

# Remarks by Assistant Secretary for Financial Institutions Graham Steele at the Amazon Web Services (AWS) Gov2Gov Summit on Responsible Artificial Intelligence Innovation for the Public Sector

October 24, 2023

*As Prepared for Delivery*

## INTRODUCTION

Good morning,

Thank you for having me. I appreciate AWS hosting events like today's to promote a better understanding of responsible Artificial Intelligence (or "AI") and Machine Learning (or "ML") practices and to foster discussions among government officials to address the challenges and opportunities in this area.

As the Assistant Secretary for Financial Institutions, I am responsible for the Treasury's policy views on matters affecting banks, credit unions, insurance, consumer protection, access to capital, and financial sector cybersecurity. At the same time, as a longtime resident of the San Francisco Bay Area who has worked near the epicenter of the U.S. technology sector in Silicon Valley, technological innovation in financial services has long been of great interest to me.

Financial institutions are increasingly becoming technology companies—from the use of mobile apps to digital payment services to models that assess the risks of certain activities or the creditworthiness of certain customers. As with other areas experiencing rapid innovation, such as fintech and cloud services, significant potential exists for financial institutions to harness the technology underlying AI products and services. However, there are also risks, including inadequate oversight and consumer harms. Treasury is actively engaged, including by coordinating with the official sector and other stakeholders, to ensure we achieve outcomes that benefit all Americans and our economic values of fairness, growth, and competitiveness.

Today, I will begin by discussing our productive work with AWS on cloud computing. Then I will share my views on some of the potential benefits and risks of AI that we at Treasury have been thinking about, including in the consumer finance and insurance industries. Finally, I am going to touch on how federal and some state policymakers are looking at these issues.

## **CLOUD COMPUTING AND AWS**

As we know, cloud computing is no longer a nascent or emerging technology. It now supports some of the financial services sector's most critical financial institutions, while providing security and operational resiliency for these institutions. Following the publication of Treasury's report on the financial sector's adoption of cloud services in February 2023, we have engaged key cloud service providers (or "CSPs"), like AWS, as we take our next steps to ensure that financial institutions mature in their adoption of cloud services in a responsible manner.

As we said in the report, when implemented properly, cloud services can offer more scalable and resilient solutions than when firms handle these services in house. However, financial institutions have expressed to us that they have been struggling with a lack of transparency and negotiating power disadvantages as they contract with the largest CSPs, which comprise a significant share of the cloud services market. This hinders their ability to clearly understand and implement the services they are purchasing and the level of security being provided to them, and to negotiate for solutions that are specific to their enterprise or security needs.

By bringing CSPs into the fold alongside other private sector and regulatory stakeholders, we are working toward establishing a more transparent model that places less pressure on cloud customers and asks CSPs to take more responsibility for the security of those customers.

Through its work with the Cloud Executive Steering Group (or "CESG"), AWS is helping advance the effort toward greater transparency and responsible technology innovation and implementation within the financial services sector.

The Cyber Risk Institute's Cloud Adoption Profile, and subsequent update to that work through the CESG Cloud Profile Refinement & Adoption workstream, has helped lay the groundwork to establish a common language that will facilitate greater understanding and accessibility for financial institutions considering cloud adoption. This framework is unique in its focus on both technical controls and regulatory policies, with tiered security protocols tailored to the type of data that institutions either own or provide to third party service

providers. The trust established through this type of transparency is a useful model for what responsible innovation can look like.

With the work we are now undertaking, we are moving to a model that should empower financial institutions of all sizes to unbundle one-size-fits-all cloud service packages and enable them to better negotiate for solutions that best suit their operational footprints and individualized risk assessments.

## **POTENTIAL BENEFITS AND RISKS OF AI IN FINANCIAL SERVICES**

Turning to AI, Treasury continues to actively monitor the implications of AI on the financial services sector. Financial institutions have been using automated systems for decades, and Treasury and federal regulators have long been engaged on this issue. However, newer forms of AI have become increasingly prevalent in financial services in recent years, powered by more advanced algorithms and data storage and processing power improvements in the underlying cloud technology. Of course, as this group knows well, the broad term “AI” encompasses many different types of technologies and processes, and therefore has many potential applications.

AI may offer benefits, such as reducing costs and improving efficiencies, identifying more complex relationships, and improving performance and accuracy. Financial institutions currently use AI for various tasks, ranging from fraud prevention and detection to customer service, document review, and retail credit underwriting. Some institutions use AI extensively, while others take a more limited approach. Even within a single institution, AI may be used to varying degrees in different areas.

However, the adoption of AI raises certain risks, which fall into three broad categories: (1) risks arising from the design of AI; (2) risks arising from how humans use or deploy AI; and (3) operational and cyber risks of AI.

In the first category, the opacity of certain AI models can create challenges in explaining how the technology produces its output. This could produce, and possibly mask, biased or inaccurate results that could, in turn, implicate consumer protection issues such as fair lending. It’s important to consider how providing transparency into AI models can allow organizations and regulators to better assess the systems’ conceptual soundness and remove uncertainty about their suitability and reliability.

In the second category, the use of flawed internal models can cause significant model risk management issues. As the financial crisis of 2007-09 and other failures of financial institutions, like Long-Term Capital Management, have shown, the overreliance on faulty risk models can have financial stability implications. As a result, the post-crisis prudential regulatory framework has sought to move toward more standardized risk measurements. It is important to consider these historical lessons regarding the broader use of models by financial institutions and regulators as we evaluate specific use cases for AI models.

Finally, in the third category, the high volumes and wide range of data consumed by AI, particularly generative AI, makes controls around data quality, suitability, and security and privacy vital for ensuring that AI is sound. As referenced in the national cyber strategy, responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product. CSPs that play a major role in storage and processing of big data today can and should lead the effort to develop and establish necessary controls.

Let me now turn to a couple of specific applications for AI in financial services, in order to put a finer point on some of the risks and benefits that I have just outlined.

## **AI IN CONSUMER FINANCE**

In a November 2022 report focusing on the impact of non-bank firms on the consumer finance marketplace, Treasury noted that fintech firms have garnered attention for their leveraging of advances in technologies—including AI/ML—and newly available data, as well as business models differentiated from depository institutions, all of which they often cite as enabling them to enhance credit underwriting and expand access to credit. Specifically, market participants claim that they are enhancing capabilities to assess creditworthiness and thus expand access; reducing discrimination in credit decision-making; and, in some segments, enabling firms to offer more affordable credit than existing alternatives accessible to consumers. While there is some limited evidence to suggest that fintech firms are serving more customers at different and sometimes lower price-points, this may be due to a variety of factors, including competitive dynamics, business decisions, different cost-structures, marketing, or use of AI/ML technologies or newly available data in underwriting models.

At the same time, the report also noted that new uses of data and technology—including AI—could create the potential for new forms of discrimination, including increased opportunities

for predatory targeting and price discrimination. The report highlighted concerns related to the opacity of AI models and difficulty of explaining outputs, which poses challenges for compliance with fair lending requirements. The report also noted the potential for such models to perpetuate discrimination by utilizing and learning from data, including proxy data, that might reflect and reinforce historical biases.

The November 2022 report also highlighted general concerns that the large amount of consumer data being collected and used in AI applications poses broad societal surveillance and privacy risks. The report pointed to the use of alternative data and observed that including alternative data on consumers' non-financial behavior in financial decision making, such as in AI-enabled credit underwriting, could lead to growing amounts of consumer behavior being subject to commercial surveillance. This could be disruptive to consumers' lives and have unintended and unforeseen consequences across the economy. With the increasing prevalence of collection and utilization of consumers' data, there are concerns about a potential lack of a meaningful choice in financial services for consumers seeking to protect their privacy, both for those that feel compelled to agree, but also for those who opt out.

There are important policy discussions that need to happen to ensure we address these and other concerns related to the use of AI in the provision of consumer financial services.

## **AI AND THE INSURANCE SECTOR**

Next, I would like to talk about how AI has the potential to transform the insurance sector.

The National Association of Insurance Commissioners (or "NAIC") recently found that 88 percent of surveyed private passenger auto insurers use, plan to use, or plan to explore using AI/ML, with the most use in claims, marketing, and fraud detection. By comparison, approximately 70 percent of surveyed homeowners insurers use or plan to use AI /ML, with the greatest use in claims, underwriting, marketing, fraud detection, and rating.

AI can streamline the function and lower the cost of nearly every aspect of the insurance business, including claims, underwriting, customer service, marketing, fraud detection, and rating. At the same time, as with consumer financial services, the incorporation of AI in insurance raises privacy concerns and the risk of unlawful consumer discrimination.

For example, as the most recent annual report from Treasury's Federal Insurance Office (or "FIO") notes, property and casualty insurers increasingly use telematics, which is a method of monitoring vehicles with GPS technology and on-board diagnostics to gather data on a

multitude of factors such as miles driven, speeding, hard stops, and cell phone use while driving. Through AI, auto insurers can estimate the risk of an accident more accurately than with traditional underwriting. Insurers can also use the miles driven data to better customize insurance plans so that consumers only pay for what they need. In addition, AI can augment the claims management process in homeowners insurance by quickly assessing the severity of damage to property and predicting the repair costs from historical data, sensors, and images.

AI has the potential to align insurance premiums more closely with individualized data, ease the claims process, and make underwriting more efficient. All of this can mean greater affordability and equity in the cost and availability of insurance coverage, provided these new tools are used appropriately.

As I noted earlier, there may be privacy issues with these uses of AI, because they require collecting significant amounts of consumers' personal information. For instance, many telematics programs require access to a policyholder's smartphone and can track the user's location, whether or not the user is actually driving.

Life insurers are increasingly using AI to accelerate their underwriting process. AI can quickly identify an applicant's health risks and corroborate information, skipping the medical exams and slow "back and forth" exchange of information typical in a traditional underwriting process.

However, if an AI model is trained on data with biases, it is likely to perpetuate them in its decision-making process. For example, algorithmic bias in AI may unfairly calculate higher premiums for a specific racial group with historically higher mortality rates, even if individual risk factors differ.

More generally, the increased use of consumer data, particularly the use of non-driving data as proxies in automotive insurance policies, is raising important questions about the proper collection and use of consumer data in insurance underwriting.

In both consumer finance and insurance, it is important to center equity concerns and remain aware of the potential disparities that could be created or reinforced if new products and services like AI are designed or implemented without adequately accounting for the concerns and needs of the most vulnerable and marginalized. As Secretary Yellen has said, "just as much as we need responsible innovation, we also need equitable innovation."

## **ACTIONS BY POLICYMAKERS**

Policymakers are addressing privacy and discrimination concerns with AI at both the federal and state level. In September, a bipartisan group of senators convened the first in a series of AI Forums in D.C. The series brings together lawmakers with Big Tech, unions, civil rights advocates, and other stakeholders to discuss AI regulation. Also in September, the Biden-Harris Administration announced that 15 companies had agreed to voluntary safety and security standards for their AI tools. These voluntary commitments are an important step and a bridge to further action. As the President has said, the Administration is currently developing an executive order that will help advance responsible AI and manage its risks.

These efforts build on the 2022 release of the White House's Blueprint for an AI Bill of Rights, which established a set of five principles and associated practices to help guide the design, use, and deployment of AI systems to protect the rights of consumers. One principle, aimed at preventing algorithmic discrimination, suggests proactive assessments of algorithms and ongoing disparity testing and mitigation. Another principle, addressing data privacy, recommends that data collection conform to consumers' reasonable expectations and that only data strictly necessary for the specific context is collected. And as many of you know, NIST released an AI Risk Management Framework with detailed recommendations for organizations to manage and mitigate AI risks.

With respect to insurance, FIO is monitoring related action at the state level as well.

Colorado, for example, enacted legislation to require insurers to test their algorithms, predictive models, and information sources to ensure that they do not unfairly discriminate against protected classes. The NAIC adopted Principles on Artificial Intelligence which emphasize the importance of the ethical use of AI. And, beginning in 2021, the NAIC began surveying insurers to learn how AI and machine learning techniques are currently being used and what governance and risk management controls are in place.

Finally, some financial regulatory agencies are taking steps to address broader acts and practices that will have implications for financial institutions' use of AI. As an example, the Consumer Financial Protection Bureau (or "CFPB") is considering regulatory proposals relating to data brokers and data boundaries, in order to enhance transparency and hold covered entities accountable for their data practices. Treasury has previously recommended that the CFPB consider whether and how it may directly supervise data aggregators, who store vast and ever-growing amounts of consumer financial data, generally without the kind of supervision of their data practices applicable to regulated depository institutions.

The banking agencies have also issued guidance regarding the oversight of bank partnerships with third parties, which could include firms offering AI products and services. Regulatory and supervisory expectations to address model risk management and prevent discrimination or bias can also help to address some of the risks associated with AI and promote responsible innovation that ultimately benefits consumers.

## CLOSING

I'd like to close by again thanking AWS for convening this group and inviting me into this important set of conversations that no doubt will continue. I hope this has been a useful discussion of both the benefits and risks of AI adoption in the financial services sector.

I would also like to make an observation—perhaps one that is both obvious and, some might say, maybe even a little naïve, but I think is nonetheless important to remember. As we continue to think about the evolution of AI in the financial services space, we all—from the private sector companies that design and utilize AI to the public sector policymakers that construct and enforce the rules of the road—must remember that human beings are ultimately responsible for designing the information that goes in, the ways that information is processed, and how the resulting output is used.

The Treasury Department will continue to monitor the use of AI in financial services and prioritize this issue. We are committed to the responsible innovation and appropriate regulation of technologies that are accurate and fair, protect privacy and security, and advance the financial wellbeing of the American people.

Thank you again for your time.

###