do with driving, but they are asking for that data as well.

What happens when AI models now—again, using this technology—are trained on historic or contemporary data that reflects past or present discrimination? Does not this risk create models that perpetuate or reinforce discriminatory practices? Because it is teaching it to go around, telling on themselves.

Mr. BRANCH. That is correct, Congresswoman. I mean, the thing that a lot of folks do not necessarily understand about AI is that its goal is to move toward its goal as efficiently as possible. So, that can be replicating discrimination. That can be just trying to get the best price possible for the corporation or for the business at hand. Again, I think that leads back to the fact that a lot of these companies have the data and the power—

Ms. TLAIB. Mr. Branch, I need my colleagues to know this. They are not going in there and saying, how can we make this cheaper for the consumer? They are saying how we can make it cheaper internally so we can—but they are going to charge our residents more, using this technology. We need to face the fact that is exactly what is going to happen. This thing of pretending it is going to make things easier—no, it is not. It is going to charge people more because they are going to know all this private information, know that they need these products and charge them more. Even if it is 10 cents, that is 10 cents too much for our residents. Thank you.

Mr. MEUSER. The gentlelady’s time has expired. I now recognize myself for 5 minutes.

Thank you all very, very much, by the way, for being here. It is a terrific panel and highly informative.

I think you are aware that many of us, the leadership of this committee, as well as the Trump Administration, is committed to unleashing AI’s full potential, so we, indeed, in the United States, wins the AI race with investment and energy dominance to support

the AI infrastructure. My home State of Pennsylvania is doing everything we can to draw in as much AI infrastructure as possible.

However, it brings risks that we are talking about and exposing here, which are happening now and we want to mitigate for the future. They definitely include fraud, scams, profiling, and seem to be growing more sophisticated.

AI is proving to be an incredibly strong tool for detecting and shutting down these very threats, but as well, creating them.

Ms. Manfra, I would like to first start with you. First off, thank you to Google for the good work that—you folks seem to be in the lead of mitigating and finding out scams and addressing them in the—in the manner that they should be, because it is a really serious problem facing all walks of life and our constituents and consumers throughout the United States, on the international level and on the local level. I know I do not have to tell you that.

You recently highlighted the use of AI to uncover a Chinese-linked operation known as Lighthouse which reportedly targeted Americans with E-ZPass, postal service, fraudulent messages, demanding payments to settle fines, and very other common scams that my constituents often encounter. Can you describe how Google—what you did to identify this Lighthouse operation and what role AI detection played in surfacing those scam campaigns?

Ms. MANFRA. Sure. First, let me say that we would be happy if you are interested in further deep dive to follow up. But generally what we do is we have threat intelligence, individuals, and detection capabilities that use advanced technologies, including AI, that are increasingly more finely tuned and able to spot both scale, but also be able to identify networks of organizations that are using our infrastructure and our services. So it is a combination of all of these things coming together to identify this. Then you know, of course, the partnership with law enforcement to ultimately bring this down.

Mr. MEUSER. Well, that is great. Congratulations.

How do you envision and even how is AI playing a role in financial fraud and scam prevention?

Ms. MANFRA. I think AI and ML is—because of—it is a scale, and it has been quite helpful for many years now, and the newer technologies in AI even more so, again, in being able to detect various different networks in addition to being able to be very good at filtering out the signal from the noise, if you will, which is a huge challenge for fraud detection, and also getting very good at being able to reduce the noise around false positives, which organizations spend a lot of time—when they get an alert, they have to go chase that down, go investigate that.

So as our AI and ML capabilities are getting better, they are becoming more targeted. They are reducing that noise that financial organizations have to deal with, and they are better able to deploy their investigators and their teams—

Mr. MEUSER. Be great if that formula could be socialized elsewhere and not be a competitive model within fraud. That would be great for that to serve and help others. But I need to move on. Thank you very much.

Mr. Cohen, Nasdaq has been at the forefront of deploying AI to markets. Last year Nasdaq introduced Dynamic M-ELO, which

stands for, as you well know, Dynamic Midpoint Extended Life Order, designed to ensure the best trade execution for the investor. Can you briefly walk us through it?

Mr. COHEN. Yes. So Dynamic M-ELO employs a delay that—it is almost like a timer that we put on the order so that institutions who are trading large blocks of shares can avoid price impact when they try to execute those shares. So we take in 130 data points to help that institution to identify the ideal time to trade. As a result of that, after they trade, there is no price movement. The result of that is the individual investors that sit behind those large institutions get a better price, get better price execution, and benefit from that order type. We have grown that order type by 50 percent because of the success we have had.

Mr. MEUSER. Well, it sounds terrific. Thank you. My time is expired. I yield back.

Now I want to recognize the gentleman from California, Mr. Liccardo, for 5 minutes.

Mr. LICCARDO. Thank you very much, Mr. Chair. Appreciate the testimony and thank all the witnesses for taking time.

Ms. Manfra, it is good to have somebody from a local neighborhood business, from District 16 here. I should tell Mr. Stevens my wife is probably one of the people who crashed the system when Zestimate came out. She is a big Zillow addict. Ms. Whitmore, I know you employ many of our residents, even though you are just next door. So we appreciate having you all here.

I am brand new here to Congress, but I observed in my 45 or so weeks here that there is essentially a paralysis in Congress about AI. It seems to be borne of a few basic challenges. One is that we generally do not regulate tech very timely or effectively anyway. We have been waiting about 30 years for any kind of regulation or statute governing digital privacy. Folks have been waiting for us to update Section 230 to make social media platforms safer, and we have waited about a quarter century for that.

So that is a basic challenge when we approach AI, to be sure. I think there are a lot of doubts about whether or not Congress is really terribly effective or competent at this. I think many of us are still trying to learn to spell AI. We are still—I think we recognize this technology has moved very quickly; we cannot possibly legislate at the pace of the technology that is changing.

In the absence of this congressional action, we now see 50 States rushing in. I think this year alone, we have had 36 States that have approved more than 100 pieces of legislation governing AI. I appreciate that is mightily difficult for an industry to navigate. Now, the counter or the reaction is we need a moratorium on everything States are doing and that is an understandable reaction. I do not support a moratorium without some kind of sensible Federal regulation to actually supplant it, but I certainly understand or appreciate why industry would need and want it, given the fact that we are an international arena, and certainly China does not have 50 States trying to regulate the industry as we do.

I think—look. As was pointed out, 97 percent of Americans do support some regulation in AI, and that is for good reason. I would like to see how we can move beyond this binary debate that has us stuck between moratorium or no moratorium. I think it is pre-

venting sensible legislation and sensible regulation from moving forward. I wanted to sort of imagine that we took a different approach. I would be interested in any feedback you might offer. The approach we would take would focus on outcomes. I do not think anybody here—I certainly do not know how exactly to regulate algorithms or model weights, and I think outcomes are something we can measure. The good news is we have laws that regulate outcomes. Whether it is discrimination or fraud or anything else, we should be able to do that.

We should be relatively tech neutral when we talk about financial service providers who use AI, just like any other tool. They should be held to the same standards under, for example, Fair Housing Act or anything else that governs whether to use AI or not.

Certainly, large language models (LLMs), we know—since we have one representative from that community—you know, we recognize there are real challenges here in trying to simply get involved in the machines. I do not think most LLM developers are particularly good or will admit—I think they admit that they are not terribly good at explainability of the models. We would not have hallucination if we thought we could transparently eliminate it.

So, perhaps a better approach might be to take away from Congress and have an independent commission of some kind, industry experts, academics, and others who can set, essentially, industry best practices, establish what is the technology, whether it is around security, privacy, a host of other measures, fraud detection, whatever it might be, here is the industry best practices, and if the model meets it, great. You have preemption. You also have a standard of care that you have met and if you do not, then good luck navigating the thicket of 50 different rules.

I guess I will ask—I will start with Ms. Manfra. Do you have any sense about is that something that is viable, in terms of how we can move forward with sensible regulation?

Ms. MANFRA. Yes, sir. Absolutely. Thank you for the question. I think this is already happening. Industry is working together through formal and informal channels at Google, with partners across industry. We have created the Coalition for Secure AI. So committing to research—and this is with Microsoft, with Amazon, with other partners across industry—to drive best practices aligned with what we have learned internally in the development of large language models and others, we have deployed tool kits for our partners and guidance based, again, on what we have learned. I do agree with you is focusing on outcomes is, I think, the priority and——

Mr. MEUSER. Time has expired. That is an important answer. But——

Ms. MANFRA. Sorry.

Mr. MEUSER [continuing]. thank you very much. Gentleman yields back.

Mr. LICCARDO. I yield.

Mr. MEUSER. The gentleman from Georgia, Mr. Loudermilk, is now recognized for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman. I thank everybody for being here.

This is an extremely important discussion we need to be having, and I think it is timely as well.

I spent 30 years in the information technology industry, 20 years in public service in the State legislature and here in Congress. When I was first elected to State legislature in 2005, I was probably one of the few technologists in the State legislature at the time, so I took the lead on a lot of policy initiatives. One thing that I brought up at the time—if you look at the device here, everybody has got one of these, right? The least used part of this, ironically, is what we call it. The phone, right? That is the legacy part of this. I literally talk to people in younger generations than mine that have literally never used the telephone feature of this device. Part of the reason is, it was not the phone that led to the massive technological development that we have seen today. It was the internet and it was broadband. Ironically, those were the least regulated aspects of technology.

If you go back and you look at the massive growth in technological advancements; it was not over the wired network. It was over broadband, the cable television network, which was not heavily regulated as the big cell—or the big carriers were.

So with that in mind, what we have seen from history is government can seriously stifle innovation if it is overly regulated. So, it is kind of a balance that we strike because we do have a need to put guardrails up but to leave this sandbox available for innovation. I think that is where we need to be looking, especially when it comes to tools like AI. There are benefits to that, and there is also reason to be fearful of the misuse of AI.

Ms. Manfra, modernization of the Bank Secrecy Act is an area of great interest to me. I have put a lot of effort into that over the past several years, and especially the significant obligations that the Bank Secrecy Act imposes on financial institutions to monitor and report potential illicit finance activity. It is especially impactful on smaller financial institutions.

Keeping in mind, we have not modernized this thing since the early 1970s when the thresholds of \$10,000 were put in place which, if it had been adjusted, would be \$80,000 today. How do platforms like Google Cloud help financial institutions automate processes for generating currency transaction reports (CTRs) and suspicious activity reports?

Ms. MANFRA. We have a couple of different offerings. Particularly around anti-money laundering tools that we have co-developed with our partners to ensure that they are able—and again, this goes back to the questions around transparency and explainability of the model to ensure that it is getting to the right decisions. But as I mentioned, our customers are seeing huge improvement in detection as well as a reduction in the false positives as well, which has been hugely impactful to actually finding the true risks, the true illicit finance, and being able to more effectively deploy their investigative resources and more successfully report on suspicious activity.

Mr. LOUDERMILK. I think it is really important with suspicious activity reports (SARs) especially because what I hear from a lot

of financial institutions is we just do not want to get dinged by the Federal Government, right? So they may report a SAR that the local bank president may know is not suspicious for that particular customer, but the same action may be suspicious for someone else, but to save the integrity of the bank from any action by regulators, they will report it anyhow.

Can you talk about how Google Cloud's Anti-Money Laundering (AML) AI system uses explainable risk scores and ensures they are auditable for regulators?

Ms. MANFRA. Thank you for the question.

We have invested a lot in explainable AI and so in the end, getting to a point where the customer or auditor or regulator is able to go back and look at how was a decision arrived at so that you can redress of a decision or auditability for the purposes of compliance.

We do offer that and work very closely with our customers, especially in financial services, in particular for AML, but it is used in other areas as well.

Mr. LOUDERMILK. All right. Thank you.

I yield back.

Mr. MEUSER. The gentleman yields.

The gentleman from New York, Mr. Torres, is now recognized for 5 minutes.

Mr. TORRES. Thank you, Mr. Chair.

One of the greatest challenges confronting America is the utility affordability crisis. The proliferation of data centers is one of the drivers—not the only one, but one of the drivers—of rapidly rising electricity costs.

In America, utility rates and returns depend not on efficiency or affordability, not on performance, but on capital spending. The more a utility spends on infrastructure, the more profit it earns and the more customers pay. The electricity cost of new data centers is therefore socialized.

So, given our broken system of utility rate setting in America, how do we ensure that the tech companies, rather than working-class families and small businesses, are the ones shouldering the cost burden of new data centers?

So Mr. Branch?

Mr. BRANCH. Thank you for the question, Congressman.

Public Citizen believes it is critically important to be collaborating with local communities to ensure that they are looped into the process of when these data centers may or may not be built. We argue, and we are seeing it across the country, that a lot of these communities are fighting back against these data centers.

But, just as importantly, we need to ensure that these large tax incentives are not provided to these data centers, because that ultimately ends up being disbursed throughout consumers, and that is why Americans across the U.S. are seeing their electricity bills skyrocketing.

Mr. TORRES. You see, I am pro-AI. My whole life is integrated with ChatGPT and Gemini. So, for me, the question is not whether we should have AI. Of course we should have AI, and we need data centers to enable AI. The question is, who should pay for it, right? Should the cost be borne by working-class families and small busi-

nesses, or should it be borne by the owners and operators of the data centers?

What say you?

Mr. BRANCH. I think these data centers are worth a lot of money, these corporations make a lot of money, and they should be footing that bill responsibly.

Mr. TORRES. There are tens of millions of Americans who have next to no credit history. TransUnion estimates the number at 45 million; FICO, more than 50 million; Experian, more than 60 million.

In the Bronx, I have thousands of constituents who have paid their rent and utilities on time and in full for decades, who maintain steady income and sufficient bank deposits, and yet who remain deprived of a credit score.

Without a credit score you have no access to credit. Without credit, you have no access to home ownership and without home ownership, you have no means of building equity and passing down wealth from one generation to the next. So America's exclusionary model of credit scoring has done irreparable intergenerational damage to working-class communities in places like the Bronx.

Does anyone here have any thoughts on how we can harness the power of AI to build an underwriting system that is more predictive, more inclusive, and more representative of the full financial reality of working-class Americans?

Mr. STEVENS. I will take a stab, Congressman. I really appreciate the question.

Of the 4 million families that are going to buy for the first time this year, most of them are previous renters. At Zillow we are big fans of working with TransUnion, Equifax, and others to consider those on-time rent payments as part of the larger equation.

We believe that AI is that ability to look at disparate sources of information that otherwise a loan officer or underwriter would not have time to consider, and then ultimately leave it to them as humans to make the right decision on what to underwrite.

Mr. TORRES. Because we should harness the power of AI not only to disrupt but to democratize—

Mr. STEVENS. Exactly. Equal access.

Mr. TORRES [continuing]. finance and access to credit is exhibit A.

The Federal Government is drowning in vast oceans of data. For example, in Fiscal Year 2024, FinCEN received a staggering 4.7 million suspicious activity reports, an average of 12,870 a day.

Now, there is no agency in the Federal Government that has sufficient human resources to thoroughly review millions upon millions of reports, and so valuable information can easily disappear into the black box of bureaucracy.

You know, AI can process vast quantities of data that the human mind cannot process. It can recognize patterns that the human mind cannot readily recognize.

Do any of you have thoughts on the role of AI in facilitating not only finance but also financial regulation and oversight?

Mr. COHEN. So Nasdaq employs AI in its surveillance solution, so we are trying to root out market abuse through our surveillance solution, and we use AI to do that.

One great example—and it just keys off of what you said—is, a human investigation analyst combs through many, many possible market manipulations. How do they know which ones to pay attention to? How do they know which ones to let go?

We use AI to help you, number one, do all the manual tasks, the series of tasks that you would otherwise go through to make that analysis, and we provide you with a risk score, so then you can focus on the bigger issues, the most important issues affecting our markets. That is how we use AI.

We always—again, we have the human making the complex judgment decision around that, but we are just reducing the manual workload to get to that decision.

Mr. TORRES. Thank you.

Mr. TIMMONS [presiding]. Thank you.

I now recognize myself for 5 minutes.

Thank you to the witnesses for being with us today.

Like other areas under the Digital Assets jurisdiction, artificial intelligence is a transformative technology that will shape how American companies, consumers, and investors engage with our financial system. If the United States is going to remain a global leader in innovation, we must adopt clear and harmonized rules that support technological progress while also protecting consumers and preserving market integrity.

Industry leaders are increasingly concerned about the growing patchwork of State laws related to artificial intelligence. These State requirements often conflict with one another, whether in the form of impact assessments, documentation standards, or definitions of high-risk systems.

For firms that operate across the country, these inconsistencies can create significant operational challenges, especially when artificial intelligence supports critical functions such as fraud detection and cyber defense.

Without a unified Federal framework that replaces duplicative and contradictory State rules, we risk higher compliance costs, slower innovation, and weaker protection for consumers.

Ms. Manfra, Google Cloud supports financial institutions that rely on artificial intelligence for essential operations. What regulatory obstacles or outdated requirements are hindering firms from deploying artificial intelligence responsibly at scale, particularly when those challenges grow under inconsistent State laws?

Ms. MANFRA. Thank you for the question.

I would say, first of all, it is important to be able to have a national framework that is addressing all of the issues that we have been talking about and not have that patchwork that does pose undue burden and unduly impacts smaller and medium-size players and creates higher barriers to entry that would otherwise be available to them with all this new technology. So I think that is very important.

I also think it is important to recognize that existing laws and frameworks are in place and apply to these new technologies, but to be able to provide spaces for financial institutions to innovate and to test how these tools might be applicable into higher-risk areas is also very important.

Mr. TIMMONS. Thank you for that.

A follow up question. Many State proposals include different documentation and testing requirements for similar artificial intelligence systems. From an operational point of view, how difficult is it for a cloud provider or a financial institution to adjust model governance and controls to comply with several conflicting regimes?

Ms. MANFRA. It is very difficult, and it would be incredibly resource-intensive onto an organization in putting personnel and other resources into positions that are not enabling the core business of that organization.

Mr. TIMMONS. I feel like we have seen this before. We watched Europe pass the General Data Protection Regulation (GDPR), and then now we have the California Consumer Privacy Act (CCPA), and we have all these different data privacy and data security standards. I think everyone agrees that we need to have a Federal standard that preempts everything and leads in the global economy, and we are not learning from past mistakes.

So not only do we need to lead here in Congress on AI, but we also need to get with the program and address the patchwork framework that is costing incredible amounts of money for compliance for businesses. I feel like the larger businesses have a better capacity to deal with the patchwork frameworks for cybersecurity, but in AI it is just going to stifle growth and innovation. We are competing in the global economy, and we cannot lose this fight.

Although there are real challenges in establishing clear rules for artificial intelligence, there are also significant opportunities. AI can strengthen the safety and soundness of our financial system by improving anomaly detection, accelerating the identification of fraud, enhancing cybersecurity, and enabling faster, more accurate risk analysis.

At the same time, compliance expectations continue to rise for institutions of every size. Smaller banks, credit unions, and broker-dealers feel this burden most. AI tools can help reduce manual compliance work, streamline reporting, and allow institutions to devote more time and resources to customer service and innovation.

Mr. Cohen, Nasdaq relies on AI to support its market operations and oversight responsibilities. From your perspective, how is AI helping strengthen the integrity, stability, and resilience of the U.S. financial system?

Mr. COHEN. All markets operate on the mandate of trust and investor confidence. If we compromise either of those, then we will not have the standing we have today in our markets.

So we use our surveillance solution, and we employ AI in it, to essentially allow investigation analysts to scale up, focus on the high-value activities, and also focus on the sophisticated manner in which market abuse is being conducted today.

What we are seeing is, market abuse today, it is the same outcome, but the techniques used are hard for any single human or a series of humans to detect. What used to be, if you will, clear patterns are now noise. To make them and convert them back into signals, we have been using AI to help, if you will, regulators, exchanges, and broker-dealers around the globe protect the integrity of their markets.

Mr. TIMMONS. Thank you for that.

The gentleman from Texas, Mr. Green, is now recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the witnesses for appearing.

I especially thank the chair and the ranking member for allowing me this privilege to ask this question.

I have intelligence indicating that over the next 10 years approximately 100 million jobs will be lost to AI. I know that is a large number. Perhaps you have a number that is somewhat different but let us just assume that this number is accurate.

My question is, how do we provide for 100 million jobs being lost, in terms of how they will impact people? Jobs usually have people associated with them. So how do these people maintain their lifestyles? Will there be some emolument accorded them by way of the Federal Government?

Let us start with you, Mr. Branch, if you do not mind, and we will go to your right and down the line.

Mr. BRANCH. Thank you for the question, Congressman.

If I had the answer to that, I would be a very rich guy, because there is currently not really an answer to this solution, and that is the big problem.

A lot of these tech companies are moving full-fledged forward with this theory of having AI take up a variety of jobs, but there is no solution for when those folks end up being laid off or unemployed.

Mr. GREEN. All right.

Next, please?

Ms. WHITMORE. Thank you, Congressman.

So I work in the field of cybersecurity, and we have historically had a pretty significant job shortage. I think, right now, any estimates would probably be over 1 million jobs within our industry that are not filled and that is due to a lack of skills with that labor shortage.

In that regard, I think we are looking at cybersecurity usage of AI as really being able to put on an exoskeleton for our defenders, making them more capable, being able to conduct tasks that are much more efficient, and defend our networks in a way that we are not able to do at human scale today.

Interestingly, in the field of cybersecurity, I think we are actually providing a lot more job satisfaction to our industry analysts and defenders, who primarily deal in very repetitive tasks.

Mr. GREEN. Well, I appreciate your answer, but, if I may, I am posing a different question. You have answered a question associated with how well and how efficacious your business model is. My question has to do with the people who are displaced. How will they make a living?

Ms. WHITMORE. I think that is a great question, but as a cybersecurity expert, I am not sure that I am in the best position to answer that, so I may turn it to Mr. Stevens.

Mr. GREEN. All right.

Mr. STEVENS. Thank you, Congressman. I will talk briefly about how important humans are to housing and then also offer how we can improve building the next-generation U.S. workforce.

In housing, ultimately, where people are going to live is a very human-based decision. We find time and time again; people want a real estate agent to sit across the table and give them advice on if they are making a good decision. So, in housing, we continue to see humans being very important.

Outside of that, I think something that has come up briefly is, we really need to invest more in training the next generation here at home to work on these models and help really improve them over time. And that is——

Mr. GREEN. Excuse me, if I may.

Mr. STEVENS. Of course.

Mr. GREEN. A hundred million people, 100 million jobs—100 million.

Mr. STEVENS. I have not seen that stat, but I certainly believe, if we gave equal access——

Mr. GREEN. Okay.

Mr. STEVENS [continuing]. of this technology, that——

Mr. GREEN. Okay. Thank you. I think that your model is a good one, but we are talking about 100 million.

Mr. STEVENS. Yep.

Mr. GREEN. Yes, sir?

Mr. COHEN. It is a great question. The first thing that we have to do is be honest about the workforce transition that we are going to go through as a country.

What we are doing in terms of our part is, we are trying to make sure that we upskill/reskill employees and we are actually creating roles of the future. So we are trying to do our part to make sure that our workforce comes with us into the next generation.

Then you also have to believe in the power of AI to generate new business models, new opportunities and that is why it is important that we capture them here so that we can make sure that those individuals that——

Mr. GREEN. Okay.

Mr. COHEN [continuing]. may be displaced have opportunities in the future.

Mr. GREEN. I have to go to the last speaker.

Please, ma'am.

Ms. MANFRA. Thank you, sir. It is a very important topic and one that we care a lot about.

Similar to our colleagues, we are very invested in ensuring our own workforce has the tools to be able to be successful. This includes our engineers using AI to be more productive.

I would say more broadly is that we are seeing more job creation, we are seeing businesses grow as a result. It is important that we invest in education at the lowest levels of—into elementary school to make sure our kids are——

Mr. GREEN. The chairperson is admonishing me.

Let me thank you, Mr. Chairman, and simply indicate that this is a question that we have to give some serious consideration to.

Mr. TIMMONS. The gentleman's——

Mr. GREEN. A hundred million jobs.

Mr. TIMMONS [continuing]. time has expired.

Mr. GREEN. I thank you, Mr. Chairman. I yield back.

Mr. TIMMONS. The gentlewoman from California, Mrs. Kim, is now recognized for 5 minutes.

Mrs. KIM. Thank you, Chairman and Ranking Member, for convening our hearing today.

Earlier this year, the State of California, where I am from, passed SB 54 that would unfairly regulate AI and impose heavy compliance burdens on companies. Now States across the country are looking to this California model as a basis for developing their own artificial intelligence regulations.

Therefore, there is an urgency for Congress to establish a Federal framework for AI. That is why I support legislation like Chairman French Hill's Unleashing AI Innovation in Financial Services Act that would create Federal regulatory sandboxes.

Ms. Manfra, if that bill is signed into law, will those Federal protections be respected if you are simultaneously fighting a patchwork of restrictive State laws, particularly the anti-innovative regulatory framework in my home State of California?

Ms. MANFRA. Thank you for the question, ma'am.

Yes, we absolutely think the need for a national framework is critical and having to navigate a patchwork of regulations does not help either our company or our customers.

Mrs. KIM. Thank you.

What has made America a leader compared to other countries is our philosophy of trying first, rather than regulation first. So the longer we fail to act, the regulatory standard will be set at the State level, not—and the innovation will suffer.

So thank you.

Another area where AI has high value is in its application in the field of cybersecurity.

So I want to ask you, Ms. Whitmore: By leveraging AI, how have banks been able to save time and protect themselves through cybersecurity efforts?

Ms. WHITMORE. Thank you for the question.

So I think one of the most measurable areas we see with financial institutions is actually the applications to cybersecurity and, in particular, measuring outcomes in how quickly we detect attacks and how quickly we respond to them.

As we have seen the use of AI increase, we have seen ransomware attacks that have been completed from initial part of the attack to stolen data or encryption of data in 25 minutes. We have worked with customers in the financial services industry who have taken a mean time to detect from 24 hours to as little as 10 minutes.

So those types of measurable outcomes are incredibly critical in our ability to defend financial services networks.

Mrs. KIM. Thank you.

You know, scams are an issue that I hear constantly about from my constituents. We know that modern financial scams are rarely isolated to a single app. They may start with a text on a phone, move to a fraudulent website, and follow up with an email.

Ms. Manfra, let me come back to you. How does Google connect the technical dots in the background to prevent those foreign scammers?

Ms. MANFRA. Thank you.

We have invested a lot in this space and seen a lot of very positive results going to the ability to identify a fourfold increase in activity that we are then able to detect and take down on a variety of our platforms.

We do not want fraudulent or scam information that is sitting on our platforms or that is impacting our customers. So, every day, we are identifying millions and taking down millions of fraudulent ads, preventing scams, preventing phishing through the use of AI and ML technologies.

Mrs. KIM. So let us say, if AI detects a threat in Gmail, how does that transfer across Android or Chrome to ensure that it is neutralized across a person's accounts?

Ms. MANFRA. Well, in some cases we use common tools, and many of our platforms and tools reside on common infrastructure, so oftentimes we are able to leverage that scale to be able to identify commonality.

In other cases, we do have to use unique tools, but we are sharing the outcomes, the detections, the things that we are finding, to make sure that other products and platforms are available to use that.

Mrs. KIM. Uh-huh. Well, thanks for your work on that.

Let me quickly shift gears to AI. It has a large role to play in preventing financial crime as well.

So, Mr. Cohen, I want to give you a chance to answer. How does Nasdaq utilize AI to address compliance and prevent financial crime?

Mr. COHEN. So we were saying earlier that we have a leading financial crime platform. It is cloud-native, AI-enabled and what we do is use consortium data to detect patterns that no single institution can do on its own. We have 725 million accounts.

What we are able to do is reduce false positives and help investigators focus on real crime and identify real crime——

Mr. TIMMONS. The gentlelady's——

Mr. COHEN [continuing]. that is otherwise a drain on——

Mr. TIMMONS. The gentlelady's time has expired. Sorry.

I now recognize the gentleman from New Jersey——

Mrs. KIM. Thank you.

Mr. TIMMONS [continuing]. Mr. Gottheimer, for 5 minutes.

Mr. GOTTHEIMER. Thank you, Mr. Chairman.

AI is being used, as we all know, to detect fraud and stop seniors from getting manipulated, those especially who are targeted by scams involving deepfakes and other AI-powered tools.

According to the Federal Trade Commission (FTC) report released just last week, adults over 60 lost \$2.4 billion to scams and fraud in 2024. Alarming, this is the same report that found that older adults who reported losing more than \$100,000 increased more than five-fold between 2020 and 2024.

I am very grateful to Chairman Hill and the Capital Markets Subcommittee chairwoman, Ann Wagner, for recognizing the importance of my Senior Security Act and including it in the INVEST Act, which the House will vote on this week, to put a new senior-protection-focused cop on the beat at the SEC.

Ms. Whitmore and Mr. Cohen, what specific safeguards should be considered to prevent and detect elder financial fraud and abuse

related to AI and how should industry coordinate with Congress and regulators and law enforcement and others to ensure those protections keep pace with rapidly evolving AI-enabled threats?

Ms. WHITMORE. Thank you, sir, for the question.

So I think specific to the demographic you are talking about, education is a huge concern and really an issue. If we can raise awareness that these scams are being conducted and can create a level of education that does not necessarily exist that widespread today, I think that really helps with that.

Additionally, what we are also talking about is visibility at large scale to protect the transactions on the back end and that is where organizations like ours truly focus, is looking at the packets that are moving. So, in your specific use case, we will be looking at the financial services transactions and ensuring that our detection capabilities are not facilitating those types of crime.

Mr. GOTTHEIMER. Mr. Cohen.

Mr. COHEN. Thank you.

There are two important elements here.

There is the public-private partnership. We need information-sharing, because these scams scale incredibly fast in the world that we live in today. It should not be that the elderly find out on Facebook from their friends about a scam. We should have this information-sharing at a scaled level to make sure that we can prevent it and not just deal with it after the fact.

The second thing is, we can use AI to detect it at scale. Right now, what we are doing is, we are coming into it, and we are trying to deal with it on a one-off basis. We need the tools and the automation to be able to stop it the second we see it and not let it propagate through the system, and AI can help us do that.

Mr. GOTTHEIMER. Are we seeing that?

Ms. Manfra, are you taking steps to actually make sure that happens, from a Google perspective?

Ms. MANFRA. Absolutely. We are identifying, blocking, and taking down fraudulent use of our platform—fraudulent postings, fraudulent ads, scams that are targeting various customers, phishing attempts. Gmail alone blocks 180 million phishing attempts every day and so we are investing in AI as a critical component to being able to do that.

Mr. GOTTHEIMER. Thank you very much.

Regulators have used innovation hubs and sandboxes to encourage responsible experimentation in other areas of fintech. I am personally very focused on this area.

For the entire panel, what features and guardrails do you think are essential for AI pilots to truly encourage innovation and protect consumers and communities in this space?

Josh, do you want to start?

Mr. BRANCH. Thank you for the question, Congressman.

Well, I think these sandboxes need to be time-limited; they need to be specific, and I think those are two of the primary, sort of, components that are at least not seen currently in the sandbox offerings.

Mr. GOTTHEIMER. Ms. Whitmore.

Ms. WHITMORE. Thank you.

So I think we look at it from three categories.

First is defining a risk-based approach with consistent definitions. The focus is on actual threats and not necessarily those that are hypothetical and those, certainly, that are more high-risk applications.

Second would be distinguishing between the developers and the deployers.

Third is making sure that defense is a priority, so having a voluntary standards, a framework that then looks at making sure we are protecting our most critical information and not getting it in the hands of our adversaries.

Mr. GOTTHEIMER. Thanks.

Nick.

Mr. STEVENS. Thank you.

I would say briefly that laws stay enforced, that we test responsibility in these sandboxes. Independence checks still happen, bias testing and the like. Last, I would add, transparency is obviously paramount.

Mr. GOTTHEIMER. Yes.

Mr. STEVENS. Regulatory reviews, consistent—

Mr. GOTTHEIMER. Tal, you agree?

Mr. COHEN. Controlled, targeted, and time-boxed, and do not allow for circumvention of approval process.

Mr. GOTTHEIMER. Jeanette.

Ms. MANFRA. I agree with Mr. Cohen and the previous statements.

Mr. GOTTHEIMER. Great.

Thanks so much.

I yield back.

Mr. TIMMONS. The gentleman from York, Mr. Garbarino, is now recognized for 5 minutes.

Mr. GARBARINO. Thank you, Chairman.

Thank you all for being here today.

As chairman of the House Committee on Homeland Security, one of my top priorities is reauthorization of the Cybersecurity Information Sharing Act of 2015, also known as CISA 2015. It is a vital framework that allows for voluntary exchange of cybersecurity information between the Federal Government and private entities.

From energy companies to major financial institutions on Wall Street, the private sector's first line of defense against malicious cyber adversaries in CISA 2015 is critical to ensuring those threats are not realized.

Ms. Manfra, as someone who previously served as Assistant Secretary for Cybersecurity at CISA, how important is the reauthorization of CISA 2015 to ensure our cybersecurity needs are met to combat AI-powered threats?

Ms. MANFRA. It is very important, sir.

Mr. GARBARINO. Can you give me some examples of what could happen in the financial services space if CISA 2015 authorization were to lapse—like it did under the shutdown, but it would lapse for a longer time?

Ms. MANFRA. The framework that the legislation provides CISA to be able to share information in protected spaces with its partners, to include financial services, means that they are actively reducing risks in those protected conversations and information-shar-

ing environments and so not having that is detrimental to those partnerships.

Mr. GARBARINO. Yes. I mean, financial services companies are hit all the time with cyber-attacks. They learn about vulnerabilities before—because they are the front line of defense. They cannot share that information with the Federal Government. The Federal Government cannot then share it with everybody else. Which means those vulnerabilities cannot be fixed and we are just facing more and more threats, correct?

Ms. MANFRA. Correct.

Mr. GARBARINO. Thank you.

Ms. Whitmore, is our existing financial data privacy and cybersecurity framework well-suited for the current era of AI, or are reforms needed?

Ms. WHITMORE. I think we can leverage existing regulation, but what we are really advocating for, moving forward, are actions that benefit the defenders and not the attackers.

So the more that we look at streamlining regulation and harmonizing it, the better we make it for defenders to really focus on truly firefighting and not filing the complexities of too much paperwork.

Mr. GARBARINO. Yes, harmonization. I had lunch with Jamie Dimon once, and he said more than 50 percent of—his cybersecurity employees spent more than 50 percent of their time on compliance instead of actual cybersecurity defense, which is wild to me.

Ms. WHITMORE. Yes.

Mr. GARBARINO. So harmonization is another thing that I know I have spoken to Chairman Hill about as something we should focus on here as well.

Switching gears a bit, the mortgage industry has spent decades under Federal oversight, starting with the Great Depression, when agencies like the Federal Housing Administration (FHA) and Fannie Mae were created to stabilize the housing market and expand access to home ownership, and intensifying again after the 2008 financial crisis through the Dodd-Frank Act and then the creation of the CFPB. Today, Federal rules shape nearly every part of the mortgage process.

Mr. Stevens, as AI enters mortgage lending, should we extend existing Federal financial services regulatory frameworks to cover AI?

Mr. STEVENS. Definitely. Any law or regulation that humans have to follow, AI definitely should too.

I think, to the first part of your question, AI has that ability to take on a lot of the administrative burden that slows everyone else down. If you shadow a loan officer, they spend hours just collecting documents, copying and pasting data. AI can do that so they can focus on the right decisions.

Mr. GARBARINO. Absolutely.

So what should Congress do to ensure—or maybe not do—to ensure that you can continue to innovate here?

Mr. STEVENS. I think national right-sized frameworks. I mean, we rely a lot on the risk AI management framework, and so anything that has a consistent baseline for all of our States will help us.

Mr. GARBARINO. Are there any—and maybe it is the States but are there any regulatory structures that are currently standing in the way of AI delivering on the promise to expand access to affordable housing?

Mr. STEVENS. It is something we could certainly follow up on.

I think, in housing, a lot of the regulations were written before the age of the internet. For example, we have a whole database at Zillow that is just mindful of when e-sign is allowed depending on the State you are in. So I would say a comprehensive review of some of those older frameworks would be useful.

Mr. GARBARINO. Yes. If you could get us more ideas, that would be—

Mr. STEVENS. Yep. Would love to follow up.

Mr. GARBARINO [continuing]. more details, that would be great.

From your vantage point, Mr. Stevens—last question—building consumer products, how can technology and modernization, not more regulation, actually help lower the costs for buyers and renters?

Mr. STEVENS. Yes. Both the efficiency, we were talking about, with loan officers and real estate agents. I would say also, the democratic—democratization of data access.

If you have a nationwide framework, that means we can give guidance about what home to buy across State lines, which many consumers consider all the time.

Mr. GARBARINO. Uh-huh.

Mr. STEVENS. If it is a patchwork, that means we have to build very custom models depending on the State you are looking in right now and that kind of efficiency helps people make better decisions at the right price.

Mr. GARBARINO. Thank you very much.

I am out of time. I yield back.

Mr. TIMMONS. Thank you.

The gentleman from Nebraska, Mr. Flood, is now recognized for 5 minutes.

Mr. FLOOD. Thank you, Mr. Chairman.

I really think about AI in, really, two buckets: Number one, as it relates to entities that are already regulated in the financial services lane, whether it be by the Fair Housing Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, or statutes that apply to financial actors.

Basically what I tell people is, if we find you discriminating, we will fine you, and we will enforce the law. In other words, if you are using AI to break consumer protection law or discrimination law, we need to ensure that our regulators are equipped to track and identify that.

I have this idea that someday we are going to begin an enforcement action, and the regulated entity will say, “Well, we did not intend to do that. It was all in our AI model, and this is the outcome.” Well, we are not going to fall for that. Like, if you break the law, you broke the law, and you had a model that did it.

Number two, we need to work together to identify these bad actors, these folks that use generative AI to scam people out of money, to let fraudsters fool people and steal their cash, and law enforcement needs to be able to respond to these threats. We abso-

lutely need the help of technology companies in preventing AI from being used by those who do it to lie, cheat, and steal.

That is really where I come from on this.

To all of you on the panel today, can you just describe the intentions with the—the interactions, I should say, with the regulators you work with on AI, both at the Federal and the State level? Do you see in those regulators sufficient expertise in your counterparts in government to make you feel they are up to the task of overseeing this changing landscape? In other words, as you engage with regulators, do you feel like they have the tools they need to do the job, given the changed landscape with artificial intelligence?

We will start here.

Ms. MANFRA. We will say, those that we interact with, whether as customers or partners or regulators, I do think that they show a willingness and an openness to learn. I do think that, like many other organizations, they do need more skilling in this space to be able to best focus on the outcomes but also be able to apply that to new technology.

Mr. FLOOD. Mr. Cohen.

Mr. COHEN. Just to frame your question, public-private partnerships are incredibly important, and they are what will keep us ahead.

Two things, if I could take the opportunity. The Cybersecurity Information Act that needs to be extended so that we continue that on the cybersecurity side.

In terms of the regulators and the way that we work together, we do feel like they appreciate the issues; there is a deep level of understanding around the issues. The one thing we worry about is regulatory arbitrage. So you need to make sure that, as we go to the regulators, we do not want to go to the regulators that understand the least to try to get something approved.

That is why at a Federal level we are going to need some clarity there, so there are no regulatory arbitrage and people do not try to go to the regulator that understands the least.

Mr. FLOOD. Well-said.

Mr. STEVENS. Thank you. I appreciate the question.

I would say, certainly education could help when we partner at the Federal and State level but even more so, we see successful partnerships when they are outcome-focused, when they are customer-first, when they are transparent.

I could sit down and explain all the fraud models behind Zillow Rentals, but if we just agree that no customer should see a fraudulent listing or have a fraudulent payment, then we can collaborate even more efficiently.

Ms. WHITMORE. Thank you for the question.

So not only do we work on behalf of public-private partners within cybersecurity and all our counterparts on the government side, but also on behalf of our customers when we are investigating these major cyber breaches. They are then challenged so many times with the different regulatory frameworks that they need to report these breaches in.

I think the one area I would really like to share there is that more complexity never benefits the defenders who are trying to fight the fire and stop the breach while they are also worried about

the paperwork. So that really benefits the attackers. I think the more we can streamline, the better off we are going to be.

Mr. FLOOD. Mr. Branch.

Mr. BRANCH. Thank you, Congressman, for the question.

Many agencies have lost jobs due to various layoffs, and so these agencies are playing catchup and are in a bit of a difficult position to try to enforce some of the laws but, also, President Trump's AI action plan has predominantly been a deregulatory effort. As such, the agencies are not really empowered to enforce some of the laws that exist.

The last thing that I would say, as well, is that some of the sandbox bills that have been proposed allow the companies to sort of self-regulate. So, from that end of things, these companies are sort of guarding their own laws, and it is not allowing the regulators to essentially do the jobs that they are required to do.

Mr. FLOOD. Thank you very much.

With that, I yield back.

Mr. TIMMONS. Pursuant to the previous order, the chair declares the committee in recess, subject to the call of the chair. We will reconvene immediately after the floor vote series.

The committee stands in recess.

[Recess.]

Mr. FITZGERALD [presiding]. The Committee on Financial Services will come to order.

I would like to thank all the witnesses for their testimony today.

Without objection, all members will have 5 legislative days to submit additional written questions for the witnesses to the chair. The questions will be forwarded to the witnesses for their response.

Witnesses, please respond no later than January 14, 2026.

[The information referred to can be found in the appendix.]

Mr. FITZGERALD. The hearing is adjourned.

[Whereupon, at 2:38 p.m., the committee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD



CONTENTS

Introduction	3
The Regulatory Sandbox Approach	3
Purpose of the Guidelines	4
Target Audience	4
Objective and Principles of the Sandbox	4
Sandbox Evaluation Criteria	5
Extending or Exiting the Sandbox	6
Application and Approval Process	7
Annex A: Examples of Flexibility around Regulatory Requirements and Expectations for the Sandbox	10
Annex B: Application Template for the FinTech Regulatory Sandbox	12
Annex C: An Example of a Sandbox Application	18

1. INTRODUCTION

- 1.1. Singapore aims to grow a smart financial centre where innovation is pervasive and technology is used widely to enhance value, increase efficiency, manage risks better, create new opportunities and improve the lives of Singaporeans.
- 1.2. The Monetary Authority of Singapore (“MAS”) believes that a key driver to transforming Singapore into a smart financial centre is the provision of a regulatory environment that is conducive for innovative use of technology.
- 1.3. Currently, financial institutions (“FIs”) are already free to launch new financial products, services or processes (the “financial services”) without first seeking MAS’ permission, as long as they have carried out their due diligence and there is no breach of legal and regulatory requirements.
- 1.4. In this regard, FIs have been experimenting with new financial services in a production environment¹ such as by limiting the experimentation to specific type of customers or setting a threshold on transaction values.
- 1.5. However, against the backdrop of a rapidly evolving financial technology (“FinTech”) landscape, emerging financial services that utilise FinTech are becoming more sophisticated and there may be uncertainty over whether the innovation meets regulatory requirements.
- 1.6. Furthermore, the vibrancy of our FinTech ecosystem has been accentuated by a growing number of start-ups. These start-ups are keen to implement innovative financial services utilising FinTech but are looking for an approach to enable them to test the viability of these financial services in a cost effective and timely manner.
- 1.7. In circumstances where it is less clear whether a new financial service complies with legal and regulatory requirements, some FIs or start-ups may err on the side of caution and choose not to implement it. This outcome is undesirable as promising innovations may be stifled and this may result in missed opportunities.

2. THE REGULATORY SANDBOX APPROACH

- 2.1. MAS is encouraging more FinTech experimentation so that promising innovations can be tested in the market and have a chance for wider adoption, in Singapore and abroad.

¹ A production environment is where actual products or services are rendered to customers.

- 2.2. To achieve this objective, FIs or any interested firm (the “applicant”) can apply to enter a regulatory sandbox (the “sandbox”) to experiment with innovative financial services in the production environment but within a well-defined space and duration. The sandbox shall include appropriate safeguards to contain the consequences of failure and maintain the overall safety and soundness of the financial system.
- 2.3. Depending on the financial service to be experimented, the applicant involved and the application made, MAS will determine the specific legal and regulatory requirements which it is prepared to relax for each case. Please refer to **ANNEX A** for examples of the legal and regulatory requirements that MAS may consider relaxing for the duration of the sandbox, as well as those which MAS intends to maintain.
- 2.4. Upon approval, the applicant becomes the entity responsible for deploying and operating the sandbox (the “sandbox entity”), with MAS providing the appropriate regulatory support by relaxing specific legal and regulatory requirements prescribed by MAS, which the sandbox entity will otherwise be subject to, for the duration of the sandbox.
- 2.5. Upon successful experimentation and on exiting the sandbox, the sandbox entity must fully comply with the relevant legal and regulatory requirements.

3. PURPOSE OF THE GUIDELINES

- 3.1. The FinTech regulatory sandbox guidelines (the “guidelines”) set out the objective and principles of the sandbox, and provide guidance to the applicant on the application process and the information to be furnished to MAS.

4. TARGET AUDIENCE

- 4.1. The guidelines will be of particular interest to firms that are looking to apply technology in an innovative way to provide financial services that are or likely to be regulated by MAS. The target audience includes but is not limited to FIs, FinTech firms, and professional services firms partnering with or providing support to such businesses.

5. OBJECTIVE AND PRINCIPLES OF THE SANDBOX

- 5.1. This section outlines the objective and principles of the sandbox, and provides the target audience with the rationale for deploying a sandbox.
- 5.2. MAS aims to transform Singapore into a smart financial centre by encouraging the adoption of innovative and safe technology in the financial sector. To this end, the sandbox can help to encourage more FinTech experimentation within a well-defined space and duration where MAS will provide the requisite regulatory support, so as to:

- a. increase efficiency;
 - b. manage risks better;
 - c. create new opportunities; or
 - d. improve people's lives.
- 5.3. Given that a sandbox operates in the production environment, it must have a well-defined space and duration for the proposed financial service to be launched, within which the consequences of failure can be contained.
- 5.4. The applicant should clearly understand the objective and principles of the sandbox. It must be emphasised that the sandbox is not intended and cannot be used as a means to circumvent legal and regulatory requirements.
- 5.5. In addition, the sandbox may not be suitable under the following circumstances:
- a. The proposed financial service is similar to those that are already being offered in Singapore, unless the applicant can show that either:
 - (i) a different technology is being applied; or
 - (ii) the same technology is being applied differently.
 - b. The applicant has not demonstrated that it has done its due diligence, including testing the proposed financial service in a laboratory environment and knowing the legal and regulatory requirements for deploying the proposed financial service.

6. SANDBOX EVALUATION CRITERIA

- 6.1. This section outlines the main evaluation criteria which will be used by MAS to assess the application submitted by the applicant.
- 6.2. The application should contain the necessary supporting information (**ANNEX B**) to depict how the sandbox evaluation criteria listed below can be fulfilled:
- a. The proposed financial service includes new or emerging technology, or uses existing technology in an innovative way. For example, secondary research should show that few or no comparable offerings are available in the Singapore market;
 - b. The proposed financial service addresses a problem, or brings benefits to consumers or the industry. For example, these could be supported by evidence from relevant consumer or industry research;

- c. The applicant has the intention and ability to deploy the proposed financial service in Singapore on a broader scale after exiting the sandbox. If there are exceptional reasons why the proposed financial service cannot be deployed in Singapore, for example it is not commercially viable to deploy in Singapore, the applicant should be prepared to continue contributing to Singapore in other ways, such as continuing the developmental efforts of the proposed financial service in Singapore;
- d. The test scenarios and expected outcomes of the sandbox experimentation should be clearly defined, and the sandbox entity should report to MAS on the test progress based on an agreed schedule;
- e. The appropriate boundary conditions should be clearly defined, for the sandbox to be meaningfully executed while sufficiently protecting the interests of consumers and maintaining the safety and soundness of the industry;
- f. Significant risks arising from the proposed financial service should be assessed and mitigated. For example, providing evidence of preliminary testing of the proposed financial service as part of the sandbox application, identifying the risks discovered from the preliminary testing and the proposal for mitigating the risks; and
- g. An acceptable exit and transition strategy should be clearly defined in the event that the proposed financial service has to be discontinued, or can proceed to be deployed on a broader scale after exiting the sandbox.

7. EXTENDING OR EXITING THE SANDBOX

- 7.1. At the end of the sandbox period, the legal and regulatory requirements relaxed by MAS will expire, and the sandbox entity must exit from the sandbox.
- 7.2. In the event that the sandbox entity requires an extension of the sandbox period, the sandbox entity should apply to MAS at least **1 month** before the expiration of the sandbox period and provide reasons to support the application for extension. For example, additional time is needed to make changes to the financial service under experimentation after taking into account customer feedback or to rectify flaws, or the sandbox entity requires more time in order to fully comply with the relevant legal and regulatory requirements. MAS will review the application and approval will be granted on a case-by-case basis. MAS' decision on the application for extension is final.
- 7.3. Upon exiting, the sandbox entity can proceed to deploy the financial service under experimentation on a broader scale, provided that:
 - a. both MAS and the sandbox entity are satisfied that the sandbox has achieved its intended test outcomes; and

- b. the sandbox entity can fully comply with the relevant legal and regulatory requirements.

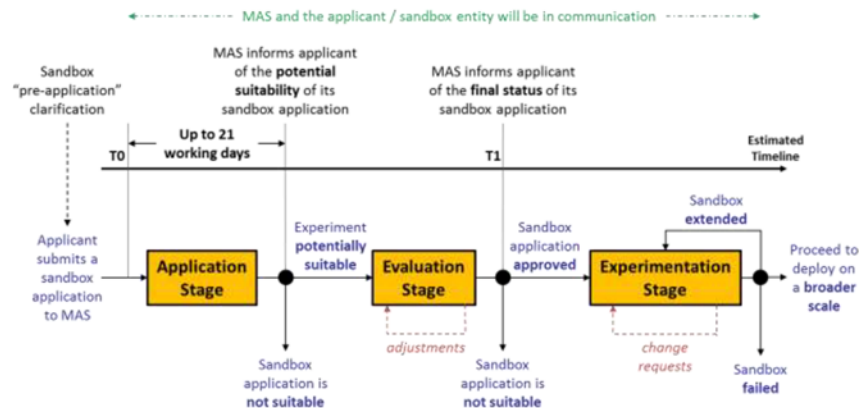
7.4. The sandbox will be discontinued when:

- a. MAS is not satisfied that the sandbox has achieved its intended purpose, based on the latest test scenarios, expected outcomes and schedule mutually agreed with the sandbox entity;
- b. the sandbox entity is unable to fully comply with the relevant legal and regulatory requirements at the end of the sandbox period. If such a situation is anticipated, the sandbox entity is encouraged to engage MAS earlier;
- c. a flaw has been discovered in the financial service under experimentation where the risks posed to customers or the financial system outweigh the benefits of the financial service under experimentation, and the sandbox entity acknowledges that the flaw cannot be resolved within the duration of the sandbox;
- d. MAS terminates the sandbox due to reasons such as the sandbox entity breaching any condition imposed for the duration of the sandbox; or
- e. the sandbox entity has informed MAS of its decision to exit the sandbox at its own discretion.

7.5. The sandbox entity should ensure that any existing obligation to its customers of the financial service under experimentation must be fully fulfilled or addressed before exiting the sandbox or discontinuing the sandbox.

8. APPLICATION AND APPROVAL PROCESS

- 8.1. The applicant should ensure that the objective, principles and criteria specified under **Section 5** and **Section 6** are satisfied before submitting the application and **ANNEX B** to the MAS Review Officer if the applicant is an MAS regulated FI or to FinTech_Sandbox@mas.gov.sg.
- 8.2. The following diagram depicts the application and approval process. MAS will communicate with the applicant / sandbox entity in the course of evaluating the sandbox application, and continue to do so during experimentation:



- Prior to submitting an application, the applicant can and should clarify any question regarding the sandbox by contacting MAS at FinTech_Sandbox@mas.gov.sg.
- At the “**Application Stage**”, MAS shall review the application and endeavour to inform the applicant of its potential suitability for a sandbox within **21 working days** after MAS receives a complete set of information necessary for the assessment (T0). The preliminary indication serves to help the applicant with its business and resource planning.
- At the “**Evaluation Stage**”, the time required to fully assess the application (T1) is dependent on its completeness and complexity, and the specific legal and regulatory requirements involved. Due to the exploratory nature of the sandbox approach, the applicant is allowed to make adjustments to the application for resubmission (for example, refining the boundary conditions) after discussing with MAS. The applicant will be informed in writing whether to proceed with the sandbox.
- The applicant will be informed if the application is rejected. The reasons for rejection could include failure to meet the objective and principles of the sandbox or any of the evaluation criteria. The applicant may re-apply for the sandbox when it is ready to meet the objective, principles and evaluation criteria of the sandbox.
- Upon approval of the application, the sandbox is launched into the “**Experimentation Stage**”, and **Section 7** shall apply. The sandbox entity shall notify its customers that the financial service is operating in a sandbox and disclose the key risks associated with the financial service. The sandbox entity is also required to obtain the customers’ acknowledgement that they have read and understood these risks.

- f. In the event that the sandbox entity intends to make material changes to the financial service under experimentation during the “**Experimentation Stage**”, the sandbox entity should apply to MAS at least **1 month** in advance and provide details of the changes with reasons (the “change requests”). The sandbox entity can continue experimenting with the existing solution while MAS reviews the change requests and inform the sandbox entity of its decision.
 - g. For the purpose of transparency and provision of information to customers, relevant information of all approved sandbox applications such as the name of the applicant, and the start and expiry dates of the sandbox experimentation, will be published on MAS’ website.
- 8.3. To illustrate the application and approval process, **ANNEX C** provides a case study on how an application that meets MAS’ expectations is processed, which will allow for a sandbox to be implemented.

ANNEX A**EXAMPLES OF FLEXIBILITY AROUND REGULATORY REQUIREMENTS AND EXPECTATIONS FOR THE SANDBOX**

The following table provides examples of the legal and regulatory requirements that MAS is prepared to consider relaxing for the duration of the sandbox, as well as those which MAS intends to maintain. It must be emphasised that the examples outlined in the table are not exhaustive. Depending on the proposed financial service, the applicant involved and the application made, MAS will determine the specific legal and regulatory requirements which it is prepared to relax for each case.

Examples of "To Maintain" requirements
Confidentiality of customer information
Fit and proper criteria particularly on honesty and integrity
Handling of customer's moneys and assets by intermediaries
Prevention of money laundering and countering the financing of terrorism

Examples of "Possible to Relax" requirements
Asset maintenance requirement
Board composition
Cash balances
Credit rating
Financial soundness
Fund solvency and capital adequacy
Licence fees
Management experience
MAS Guidelines, such as technology risk management guidelines and outsourcing guidelines
Minimum liquid assets

Minimum paid-up capital
Relative size
Reputation
Track record

ANNEX B
(Updated on 19 February 2018)

MAS FINTECH REGULATORY SANDBOX APPLICATION FORM

Organisation (Applicant)	
Address	
Telephone	
Country of Incorporation	
Principal Place of Business	

Contact Person	
Designation	
Email	
Telephone	
Signature	
Date	

Note:

1. Please note that the regulatory sandbox is meant to enable experimentation of innovative financial services/products that are regulated by MAS.
2. Before submitting an application, you may write to FinTech_Sandbox@mas.gov.sg to seek specific clarifications.
3. Please refer to **Section A** for the application details required, and submit the completed application using the template in **Section B**.
4. The completeness and clarity of the information provided in the application will determine the time taken for MAS to review your sandbox application.

Section A: Details Required for the Sandbox Application

1. Please provide full details of your organisation, covering the following areas:
 - a. Profile of the organisation, including the organisation structure, past achievements and business profile with ACRA¹ and/or other regulatory bodies of business entities;
 - b. Profile of key personnel, including relevant domain knowledge and experience;
 - c. Financial standing, including any funding raised and/or to be raised; and
 - d. Authorised regulatory status (e.g. licensing, registration, notification, approval, recognition) under MAS² and/or other regulators.

2. Please provide full details of the proposed financial service/product to be experimented in the sandbox, covering the following areas:
 - a. Problem statements that the proposed financial service/product aims to address;
 - b. Benefits of the proposed financial service/product, in particular, those that may not exist today;
 - c. Business model(s), including the target customers and specific use cases. For each use case, provide an end-to-end illustration on how the proposed financial service/product will be made available, including:
 - i. The interactions and money flows between you, your target customers and your business partners (if any);
 - ii. The entity that will be holding your customers' monies; and
 - iii. The remuneration structure.
 - d. Technical architecture and solution, detailing the specific technology and innovative ways in which the technology will be applied;

¹ Accounting and Corporate Regulatory Authority.

² MAS regulations, guidance and licensing: <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing.aspx>

- e. Comparison with existing offerings (including in Singapore) that are similar to the proposed financial service/product, focusing on the problem statements, benefits, technology and business model; and
 - f. The readiness of the prototype development, including an estimated timeframe on the readiness to provide an end-to-end demonstration of the proposed financial service/product to MAS.
3. Please provide full details of the applicable legal/regulatory requirements and the relaxation that you are seeking in order to deliver the proposed financial service/product in the sandbox:
- a. State all the regulatory status³ (e.g. licensing, registration, notification, approval, recognition) required.
 - b. Include a legal opinion, if available, from a qualified legal practitioner applying the relevant laws administered by MAS to the facts of your case. For a digital token offering⁴, a legal opinion is required and should also refer to terms and conditions for the offering, which would be executed and be legally binding on the token issuer and on token holders;
 - c. State the specific legal and regulatory requirements that you are seeking MAS to relax for the duration of the sandbox, and why so; and
 - d. Describe how you intend to meet the full legal and regulatory requirements before exiting the sandbox.
4. Please provide full details of the proposed sandbox design, covering the following areas:
- a. Describe the experiments to be conducted in the sandbox, including specific testing of the application of technology in the proposed financial service/product;
 - b. For each experiment described in 4(a), provide the indicator(s) and corresponding value(s) that would be used to monitor and assess the progress of the experiment;

³ MAS regulations, guidance and licensing: <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing.aspx>

⁴ A digital token offering includes an initial coin offering (ICO) or ongoing coin offering.

- c. State and justify the sandbox boundaries, including:
 - i. Start and end date of the sandbox;
 - ii. Limit on the type (e.g. retail, accredited) of customers involved;
 - iii. Limit on the number of customers involved;
 - iv. Other quantifiable limits such as transaction thresholds or cash holding limits;
and
 - v. Quantification of the maximum loss and impact, including any potential knock-on effects;
- d. Based on 4(c), describe the controls to be put in place so as to manage risk and failure in the sandbox, including money laundering, terrorism financing and technology risks; and
- e. Describe the exit and transition plan for customers in the sandbox as well as the resolution plans and how the business would be run off, in the event that the proposed financial service/product has to be discontinued.

Section B: Application Template

Please attach supporting document/information, if any.

1. Please provide full details of your organisation, addressing item 1a to 1d in Section A of Annex B.

2. Please provide full details of the proposed financial service/product to be experimented in the sandbox, addressing item 2a to 2f in Section A of Annex B.

3. Please provide full details of the applicable legal/regulatory requirements and the relaxation that you are seeking in order to deliver the proposed financial service/product in the sandbox, addressing item 3a to 3d in Section A of Annex B.

4. Please provide full details of the proposed sandbox design, addressing item 4a to 4e in Section A of Annex B.

ANNEX C

AN EXAMPLE OF A SANDBOX APPLICATION

Scenario

- A firm has developed an innovative financial service, using a combination of existing and new technology, for an activity regulated or likely to be regulated by MAS.
- Based on its research, the proposed financial service is able to address an existing gap in the financial sector, and the firm intends to deploy the proposed financial service in Singapore.
- The firm has performed rigorous due diligence on the proposed financial service in its laboratory environment.
- However, the firm is uncertain if significant risks have been effectively addressed given that there was no precedent to guide the testing.
- In addition, the firm is still at the early growth stage, and is unable to fully comply with existing legal and regulatory requirements. It is looking for certain exemptions to be granted by MAS.

Existing Approach

- The firm submits a licence application to MAS and indicates the specific exemptions required.
- Given the novelty of the proposed financial service and that the firm does not have a track record comparable with established FIs, MAS could take a longer time to understand the business model and technology, and clarify the potential risks.
- With the existing approach, the scenario could potentially develop into the following outcomes, whereby promising innovations were being stifled and the doors to potential opportunities were being closed:
 - The firm could face uncertainty during the application process;
 - The firm may drop the idea and stick to business-as-usual; or
 - The firm may consider deploying the proposed financial service outside of Singapore if the regulatory environment is perceived to be more conducive.

Sandbox Approach

- Given MAS' encouragement of experimentation of FinTech innovations through the adoption of a sandbox, the firm submits an application in accordance with the sandbox guidelines.
- As the firm does not have a contact point with any MAS Review Officer, it submits the application and supporting information to FinTech_Sandbox@mas.gov.sg.

- MAS receives the application and assesses it against the sandbox evaluation criteria, including the specific legal and regulatory requirements to be relaxed for the duration of the sandbox.
- To facilitate the firm with its business and resource planning, MAS will inform the applicant whether the application is potentially suitable for a sandbox within 21 working days after receiving the information necessary for the evaluation.
- MAS continues with the evaluation and clarification with the firm. The firm will be informed in writing whether to proceed with the sandbox, as the sandbox entity.

Evaluation Criteria	Assessment (illustrative and non-exhaustive)
Does the proposed financial service include new or emerging technology, or use existing technology in an innovative way?	The proposed financial service is not available in Singapore. It utilises technology to improve customer experience and streamline operations. The applicant applies for certain legal and regulatory requirements to be relaxed for the duration of the sandbox, as it is unable to fully meet the relevant legal and regulatory requirements now.
Does the proposed financial service address an issue or bring benefits to consumers or the industry?	
Does the applicant have the intention and ability to deploy the proposed financial service in Singapore on a broader scale after exiting the sandbox?	The applicant has recently secured \$1m funding. It has doubled its headcount over last year, and has provided a business plan and roadmap to deploy the proposed financial service in Singapore on a broader scale.
Are the test scenarios and expected outcomes clear?	The sandbox will be limited to 50 customers and run for a period of 6 months to measure improvements in customer experience and to validate the risk exposure and mitigation measures.
Are the boundary conditions appropriate?	
Are significant risks assessed and mitigated?	The proposed financial service has been tested under various risk scenarios in an internal test environment.
Is there a clear exit and transition strategy?	In the event that the proposed financial service has to be discontinued, the sandbox customers will be informed in advance to ensure a smooth exit.

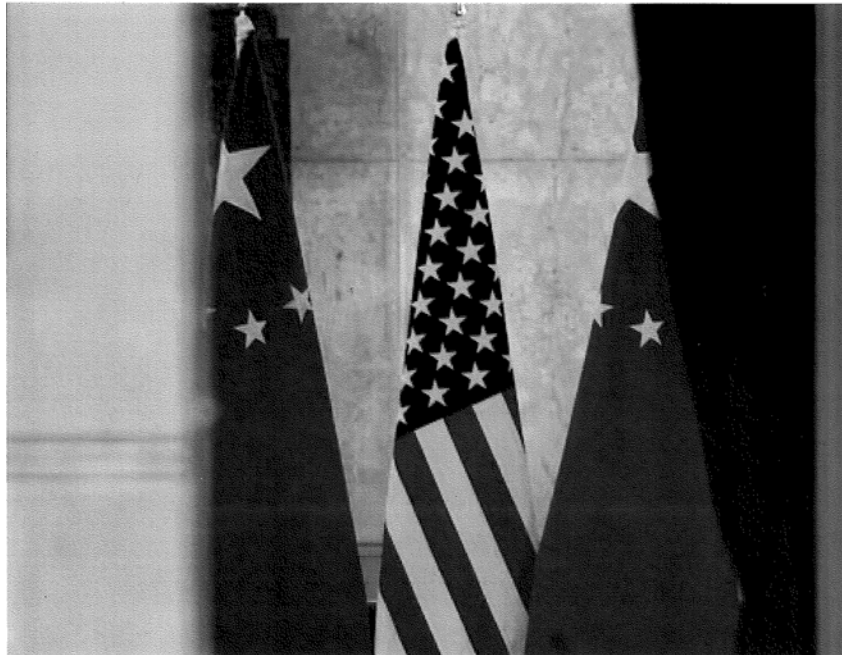
Monetary Authority of Singapore
10 Shenton Way
MAS Building
Singapore 079117

FinTech_Sandbox@mas.gov.sg

US halted plans to sanction Chinese spy agency to maintain trade truce, FT says

By Reuters

December 3, 2025 11:53 PM EST Updated December 3, 2025



U.S. and China flags are pictured at Lancaster House, on the second day scheduled for trade talks between the U.S. and China, in London, Britain, June 10, 2025.
REUTERS/Toby Melville [Purchase Licensing Rights](#)

Dec 3 (Reuters) - The United States has halted plans to impose sanctions on China's ministry of state security over a massive cyber spying campaign to avoid derailing a trade truce struck by both countries this year, the Financial Times said on Wednesday.

Chinese-linked hackers had [previously targeted](#) a host of U.S. and global telecommunications companies and a U.S. state's Army National Guard network in a wide-ranging and years-long cyberespionage campaign tracked as Salt Typhoon.

The Reuters Daily Briefing newsletter provides all the news you need to start your day. Sign up [here](#).



President Donald Trump's administration will also not enact major new export controls against China, the report said, citing several U.S. officials and others familiar with the situation.

The White House did not immediately respond to a request for comment. Reuters could not immediately verify the report.

Following months of trade tensions triggered by U.S. tariffs, Chinese leader Xi Jinping and Trump reached a framework agreement in South Korea on October 30. Washington agreed not to impose 100% tariffs on Chinese imports and China would hold off on an export licensing regime for crucial rare earth minerals and magnets.

The Honorable French Hill
Chairman
House Financial Services Committee
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
House Financial Services Committee
4340 O'Neill House Building
Washington, DC 20515

December 10, 2025

Re: Oppose the Unleashing AI Innovation in Financial Services Act (Rep. Hill H.R. 4801/Sen. Rounds S. 2528)

Dear Chairman Hill and Ranking Member Waters:

The undersigned 64 civil rights, consumer, community, tech accountability, and other organizations urge you to oppose the Unleashing AI Innovation in Financial Services Act (H.R. 4801). The legislation would allow regulated financial firms to deploy artificial intelligence (AI) systems without regulatory supervision, oversight, or enforcement. Virtually any company that uses AI — as nearly all soon will do — would be able to request full waivers of consumer and investor protection laws with hollow alternatives that could expose consumers, customers, competitors, investors, the financial industry, and the economy to substantial risks with few or no regulatory safeguards or accountability.

The use of AI in the financial sector has the potential to reduce costs, improve efficiency, detect and prevent fraud, and increase the access, quality, and choice of financial services and products. But these potential benefits for consumers, customers, investors, markets, and the financial system can only materialize if people are protected from the many risks of AI in financial services through the consistent application and enforcement of federal civil rights, consumer protection, investor protection, market integrity, and financial supervision statutes and regulations.

The financial industry has already been deploying AI within the bounds of federal laws and regulations across its business lines from customer service to automated underwriting to securities trading to risk management and more. These legal and regulatory regimes are designed to protect people and the financial system from predatory practices, market manipulation, and economic instability. There is no justification for allowing companies to deploy AI systems that would otherwise violate federal laws and pose risks to people and the economy. Nor does the use of AI, however trivial, justify broad waivers of our consumer and investor protection laws.

The risks of AI to consumers are real and substantiated, including well-documented racial and other biases in accessing affordable credit. AI credit underwriting and decision-making systems tend to amplify existing patterns of discrimination against Black, Latino, Asian American, and Indigenous people; women; and people with disabilities in the approval, pricing, and terms of credit products like student loans, mortgages, and other credit products. AI-powered debt collection can expose people to increasingly 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 and result in consumers and businesses losing their bank accounts.

Emerging concerns like agentic AI — which acts on consumers' behalf to make purchases or transactions — present growing problems and the potential for new risks and harms. AI-powered consumer relations chatbots can give incorrect or misleading answers to complex questions and AI-powered consumer fraud has become an increasing problem for the financial industry. Problems of accountability, including for assessing liability when fraud occurs, can be made more difficult when

multiple AI systems interact on a single transaction. When systems are opaque, and the rationale for their decisions is not explainable, resolving their mistakes may be difficult or impossible. These concerns underscore the need to retain supervision and enforcement of AI technologies.

Similarly, AI can exacerbate risks to investor protection, market integrity, and financial stability. AI-powered high-speed trading can manipulate markets and harm investors. 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. 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.

Unless regulators can supervise and enforce how these technologies are brought to market, the right to privacy will be under constant threat. AI systems rely on collecting and storing massive amounts of data about consumers and businesses to operate. Already, many of these Big Tech firms are pushing past existing privacy protection boundaries, challenging regulators' ability to close the loopholes these firms are exploiting. With each new incursion on privacy, surveillance of private decisions intensifies. Privacy is a foundational right in our society, but unless we give regulators the power to protect it, it will steadily erode.

The legislation does little to protect people from these risks. The modest nods to consumer protection, fraud, investor protection, anti-money laundering, and financial stability are woefully inadequate to safeguard people or the economy. The mere increase in "access" to dangerous products would justify waivers of the law. 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.

The legislation does not even pretend to address the endemic biases against Black, Latino, Asian American, and Indigenous people; women; and people with disabilities in AI systems. It does not require financial firms to disclose the use of AI to their customers, require customers' consent to collect personal data, or provide any remedies for inaccuracies or data errors.

H.R. 4801 would allow financial firms to profit by capturing most of the benefits of AI but force their customers and the economy to bear the burdens from the risks and the harms of AI deployment in the financial sector. We urge the Committee and the Congress to oppose this legislation that provides broad immunity for unlawful practices or outcomes that can substantially harm people, communities, and the economy.

Sincerely,

AFT
AI Now Institute
American Civil Liberties Union
American Economic Liberties Project
Americans for Financial Reform
Brooklyn Cooperative Federal Credit Union
California Advocates for Nursing Home Reform
CAMEO Network
Center for Democracy & Technology

Center for Digital Democracy
Center for Economic Integrity
Center for Independence of the Disabled, New York (CIDNY)
Citizen Action of New York
Coalition on Human Needs
Communication Workers of America (CWA)
Consumer Action
Consumer Federation of America
Consumer Reports

Consumer Watchdog	National CAPACD — National Coalition for Asian Pacific American Community Development
Consumers for Auto Reliability and Safety Data & Society	National Community Reinvestment Coalition (NCRC)
DC Consumer Rights Coalition	National Consumer Law Center (on behalf of its low-income clients)
Delaware Community Reinvestment Action Council, Inc.	National Fair Housing Alliance
Economic Action Maryland Fund	National Hispanic Media Coalition
Economic Security Project Action	New Economy Project
Electronic Privacy Information Center (EPIC)	New York Legal Assistance Group
Equal Rights Advocates	New Yorkers for Responsible Lending
HEAL (Health, Environment, Agriculture, Labor) Food Alliance	NJ Appleseed Public Interest Law Center
Hip Hop Caucus	Oregon Consumer Justice
Housing Action Illinois	Oregon Consumer League
Housing and Economic Rights Advocates	Progressive Leadership Alliance of Nevada
Investor Alliance for Human Rights	Public Citizen
The Leadership Conference on Civil and Human Rights	Public Good Law Center
League of United Latin American Citizens (LULAC)	Racial Justice Investing Coalition
Legal Action Chicago	Seventh Generation Interfaith Coalition for Responsible Investment
Legal Aid Center of Southern Nevada	South Carolina Appleseed Legal Justice Center
Metropolitan Interfaith Council on Affordable Housing	TechTonic Justice
NAACP Legal Defense and Educational Fund, Inc. (LDF)	Tzedek DC
National Action Network	UnidosUS
National Association of Consumer Advocates	Virginia Citizens Consumer Council
	Virginia Poverty Law Center
	Western Center on Law and Poverty
	Woodstock Institute

cc. Senate Banking Committee Chairman Tim Scott and Senate Banking Committee Ranking Member Elizabeth Warren



December 9, 2025

Chairman French Hill and Ranking Member Maxine Waters
U.S. House Committee on Financial Services
U.S. House of Representatives 2128 Rayburn House Office Building
Washington, D.C. 20515

Re: H.R. 4801, Unleashing AI Innovation in Financial Services Act

Dear Chairman Hill and Ranking Member Waters,

Consumer Reports¹ respectfully opposes the Unleashing AI Innovation in Financial Services Act as introduced. This bill's fundamental premise appears to be that companies should be permitted to exempt themselves from existing consumer protection law simply because they are using AI. While we appreciate the profound impact innovation can have on increasing competition and delivering consumer benefits in the financial sector, this bill, as currently written, would put consumers directly in harm's way by weakening much needed regulatory oversight in the already high-risk, low-transparency space in which artificial intelligence exists. The approach outlined in this bill sets a dangerous precedent and puts hard-won safeguards for consumers at serious risk.

We call attention to three major areas of concern.

Weakened Regulatory Oversight. The bill effectively grants financial institutions regulatory forbearance by allowing them to experiment with AI systems while seeking waivers from existing consumer protection laws. We believe this would significantly weaken critical safeguards. Furthermore, by removing language that would allow agencies to establish additional AI test project categories after approving initial projects, the bill also reduces regulatory adaptability in a sector defined by rapid technological change. This limitation would constrain agencies' abilities to respond to emerging AI risks and applications that were not initially contemplated.²

The bill's use of the term "substantially similar"³ with respect to previously denied submissions being resubmitted for approval is also unclear. While limiting resubmissions is a positive addition to this bill's reintroduction, the absence of clear standards for what constitutes "substantially similar" applications is conspicuous and could allow companies to repeatedly submit marginally modified proposals until one is approved.

Moreover, the "deemed approved" provision, reverses the appropriate burden of proof. Instead of companies proving their AI systems are safe, regulators must prove danger within tight

¹ Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR also advocates for laws and corporate practices that are beneficial for consumers. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities facing today's consumers, and provides ad-free content and tools to 6 million members across the United States.

² Sec. 2 (d) REGULATIONS.—After approving not fewer than 1 AI test project, an agency may promulgate regulations, after providing a notice and an opportunity for public comment, other AI activities or products that qualify as AI test projects

³ Sec. 2 (l) RESUBMITTALS

deadlines - or harmful systems could automatically proceed. This is particularly concerning given that agencies lack dedicated funding to review complex AI applications within the 120-day window required by the bill. While we recognize the 120-day extension for regulatory review is an improvement from the previous version of this bill, the lack of a clear definition of “substantially similar” undermines the effectiveness of this extension for regulators.

Additionally, the shift from requiring applicants to “demonstrate” benefits to merely “explain” them represents a significant weakening of approval standards. This lower evidentiary bar could approve projects based on speculative or overstated consumer benefits rather than proven value.

Finally, the bill requires each financial regulatory agency to establish or identify an AI Innovation Lab to review waiver submissions without addressing funding or staffing resources. The combination of vague definitions, automatic approval mechanisms, and weakened evidentiary standards creates a perfect storm where under-resourced agencies face impossible choices: approve high risk AI experiments - with a high likelihood of compromising consumer protection - quickly or let them proceed by default.

The bill's scope concerning Big Tech companies remains dangerously ambiguous. Companies like Google (with its Agent Payment Protocol) may exploit banking partnerships to access sandbox benefits while evading traditional financial regulation. This could create regulatory arbitrage where the most powerful AI systems escape meaningful oversight.

Insufficient Consumer Safeguards

This bill lacks protections that Consumer Reports sees as critical for ensuring consumer safety in the burgeoning intersection between finance and AI.

This bill lacks critical transparency and accountability requirements for AI systems while potentially allowing waivers from existing Equal Credit Opportunity Act protections. At the outset, the bill fails to meaningfully define what would constitute a, “substantial use of artificial intelligence.” This vague standard could allow companies to game the system, either avoiding oversight by claiming minimal AI use or accessing regulatory relief for systems that should face full scrutiny.

More fundamentally, the bill also fails to require companies to test their AI systems for bias or to submit those systems to formal audits that would assess their fairness, accuracy, and potential harms leaving consumers vulnerable to discriminatory or opaque decision-making. While ECOA requires adverse action notices explaining why individual credit applications were denied, these existing requirements should not be subject to waiver and are insufficient on their own for complex AI models. Disparate impact liability under ECOA is essential for detecting discrimination in opaque AI systems where intentional bias may be difficult to prove but discriminatory outcomes are measurable and real.

This concern becomes especially urgent in light of ongoing regulatory proceedings. Consumer Reports has urged the CFPB to retain disparate impact liability as an established and essential means of identifying discriminatory effects in automated underwriting systems. As we emphasize in those comments, as credit decisions become more automated and reliant upon complex models, disparate impact analysis becomes more - not less - necessary to detect discrimination that occurs without intentional bias. Yet this bill would allow financial institutions to seek waivers from these very protections, creating a pathway to avoid accountability for

qualified applicants to access credit precisely when AI systems can pose heightened discrimination risks.

These outcomes affect livelihoods and without accountability measures, they directly impact people's ability to participate fully in the economy and pursue financial independence. Without safeguards there is a real risk that AI systems could entrench historical inequities at scale, unfairly limiting financial opportunities for individuals through inaccurate or opaque decision-making.

These risks are compounded by the bill's failure to provide meaningful redress mechanisms for consumers harmed by AI-driven decisions. Put another way, not only does the bill lack adequate safeguards to prevent harm, but it also does not outline for consumers any clear mechanisms to seek redress when harms do occur. Without clear accountability frameworks when AI systems make harmful or erroneous financial decisions, consumers may be left to navigate complex, high-stakes problems on their own.

Misaligned Incentives

We are also concerned about the risk of firms optimizing AI systems for institutional profits at the cost of consumer welfare. Specifically, the inclusion of "investor" alongside "consumer" protections muddies the waters.⁴ Consumer and investor protections serve inherently different purposes and populations. Conflating them could dilute focus on vulnerable consumers who most need protection from AI bias and discrimination. As AI systems are granted more authority in financial decision making, concerns about consumer autonomy become increasingly pressing. These technologies are both influencing decisions about consumers, such as loan approvals or fraud detections, and are now beginning to act on their behalf through agentic AI. The emergence of these agentic AI tools that can initiate transactions, manage bills, or make purchases introduces new challenges around transparency, consent, and control. Without clear guardrails, consumers may unknowingly delegate sensitive financial actions to automated systems, with limited ability to monitor, override, or understand those choices. In the face of enormous financial incentives from various actors in the financial ecosystem, this is precisely the environment where strong regulation is needed.

Conclusion: Promote Innovation While Maintaining Robust Protections for Consumers

We appreciate the intent behind this bill is to encourage innovation through regulatory sandboxes and understand the desire to create a flexible framework to unleash the power of AI in financial services. That said, to strengthen the bill and better protect consumers, we recommend a narrower, more tailored approach. Rather than broadly waiving existing rules for AI-related activities, effective sandboxes should provide enhanced scrutiny alongside safe harbor protections for good-faith compliance efforts. The bill's scope should focus on genuinely novel AI applications where current regulations are unclear rather than simply easing requirements seen as burdensome or to otherwise circumvent well-established protections. Crucially, baseline consumer safeguards including anti-discrimination laws, privacy protections, safety standards, fraud prevention, and anti-deception rules, should remain fully in place and not be subject to waivers. This balanced approach will help ensure innovation flourishes while maintaining the same vital protections that consumers have come to expect and rely on in the financial services space.

⁴ Sec 3 (2)(A)(iii)(III)(aa) and Sec 3 (2)(B)(iii)(III)(aa)

Sincerely,

Lacey Aaker
Policy Analyst, CR



U.S. House Committee on Financial Services
Hearing on “*From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services*”
Responses to Questions for the Record

Ms. Jeanette Manfra
VP, Head of Risk and Compliance, Google Cloud

**Responses to Questions from the Honorable Barry Loudermilk, Representative,
Committee on Financial Services**

Question 1: Ms. Manfra, can you explain how Google Cloud's platform allows institutions to detect risks across distributed datasets while preserving consumers' privacy?

At Google Cloud, we believe that artificial intelligence (AI) offers a transformative opportunity to enhance security and risk team operations, including security operations, and drive data-based decision-making while also protecting consumer privacy. We incorporate important privacy principles such as privacy-by-design, secure-by-default and encryption-by-default from the beginning of the development of AI services. Customers have control and ownership of their datasets, and Google Cloud does not use customer data for training models without customer's prior permission or instruction. In addition to complying with applicable privacy laws, we also use privacy-preserving technologies such as [masking](#), [tokenization](#), and [data clean rooms](#).

Our advancements in AI anomaly detection help companies identify, or even predict, abnormal patterns in unbounded data streams. Whether the companies are a large retailer identifying positive buying behaviors, a financial services provider detecting fraud, or a telecommunications company identifying and mitigating potential threats, they can use our tools to help detect behavioral patterns that provide useful insights.

With Google Cloud's Anti-Money Laundering (AML) AI, we provide a consolidated machine learning (ML)-generated customer risk score as an alternative to traditional transaction alerting. The risk score is based on the bank's data including transactional patterns, network behavior, and Know Your Customer (KYC) data to identify instances and groups of high-risk retail and commercial customers. The product can adapt to changes in underlying data, delivering more accurate results, which increases overall program effectiveness and improves operational efficiency.



We [model and promote](#) the adoption of responsible and secure AI data practices that couple these detection capabilities with a holistic approach to risk management that promotes the preservation of our customers' privacy and their compliance journey. Robust privacy [commitments](#) outline how we protect user data and prioritize privacy and the greater adoption of AI rearms their importance. We adhere to a holistic approach to [AI risk management and compliance](#), including focusing on employing an AI risk assessment methodology for identifying, assessing, and mitigating risks; developing and using an automated, scalable, and evidence-based approach for auditing generative AI workloads; and emphasizing human oversight and collaboration in our risk assessments and governance councils.

We continue to empower financial institutions to activate advanced AI risk detection and stringent privacy and compliance protections. By utilizing a plethora of privacy-preserving mechanisms, such as those described above, and others, we aim to help ensure the financial sector can leverage AI advancements without compromising consumer privacy.

119TH CONGRESS
1ST SESSION

H. R. 4801

To establish AI Innovation Labs that permit certain persons to experiment with artificial intelligence without expectation of enforcement actions.

IN THE HOUSE OF REPRESENTATIVES

JULY 29, 2025

Mr. HILL of Arkansas (for himself, Mr. TORRES of New York, Mr. STEIL, and Mr. GOTTHEIMER) introduced the following bill; which was referred to the Committee on Financial Services

A BILL

To establish AI Innovation Labs that permit certain persons to experiment with artificial intelligence without expectation of enforcement actions.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Unleashing AI Innova-
5 tion in Financial Services Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this section:

8 (1) AI TEST PROJECT.—The term “AI test
9 project” means a financial product or service that—

1 (A) falls under the jurisdiction of a finan-
2 cial regulatory agency;

3 (B) makes substantial use of artificial in-
4 telligence; and

5 (C) is, or may be, subject to a Federal reg-
6 ulation or Federal statute.

7 (2) APPROPRIATE FINANCIAL REGULATORY
8 AGENCY.—The term “appropriate financial regu-
9 latory agency” means—

10 (A) the appropriate Federal banking agen-
11 cy, as defined in section 3 of the Federal De-
12 posit Insurance Act (12 U.S.C. 1813), with re-
13 spect to an institution described in subsection
14 (q) of that section;

15 (B) the Securities and Exchange Commis-
16 sion, with respect to an institution not de-
17 scribed in subparagraph (A) that is—

18 (i) any broker or dealer that is reg-
19 istered with the Commission under the Se-
20 curities Exchange Act of 1934 (15 U.S.C.
21 78a et seq.);

22 (ii) any investment company that is
23 registered with the Commission under the
24 Investment Company Act of 1940 (15
25 U.S.C. 80a–1 et seq.);

1 (iii) any investment adviser that is
2 registered with the Commission under the
3 Investment Advisers Act of 1940 (15
4 U.S.C. 80b-1 et seq.);

5 (iv) any clearing agency registered
6 with the Commission under the Securities
7 Exchange Act of 1934 (15 U.S.C. 78a et
8 seq.);

9 (v) any nationally recognized statis-
10 tical rating organization registered with
11 the Commission under the Securities Ex-
12 change Act of 1934 (15 U.S.C. 78a et
13 seq.);

14 (vi) any transfer agent registered with
15 the Commission under the Securities Ex-
16 change Act of 1934 (15 U.S.C. 78a et
17 seq.);

18 (vii) any exchange registered as a na-
19 tional securities exchange with the Com-
20 mission under the Securities Exchange Act
21 of 1934 (15 U.S.C. 78a et seq.);

22 (viii) any national securities associa-
23 tion registered with the Commission under
24 the Securities Exchange Act of 1934 (15
25 U.S.C. 78a et seq.);

1 (ix) any securities information proc-
2 essor registered with the Commission
3 under the Securities Exchange Act of 1934
4 (15 U.S.C. 78a et seq.);

5 (x) the Municipal Securities Rule-
6 making Board established under the Secu-
7 rities Exchange Act of 1934 (15 U.S.C.
8 78a et seq.);

9 (xi) the Public Company Accounting
10 Oversight Board established under the
11 Sarbanes-Oxley Act of 2002 (15 U.S.C.
12 7211 et seq.);

13 (xii) the Securities Investor Protection
14 Corporation established under the Securi-
15 ties Investor Protection Act of 1970 (15
16 U.S.C. 78aaa et seq.); and

17 (xiii) any security-based swap execu-
18 tion facility, security-based swap data re-
19 pository, security-based swap dealer, or
20 major security-based swap participant reg-
21 istered with the Commission under the Se-
22 curities Exchange Act of 1934 (15 U.S.C.
23 78a et seq.), with respect to the security-
24 based swap activities of the person that re-

1 quire such person to be registered under
2 such Act;

3 (C) the Bureau of Consumer Financial
4 Protection, with respect to a covered person, as
5 defined in section 1002 of the Consumer Finan-
6 cial Protection Act of 2010 (12 U.S.C. 5481),
7 that does not have an appropriate financial reg-
8 ulatory agency under subparagraph (A), (B),
9 (D), or (E) of this paragraph;

10 (D) the National Credit Union Administra-
11 tion, with respect to an insured credit union, as
12 defined in section 101 of the Federal Credit
13 Union Act (12 U.S.C. 1752); and

14 (E) the Federal Housing Finance Agency,
15 with respect to—

16 (i) a Federal Home Loan Bank;

17 (ii) the Federal Home Loan Bank
18 System;

19 (iii) the Federal National Mortgage
20 Association; and

21 (iv) the Federal Home Loan Mortgage
22 Corporation.

23 (3) ARTIFICIAL INTELLIGENCE; AI.—The terms
24 “artificial intelligence” and “AI” have the meaning
25 given the term “artificial intelligence” in section

1 5002 of the National Artificial Intelligence Initiative
2 Act of 2020 (15 U.S.C. 9401).

3 (4) COMMISSION.—The term “Commission”
4 means the Securities and Exchange Commission.

5 (5) FEDERAL SECURITIES LAWS.—The term
6 “Federal securities laws” means—

7 (A) the Securities Act of 1933 (15 U.S.C.
8 77a et seq.);

9 (B) the Securities Exchange Act of 1934
10 (15 U.S.C. 78a et seq.);

11 (C) the Sarbanes-Oxley Act of 2002 (15
12 U.S.C. 7201 et seq.);

13 (D) the Trust Indenture Act of 1939 (15
14 U.S.C. 77aaa et seq.);

15 (E) the Investment Company Act of 1940
16 (15 U.S.C. 80a–1 et seq.);

17 (F) the Investment Advisers Act of 1940
18 (15 U.S.C. 80b–1 et seq.);

19 (G) the Jumpstart Our Business Startup
20 Act (Public Law 112–106; 126 Stat. 306); and

21 (H) the Dodd-Frank Wall Street Reform
22 and Consumer Protection Act (Public Law
23 111–203; 124 Stat. 1376).

24 (6) FINANCIAL PRODUCT OR SERVICE.—The
25 term “financial product or service”—

1 (A) has the meaning given the term in sec-
2 tion 1002 of the Consumer Financial Protection
3 Act of 2010 (12 U.S.C. 5481);

4 (B) includes—

5 (i) activities that are financial in na-
6 ture, as defined in section 4(k)(4) of the
7 Bank Holding Company Act of 1956 (12
8 U.S.C. 1843(k)(4));

9 (ii) any financial product or service
10 provided by a person regulated by the
11 Commission, as defined in section 1002 of
12 the Consumer Financial Protection Act of
13 2010 (12 U.S.C. 5481); and

14 (iii) includes the offer or sale of any
15 security subject to the Federal securities
16 laws; and

17 (C) does not include the business of insur-
18 ance.

19 (7) FINANCIAL REGULATORY AGENCY.—The
20 term “financial regulatory agency” means—

21 (A) the Board of Governors of the Federal
22 Reserve System;

23 (B) the Federal Deposit Insurance Cor-
24 poration;

1 (C) the Office of the Comptroller of the
2 Currency;

3 (D) the Securities and Exchange Commis-
4 sion;

5 (E) the Bureau of Consumer Financial
6 Protection;

7 (F) the National Credit Union Administra-
8 tion; and

9 (G) the Federal Housing Finance Agency.

10 (8) REGULATED ENTITY.—The term “regulated
11 entity” means an entity regulated by any financial
12 regulatory agency.

13 **SEC. 3. USE OF ARTIFICIAL INTELLIGENCE BY REGULATED**
14 **FINANCIAL ENTITIES.**

15 (a) AI INNOVATION LABS.—

16 (1) ESTABLISHMENT.—Each financial regu-
17 latory agency shall establish, or identify an office,
18 division, or department of the agency that shall
19 serve as, an AI Innovation Lab to enable regulated
20 entities to experiment with AI test projects without
21 unnecessary or unduly burdensome regulation or ex-
22 pectation of enforcement actions, pursuant to the
23 approval of an application under paragraph (2).

24 (2) APPLICATIONS.—

25 (A) SUBMISSION.—

1 (i) IN GENERAL.—A regulated entity
2 may submit to the appropriate financial
3 regulatory agency an application, on a
4 form determined by the appropriate finan-
5 cial regulatory agency, to engage in an AI
6 test project through the AI Innovation Lab
7 established or identified under paragraph
8 (1).

9 (ii) CONTENTS.—An application sub-
10 mitted under clause (i) shall include—

11 (I) a description of the AI test
12 project proposed to be carried out by
13 the regulated entity;

14 (II) an alternative compliance
15 strategy that—

16 (aa) identifies a regulation
17 issued by the appropriate finan-
18 cial regulatory agency that the
19 regulated entity requests to be
20 waived or modified; and

21 (bb) proposes an alternative
22 method for the regulated entity
23 to comply with the regulation, in-
24 cluding an explanation as to why
25 the alternative method is essen-

1 tial to the operation of the entity
2 and how the regulated entity
3 would effectively manage risks
4 associated with the AI test
5 project;

6 (III) an explanation of how under
7 the strategy described in subclause
8 (II), the AI test project—

9 (aa) would serve the public
10 interest, improve consumer or in-
11 vestor access to a financial prod-
12 uct or service, or promote con-
13 sumer or investor protection;

14 (bb) would enhance effi-
15 ciency or operations, foster inno-
16 vation or competitiveness, im-
17 prove risk management and secu-
18 rity, or enhance regulatory com-
19 pliance;

20 (cc) would not present a sys-
21 temic risk to the financial system
22 of the United States;

23 (dd) is consistent with the
24 purposes of the anti-money laun-
25 dering and countering the financ-

1 ing of terrorism obligations under
2 subchapter II of chapter 53 of
3 title 31, United States Code; and

4 (ee) would not present a na-
5 tional security risk to the United
6 States;

7 (IV) a proposed date on which
8 the AI test project would terminate
9 and an explanation why such termi-
10 nation date would be appropriate;

11 (V) proposed limitations on the
12 size, scope, and growth of the AI test
13 project;

14 (VI) a detailed business plan;
15 and

16 (VII) an estimate of the eco-
17 nomic impact of the AI test project if
18 approved.

19 (iii) JOINT APPLICATIONS.—Two or
20 more regulated entities may submit a joint
21 application to the same financial regu-
22 latory agency under clause (i).

23 (iv) REGULATIONS OF OTHER AGEN-
24 CIES.—

1 (I) IN GENERAL.—A regulated
2 entity may submit an application
3 under this subparagraph that includes
4 an alternative compliance strategy for
5 a regulation issued or enforced by a
6 financial regulatory agency that is not
7 the appropriate financial regulatory
8 agency for the regulated entity.

9 (II) REQUIREMENTS.—An appli-
10 cation described in subclause (I) shall
11 be subject to the same requirements
12 as an application described in clause
13 (ii), except that—

14 (aa) the regulated entity
15 shall submit the application to
16 the appropriate financial regu-
17 latory agency and the financial
18 regulatory agency that issued or
19 enforces the regulation that is
20 the subject of the alternative
21 compliance strategy; and

22 (bb) the AI test project may
23 not take effect unless the appro-
24 priate financial regulatory agency
25 and any other financial regu-

1 latory agency that issued or en-
2 forces the regulation that is the
3 subject of the alternative compli-
4 ance strategy jointly approve the
5 application using the process de-
6 scribed in subparagraph (B).

7 (v) NOTICE.—A regulated entity that
8 is regulated or supervised by more than 1
9 financial regulatory agency shall provide
10 notice of any application submitted to the
11 appropriate financial regulatory agency
12 under this section to each financial regu-
13 latory agency by which it is regulated or
14 supervised not later than 5 business days
15 after the entity submits the application to
16 the appropriate financial regulatory agen-
17 cy.

18 (B) AGENCY REVIEW.—

19 (i) IN GENERAL.—Except as provided
20 in clause (iv), not later than 120 days
21 after the date on which an application is
22 submitted to the appropriate financial reg-
23 ulatory agency under subparagraph (A),
24 the appropriate financial regulatory agency
25 shall—

- 1 (I) review the application; and
2 (II) submit to the applicant in
3 writing a determination of the agency.

4 (ii) APPROVAL.—

- 5 (I) IN GENERAL.—If the appli-
6 cant shows that it is more likely than
7 not that the application meets the re-
8 quirements for establishing an alter-
9 native compliance strategy and satis-
10 fies the standards described in sub-
11 clauses (II) and (III) of subparagraph
12 (A)(ii), the agency shall approve the
13 application and notify the applicant in
14 writing of—

- 15 (aa) the regulation that is
16 the subject of the alternative
17 compliance strategy;

- 18 (bb) the terms of the alter-
19 native compliance strategy for
20 the AI test project;

- 21 (cc) the date on which the
22 AI test project will terminate;

- 23 (dd) any limitations on the
24 size, scope, or growth of the AI
25 test project; and

1 (ee) any additional limita-
2 tions or conditions on the AI test
3 project, as determined by the ap-
4 propriate financial regulatory
5 agency.

6 (II) EFFECT OF APPROVAL.—
7 With respect to an AI test project, ex-
8 cept as provided in subclause (III),
9 beginning on the date on which an ap-
10 plication submitted under subpara-
11 graph (A) is approved and ending on
12 the date described in subclause
13 (I)(cc)—

14 (aa) the appropriate finan-
15 cial regulatory agency may en-
16 force a regulation described in
17 subclause (I)(aa) only in the
18 manner set out in the alternative
19 compliance strategy described in
20 subclause (I)(bb); and

21 (bb) a financial regulatory
22 agency that is not the appro-
23 priate financial regulatory agency
24 may not enforce a regulation de-
25 scribed in subclause (I)(aa).

1 (III) ENFORCEMENT BY AN-
2 OTHER FINANCIAL REGULATORY
3 AGENCY.—With respect to an AI test
4 project, a financial regulatory agency
5 other than the appropriate financial
6 regulatory agency that approves an
7 application under subparagraph
8 (A)(iv) may enforce a regulation de-
9 scribed in subclause (I)(aa) if the al-
10 ternative compliance strategy de-
11 scribed in subclause (I)(bb) provides
12 for enforcement by such financial reg-
13 ulatory agency.

14 (IV) RULE OF CONSTRUCTION.—
15 Nothing in this clause may be con-
16 strued to limit the authority of a fi-
17 nancial regulatory agency to take an
18 enforcement action against a regu-
19 lated entity with respect to fraud or
20 for engaging in an unsafe or unsound
21 practice relating to an AI test project.

22 (iii) DENIAL.—

23 (I) IN GENERAL.—If an agency
24 denies an application submitted under
25 subparagraph (A), the agency—

1 (aa) shall submit to the ap-
2 plicant a written notice explain-
3 ing the reason for denial; and

4 (bb) may not take an en-
5 forcement action related to the
6 proposed AI test project against
7 the applicant earlier than the
8 date that is 30 days after the
9 date on which the agency submits
10 the written notice described in
11 item (aa).

12 (II) RESUBMITTALS.—Each time
13 an application submitted under sub-
14 paragraph (A) is denied, the regulated
15 entity—

16 (aa) may submit an amend-
17 ed application after receiving
18 feedback from the agency making
19 such denial; and

20 (bb) may not resubmit more
21 than 2 applications that are sub-
22 stantially similar to the denied
23 application.

24 (III) INJUNCTIVE RELIEF.—A fi-
25 nancial regulatory agency, by and

1 through its own attorneys, may file a
2 civil action in an appropriate United
3 States district court to enjoin an AI
4 test project if the agency determines
5 that the AI test project—

6 (aa) presents an immediate
7 danger to consumers or investors;
8 or

9 (bb) presents a risk—

10 (AA) to financial mar-
11 kets;

12 (BB) in the case of an
13 AI test project engaged in
14 by an insured depository in-
15 stitution or an insured credit
16 union, of loss to a Federal
17 deposit or share insurance
18 fund;

19 (CC) of a violation of
20 anti-money laundering and
21 countering the financing of
22 terrorism obligations under
23 subchapter II of chapter 53
24 of title 31, United States
25 Code; or

1 (DD) to the national
2 security of the United
3 States.

4 (iv) EXTENSION.—If the financial reg-
5 ulatory agency needs additional time, the
6 agency may extend the approval deadline
7 by 120 days. After the expiration of the
8 120-day extension period, if the agency has
9 not made a determination on the applica-
10 tion, the application will automatically be
11 deemed approved and effective.

12 (C) DATA SECURITY.—All data supplied by
13 sponsors of AI test projects to a financial regu-
14 latory agency submitted under this section shall
15 be stored and maintained in a secure manner
16 by the financial regulatory agency, consistent
17 with applicable data security standards.

18 (D) REGULATIONS.—Not later than 180
19 days after the date of enactment of this Act,
20 each financial regulatory agency shall promul-
21 gate regulations that—

22 (i) shall be published in the Federal
23 Register and provide a 60-day period for
24 public notice and comment; and

25 (ii) include—

1 (I) procedures for modifying the
2 AI test projects that are approved by
3 the agency;

4 (II) consequences for failure to
5 comply with the terms of an alter-
6 native compliance strategy;

7 (III) a requirement that an AI
8 test project will terminate not earlier
9 than 1 year after the AI test project
10 is approved;

11 (IV) procedures to extend the
12 termination date described in sub-
13 clause (III);

14 (V) procedures for confiden-
15 tiality; and

16 (VI) procedures for coordinating
17 decisions relating to applications sub-
18 mitted jointly by multiple regulated
19 entities or applications submitted to
20 more than one financial regulatory
21 agency.

22 (b) REPORT.—Not later than 2 years after the date
23 of enactment of this Act, and each year for 7 years there-
24 after, each financial regulatory agency shall submit to the
25 Committee on Banking, Housing, and Urban Affairs of

1 the Senate and the Committee on Financial Services of
2 the House of Representatives an annual report on the out-
3 comes of AI test projects. A report under this subsection
4 may not include the names of participating entities or any
5 proprietary or confidential business information. A report
6 under this subsection shall include aggregated findings,
7 trends, and lessons learned from the AI test projects.

8 (c) RULE OF CONSTRUCTION.—Nothing in this sec-
9 tion may be construed to limit the authority of a financial
10 regulatory agency to take an enforcement action against
11 a regulated entity with respect to fraud relating to an AI
12 test project.

○

119TH CONGRESS
1ST SESSION

H. R. 2152

To require a strategy to defend against the economic and national security risks posed by the use of artificial intelligence in the commission of financial crimes, including fraud and the dissemination of misinformation, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 14, 2025

Mr. NUNN of Iowa (for himself and Mr. HIMES) introduced the following bill;
which was referred to the Committee on Financial Services

A BILL

To require a strategy to defend against the economic and national security risks posed by the use of artificial intelligence in the commission of financial crimes, including fraud and the dissemination of misinformation, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Artificial Intelligence
5 Practices, Logistics, Actions, and Necessities Act” or the
6 “AI PLAN Act”.

1 **SEC. 2. STRATEGY TO DEFEND AGAINST RISKS POSED BY**
2 **THE USE OF ARTIFICIAL INTELLIGENCE.**

3 (a) SENSE OF CONGRESS.—It is the sense of Con-
4 gress that the development and use of artificial intelligence
5 in the commission of financial crimes by adversarial actors
6 poses a significant risk to the national and economic secu-
7 rity of the United States.

8 (b) STRATEGY TO DEFEND AGAINST RISKS POSED
9 BY MISINFORMATION, FRAUD, AND FINANCIAL CRIME
10 CONDUCTED WITH ARTIFICIAL INTELLIGENCE.—

11 (1) IN GENERAL.—Not later than 180 days
12 after the date of the enactment of this Act and an-
13 nually thereafter, the Secretary of the Treasury, the
14 Secretary of Homeland Security, and the Secretary
15 of Commerce, in consultation with the officials speci-
16 fied in paragraph (3), shall jointly submit to Con-
17 gress a report that includes the following:

18 (A) A description of interagency policies
19 and procedures to defend United States finan-
20 cial markets, United States persons, United
21 States businesses, and global supply chains
22 from the national and economic security risks
23 posed by the use of artificial intelligence in the
24 commission of financial crimes, including fraud
25 and the dissemination of misinformation.

1 (B) An itemized list of readily available re-
2 sources, hardware, software, and technologies
3 that can be immediately utilized to combat the
4 use of artificial intelligence in the commission
5 of financial crimes, including fraud and the dis-
6 semination of misinformation.

7 (C) An itemized list of resources, hard-
8 ware, software, technologies, people, and budg-
9 etary estimates needed to help Federal depart-
10 ments and agencies to combat the use of artifi-
11 cial intelligence in the commission of financial
12 crimes, including fraud and the dissemination
13 of misinformation.

14 (2) CONSIDERATIONS.—Reports required pur-
15 suant to paragraph (1) shall take the following risks
16 into consideration:

17 (A) Deepfakes.

18 (B) Voice cloning.

19 (C) Foreign election interference.

20 (D) Synthetic Identities.

21 (E) False flags and false signals that dis-
22 rupt market operations.

23 (F) Overall digital fraud.

24 (3) OFFICIALS SPECIFIED.—The officials speci-
25 fied in this paragraph are the following:

1 (A) The United States Trade Representa-
2 tive.

3 (B) The Attorney General.

4 (C) The Chairman of the Board of Gov-
5 ernors of the Federal Reserve System.

6 (D) The Director of the National Institute
7 of Standards and Technology.

8 (E) The Under Secretary of Commerce for
9 Industry and Security.

10 (F) The Chairman of the Securities and
11 Exchange Commission.

12 (c) RECOMMENDATIONS.—Not later than 90 days
13 after each report under subsection (b) is submitted, the
14 Secretary of the Treasury, the Secretary of Homeland Se-
15 curity, and the Secretary of Commerce shall jointly submit
16 to Congress a set of recommendations relating to each
17 such respective report that contain the following:

18 (1) Legislative recommendations to address the
19 risks posed by the use of artificial intelligence in the
20 commission of financial crimes, including fraud and
21 the dissemination of misinformation.

22 (2) Best practices to assist American businesses
23 and government entities with risk mitigation and in-
24 cident response to address the risks posed by the use
25 of artificial intelligence in the commission of finan-

1 cial crimes, including fraud and the dissemination of
2 misinformation.

○

119TH CONGRESS
1ST SESSION

H. R. 1734

To establish the Task Force on Artificial Intelligence in the Financial Services Sector to report to Congress on issues related to artificial intelligence in the financial services sector, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 27, 2025

Ms. PETTERSEN (for herself, Mr. FLOOD, Ms. BONAMICI, Mr. FITZPATRICK, Ms. OCASIO-CORTEZ, and Mr. HARDER of California) introduced the following bill; which was referred to the Committee on Financial Services

A BILL

To establish the Task Force on Artificial Intelligence in the Financial Services Sector to report to Congress on issues related to artificial intelligence in the financial services sector, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Preventing Deep Fake
5 Scams Act”.

6 **SEC. 2. FINDINGS.**

7 The Congress finds the following:

1 (1) Artificial intelligence is being used in new
2 and innovative ways by the financial services sector.

3 (2) Artificial intelligence may provide benefits
4 to banks, credit unions, and banking consumers.

5 (3) Artificial intelligence poses unique threats
6 to the safety and security of customer accounts.

7 (4) Voice banking is offered by many banks for
8 security and convenience reasons.

9 (5) The popularity of social media has made
10 video and audio of potential targets easier to obtain
11 for bad actors. These materials can be exploited to
12 replicate the voices and appearances of other people
13 in pursuit of data theft, identity theft, or fraud.

14 (6) Bad actors could utilize “deep fakes”, in-
15 cluding voice and audio manipulation, to compromise
16 and access a consumer’s financial accounts.

17 **SEC. 3. TASK FORCE ON ARTIFICIAL INTELLIGENCE IN THE**
18 **FINANCIAL SERVICES SECTOR.**

19 (a) ESTABLISHMENT.—There is established a Task
20 Force on Artificial Intelligence in the Financial Services
21 Sector (in this section referred to as the “Task Force”).

22 (b) MEMBERSHIP.—The Task Force shall consist of
23 the following:

24 (1) The Secretary of the Treasury, or a des-
25 ignee, who shall serve as Chair of the Task Force.

1 (2) The Comptroller of the Currency, or a des-
2 ignee.

3 (3) The Chairman of the Board of Governors of
4 the Federal Reserve System, or a designee.

5 (4) The Chairperson of the Federal Deposit In-
6 surance Corporation, or a designee.

7 (5) The Director of the Bureau of Consumer
8 Financial Protection, or a designee.

9 (6) The Chairman of the National Credit Union
10 Administration, or a designee.

11 (7) The Director of the Financial Crimes En-
12 forcement Network, or a designee.

13 (c) REPORT.—

14 (1) IN GENERAL.—Not later than the end of
15 the 1-year period beginning on the date of enact-
16 ment of this Act, the Task Force shall issue a report
17 to Congress containing the contents described in
18 paragraph (3).

19 (2) CONSULTATION.—

20 (A) REQUEST FOR INFORMATION.—Not
21 later than 90 days after the date of enactment
22 of this Act, the Task Force shall solicit public
23 feedback on the report required under para-
24 graph (1).

1 (B) INDUSTRY AND EXPERT STAKE-
2 HOLDERS.—In developing the report required
3 under paragraph (1), the Task Force shall seek
4 out and consult with industry and expert stake-
5 holders, including—

6 (i) depository institutions of varying
7 asset sizes;

8 (ii) credit unions of varying asset
9 sizes;

10 (iii) third-party vendors who use arti-
11 ficial intelligence when providing services
12 to depository institutions and credit
13 unions; and

14 (iv) artificial intelligence experts.

15 (3) CONTENTS.—The contents of the report are
16 the following:

17 (A) A description of how banks and credit
18 unions proactively protect themselves and con-
19 sumers from fraud utilizing artificial intel-
20 ligence.

21 (B) A list of standard definitions for the
22 different manners in which artificial intelligence
23 is used, including terms like “generative AI”,
24 “machine learning”, “natural language proc-
25 essing”, “algorithmic AI”, and “deep fakes”.

1 (C) A description of potential risks that
2 could result from the use of artificial intel-
3 ligence by bad actors to steal consumers' data,
4 steal consumers' identities, and commit fraud.

5 (D) A list of best practices for financial in-
6 stitutions to protect their customers from at-
7 tempts to steal consumer data, steal consumers'
8 identities, or commit fraud.

9 (E) Legislative and regulatory rec-
10 ommendations for the regulation of artificial in-
11 telligence and to protect consumers from data
12 theft, identity theft, and fraud.

13 (d) TERMINATION.—The Task Force shall terminate
14 90 days after the final report is issued pursuant to sub-
15 section (c).

○

[DISCUSSION DRAFT]119TH CONGRESS
1ST SESSION**H. RES. _____**

Expressing the sense of the House of Representatives with respect to the use of artificial intelligence in the financial services and housing industries.

IN THE HOUSE OF REPRESENTATIVES

M____ submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Expressing the sense of the House of Representatives with respect to the use of artificial intelligence in the financial services and housing industries.

Whereas generative artificial intelligence (“AI”) has the potential to provide significant opportunities as well as risks across the financial services and housing industries;

Whereas AI is playing a significant role in the financial services and housing industries and continues to be adopted in various forms;

Whereas regulatory sandboxes are an important policy tool for unlocking the potential of AI to improve Americans’ financial lives while mitigating relevant risks and expand-

ing knowledge of governance and regulatory best practices;

Whereas the United States capital markets market participants are leveraging AI to enhance research capabilities, market surveillance, and trading and execution;

Whereas the United States housing market participants are using AI to enhance underwriting, mortgage servicing, and tenant screening;

Whereas United States financial institutions are exploring the use of AI to enhance customer service capabilities, expand the pool of loan applicants, increase repayment rates, and decrease fraudulent payments;

Whereas United States financial firms are leveraging AI to streamline compliance with the Bank Secrecy Act and sanctions laws as well as enhance cybersecurity operations from evolving threats;

Whereas the use of generative AI is enhancing both employee productivity and consumer experiences across the financial services and housing industries;

Whereas regulators should understand any financial stability risks related to financial institutions' growing use of AI;

Whereas AI can be exploited by malicious actors;

Whereas the use of AI in automated decision-making does not relieve financial institutions from their obligations under anti-discrimination laws, and may lead to explainability challenges due to the complexity and opacity of certain AI models;

Whereas small community financial institutions, such as rural depository institutions, minority depository institutions, and community development financial institutions may

lack the resources to develop, train, and deploy AI models compared to larger institutions;

Whereas financial institutions' use of AI may increase their direct and indirect reliance on third-party services; and

Whereas markets should determine the most valuable use cases for AI in financial services and housing, with risk-based regulatory and legislative guardrails provided where necessary: Now, therefore, be it

1 *Resolved*, That it is the sense of the House of Rep-
2 resentatives that—

3 (1) given the critical role of the financial and
4 housing markets, the Committee on Financial Serv-
5 ices of the House of Representatives should play a
6 leading role in making public policy regarding the
7 adoption of AI in the financial services and housing
8 industries;

9 (2) the Committee on Financial Services should
10 consider how to promote a dynamic, pro-innovation
11 culture for AI across the financial services and hous-
12 ing industries;

13 (3) the Committee on Financial Services must
14 ensure regulators apply and enforce existing laws,
15 including anti-discrimination laws, and assess regu-
16 latory gaps and undue burdens as market partici-
17 pants adopt AI;

1 (4) the Committee on Financial Services must
2 ensure regulators assess the impact on innovation
3 and cost effectiveness before issuing AI-related rules;

4 (5) the Committee on Financial Services must
5 ensure any regulatory framework related to AI does
6 not disproportionately burden smaller firms and is
7 tailored to all sizes of market participants;

8 (6) the Committee on Financial Services should
9 ensure the financial regulators have the appropriate
10 focus and tools to oversee new products and services;

11 (7) the Committee on Financial Services should
12 continue to consider how to reform data privacy laws
13 for financial institutions and firms given the impor-
14 tance of data to AI;

15 (8) the Committee on Financial Services should
16 continue to consider how to strengthen cybersecurity
17 standards for AI systems;

18 (9) the Committee on Financial Services should
19 work with financial regulators to understand AI's
20 impact on the workforce; and

21 (10) the Committee on Financial Services
22 should ensure United States global leadership on AI
23 development and use.

[DISCUSSION DRAFT]119TH CONGRESS
1ST SESSION**H. R.** _____

To require the Secretary of the Treasury to carry out a study on best practices for sharing data and results from regulatory sandboxes related to the use of artificial intelligence tools, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To require the Secretary of the Treasury to carry out a study on best practices for sharing data and results from regulatory sandboxes related to the use of artificial intelligence tools, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Artificial Intelligence
5 Innovation Sandbox Information Generation and Harmo-
6 nization of Testing Act” or the “AI INSIGHT Act”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **ARTIFICIAL INTELLIGENCE.**—The terms
4 “artificial intelligence” and “AI” have the meaning
5 given the term “artificial intelligence” in section
6 5002 of the National Artificial Intelligence Initiative
7 Act of 2020 (15 U.S.C. 9401).

8 (2) **COVERED AI SANDBOXES.**—The term “cov-
9 ered AI sandboxes” means Federal programs involv-
10 ing regulatory waivers, modifications, and alternative
11 compliance methods for projects making substantial
12 use of artificial intelligence within the jurisdiction of
13 one or more financial regulatory agencies.

14 (3) **FINANCIAL REGULATORY AGENCIES.**—The
15 term “financial regulatory agencies” means the Of-
16 fice of the Comptroller of the Currency, the Board
17 of Governors of the Federal Reserve System, the
18 Federal Deposit Insurance Corporation, the National
19 Credit Union Administration, the Securities and Ex-
20 change Commission, the Department of Housing and
21 Urban Development, and the Federal Housing Fi-
22 nance Agency.

23 **SEC. 3. SENSE OF CONGRESS.**

24 It is the sense of Congress that:

25 (1) Regulatory sandboxes are an important pol-
26 icy tool for unlocking the potential of artificial intel-

1 ligence to improve Americans' financial lives while
2 mitigating relevant risks and expanding knowledge
3 of governance and regulatory best practices.

4 (2) Data generated by real-world experience
5 governing the application of artificial intelligence
6 tools, including agentic systems, to financial services
7 will be critical to advancing governance and regu-
8 latory best practices.

9 (3) Expanding and applying knowledge of gov-
10 ernance and regulatory best practices for the appli-
11 cation of artificial intelligence tools, including
12 agentic systems, to financial services will be ad-
13 vanced by mechanisms and standards for sharing
14 the results of regulatory sandboxes.

15 (4) The data generated by regulatory sandboxes
16 should be leveraged for the benefit of both public
17 and private sector learning regarding governance
18 and regulatory best practices.

19 (5) An appropriate framework for sharing the
20 data from regulatory sandboxes, including maintain-
21 ing the privacy and security of that data, will in-
22 crease the benefits to public and private sector par-
23 ticipants.

1 **SEC. 4. REPORT TO CONGRESS.**

2 (a) STUDY.—The Secretary of the Treasury shall
3 carry out a study on best practices for sharing with the
4 public and private sectors data and results collected and
5 learned by participants and regulators involved in covered
6 AI sandboxes in the course of such sandboxes analyzing—

7 (1) appropriate standards for maintaining the
8 privacy and security of data generated by such
9 sandboxes, including—

10 (A) those required under applicable law;

11 (B) reasonable expectations of confiden-
12 tiality for proprietary and commercially sen-
13 sitive data and intellectual property; and

14 (C) standards promulgated by industry
15 self-regulatory organizations and Federal agen-
16 cies;

17 (2) appropriate standards for collecting, trans-
18 mitting, processing, and publishing data generated
19 by such sandboxes, which shall consider—

20 (A) allocation of responsibility between and
21 among participants and regulators involved in
22 such sandboxes for collecting, transmitting,
23 processing, and publishing such data;

24 (B) the importance of open-source and
25 publicly accessible data and results;

1 (C) platforms and frameworks that facili-
2 tate analysis of data and efforts to reproduce
3 results, including automated cloud-enabled labs;

4 (D) efforts by private sector organizations
5 and research institutions to harmonize such
6 standards; and

7 (E) best practices from public-private part-
8 nerships in research data sharing, including for
9 aggregating and anonymizing data;

10 (3) appropriate tools and standards for meas-
11 uring, evaluating, and interpreting the results and
12 efficacy of sandboxes and related test projects, which
13 shall consider—

14 (A) guidelines and resources published by
15 Federal agencies related to AI evaluations;

16 (B) guidelines and resources published by
17 private sector organizations and research insti-
18 tutions related to AI evaluations; and

19 (C) best practices for independent valida-
20 tion and reproducibility of data and results; and

21 (4) how the application of artificial intelligence
22 tools and related technologies, including agentie sys-
23 tems, can facilitate and support the analysis and im-
24 plementation of standards, tools, and methods de-
25 scribed in paragraphs (1) through (3).

1 (b) CONSULTATION.—In carrying out the study re-
2 quired under subsection (a), the Secretary of the Treasury
3 shall—

4 (1) consult with the financial regulatory agen-
5 cies; and

6 (2) seek input from private sector stakeholders,
7 including academics, technologists, and industry rep-
8 resentatives with relevant expertise in artificial intel-
9 ligence and data sharing standards.

10 (c) REPORT.—Not later than 1 year after the date
11 of enactment of this Act, the Secretary of the Treasury
12 shall submit to the Committee on Financial Services of
13 the House of Representatives and the Committee on
14 Banking, Housing, and Urban Affairs of the Senate a re-
15 port that includes the results of the study required by sub-
16 section (a).

[DISCUSSION DRAFT]

119TH CONGRESS
1ST SESSION

H. R. _____

To require certain supervisory agencies to assess their technological vulnerabilities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. STUTZMAN introduced the following bill; which was referred to the Committee on _____

A BILL

To require certain supervisory agencies to assess their technological vulnerabilities, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Fostering the Use of
5 Technology to Uphold Regulatory Effectiveness in Super-
6 vision Act”.

7 **SEC. 2. FINDINGS.**

8 Congress finds the following:

1 (1) Banking regulators continue to examine and
2 monitor depository institutions without sufficient ac-
3 cess to real-time information.

4 (2) Supervisory regulators should leverage tech-
5 nologies to more effectively carry out their duties.

6 (3) When updating supervisory technology,
7 risks surrounding technology procurement must be
8 effectively managed.

9 (4) Agencies' reliance on outdated technology
10 can create vulnerabilities for the financial system,
11 through—

12 (A) difficulties in collecting, compiling, and
13 analyzing relevant information about risks and
14 noncompliance at supervised firms;

15 (B) reliance on information that is inac-
16 curate, incomplete, or not timely;

17 (C) reliance on limited and outdated tools
18 for data analysis;

19 (D) difficulties in using data to identify
20 risk trends;

21 (E) difficulties in producing accurate and
22 timely reports;

23 (F) inadequacy of cybersecurity safe-
24 guards; and

25 (G) failure to detect illegal activities.

1 (5) The rapid expansion of financial firms' use
2 of artificial intelligence may generate opportunities
3 to improve the financial system while also intro-
4 ducing a range of risks, making it essential that
5 agencies be equipped with the technology, expertise,
6 and skills needed to analyze these opportunities and
7 potential risks.

8 (6) While agencies assess their supervisory ca-
9 pabilities on an ongoing basis, it is imperative that
10 there be a unified goal of enhancing supervisory
11 technologies that ensure effective and sustainable
12 oversight.

13 **SEC. 3. TECHNOLOGICAL VULNERABILITIES AND PRO-**
14 **CUREMENT PRACTICES ASSESSMENT.**

15 (a) IN GENERAL.—

16 (1) TECHNOLOGICAL VULNERABILITIES ASSESS-
17 MENT.—Each covered agency shall, not later than
18 180 days after the date of the enactment of this sec-
19 tion, assess how existing technologies used by the
20 covered agency inhibit the covered agency from con-
21 ducting adequate, real-time supervisory assessments
22 of entities over which the covered agency has super-
23 visory authority. Such technologies include—

24 (A) core information technology infrastruc-
25 ture;

1 (B) technologies used to supervise entities;

2 (C) technologies for monitoring general
3 market risks using reported data and external
4 data; and

5 (D) technologies for data collection, stor-
6 age, processing, and security.

7 (2) PROCUREMENT PRACTICES ASSESSMENT.—

8 Each covered agency shall, not later than 180 days
9 after the date of the enactment of this section—

10 (A) assess the procurement rules and pro-
11 tocols adhered to by such covered agency when
12 such covered agency acquires or develops new
13 technological systems; and

14 (B) identify any opportunities to further
15 streamline procurement rules and protocols, in-
16 cluding an assessment of the impact such rules
17 or protocols have on the ability of the covered
18 agency to test new technological systems.

19 (b) REPORT.—Not later than 1 year after the comple-
20 tion of the assessments required under subsection (a), and
21 every 5 years thereafter, the covered agencies shall coordi-
22 nate and jointly submit to the Committee on Financial
23 Services of the House of Representatives and the Com-
24 mittee on Banking, Housing, and Urban Affairs of the
25 Senate, in a manner that does not pose a risk to the integ-

1 rity or security of any technologies, systems, or capabili-
2 ties of covered agencies, regulated entities, or market par-
3 ticipants, a report that includes the following with respect
4 to each covered agency:

5 (1) A general overview of hardware and soft-
6 ware used for information gathering and advanced
7 analytics during supervision activities, including cat-
8 egories of technology purchased from vendors and
9 developed by the covered agency or contractors of
10 the covered agency.

11 (2) A description of the procurement practices
12 and protocols of the covered agency, including a de-
13 scription of—

14 (A) whether such processes are voluntarily
15 adhered to or mandated; and

16 (B) any opportunities to further streamline
17 procurement rules and protocols, including an
18 assessment of the impact such rules or proto-
19 cols have on the ability of the covered agency
20 to test new technological systems.

21 (3) A general overview of the portion of the
22 workforce of the covered agency that is engaged ma-
23 terially in technology development within the covered
24 agency, including—

1 (A) an overview of the ability of the cov-
2 ered agency to recruit and retain appropriate
3 technology experts; and

4 (B) a description of the degree to which
5 the covered agency relies on contractors to de-
6 sign, develop, or deploy technology and perform
7 technology-related tasks.

8 (4) A general description of the processes used
9 by the covered agency to obtain information from
10 entities supervised by the covered agency and any
11 impediments thereto, including regulatory obstacles.

12 (5) General information about market and tech-
13 nology trends and risks in the underlying regulated
14 markets including—

15 (A) market developments influenced by the
16 adoption of new technologies;

17 (B) the use of new technologies by super-
18 vised entities for compliance and risk manage-
19 ment purposes;

20 (C) the impact of new technologies on the
21 collection, analysis, and reporting of regulatory
22 data, including on data quality, interoperability,
23 and standardization; and

24 (D) potential risks, including risks of illicit
25 activity, related to new technologies.

1 (ii) estimates of any potential cost re-
2 ductions.

3 (d) COVERED AGENCY DEFINED.—In this section,
4 the “covered agency” means the Board of Governors of
5 the Federal Reserve System, the Federal Deposit Insur-
6 ance Corporation, the Department of the Treasury, includ-
7 ing the Office of the Comptroller of the Currency and the
8 Financial Crimes Enforcement Network, the Federal
9 Housing Finance Agency, and the National Credit Union
10 Administration.