
August 12, 2024

Moses Kim
Director, Office of Financial Institutions Policy
United States Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

**RE: FR Doc. 2024-12336 (Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence)**

The African American Alliance of CDFI CEOs (the Alliance) is pleased to submit comments regarding the uses, opportunities, and risks of Artificial Intelligence (AI) in the financial services sector. The Alliance is a national membership-based organization with a mission to empower Black communities by promoting economic stability, wellbeing, and wealth. Leveraging a network of 80 Black-led Community Development Financial Institutions (CDFIs), the Alliance is working towards establishing power and promoting equal economic opportunity for Black individuals, families, and communities across all 50 states.

* * *

**A. *General Use of AI in Financial Services***

> ***A.1. Is the definition of AI used in this RFI appropriate for financial institutions? Should the definition be broader or narrower, given the uses of AI by financial institutions in different contexts?***

The current definition of artificial intelligence (AI) in the Request for Information (RFI) is:

*"The term 'artificial intelligence' or 'AI' has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."*

However, this definition could be further refined to better reflect the specific needs of institutions like CDFIs, which serve underserved and low-income communities. These organizations often

employ unique data sources and applications tailored to their target populations. Broadening the definition slightly could ensure it encompasses all the potential ways CDFIs may use AI. One way to improve the definition is by explicitly mentioning the use of non-traditional and alternative data sources. Non-traditional data sources refer to information not typically found in standard credit files. This might include rental payment history, utility bills, and other regular payment records that can demonstrate financial responsibility. Alternative data can also encompass educational background, employment history, social media activity, and other behavioral data that provide a broader picture of an individual's creditworthiness and economic behavior. These types of data are especially useful for assessing creditworthiness in communities that are typically underserved by traditional financial metrics.

Additionally, emphasizing the focus on community impact and financial inclusion would align the definition more closely with the core mission of CDFIs. Highlighting the adaptability and flexibility of AI systems to local contexts and diverse economic conditions would also be beneficial.

Finally, the definition should consider the economic feasibility of AI technologies for small and community-based financial institutions. Ensuring that AI technologies are affordable and accessible is key for inclusive financial innovation, and the inclusion of a clause that highlights the need for AI technologies to be economically viable for smaller institutions will support broader access to these advanced tools.

Here is a suggested expanded definition:

*"Artificial intelligence (AI) refers to a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. These systems utilize machine and human-based inputs to perceive real and virtual environments, abstract these perceptions into models through automated analysis, and use model inference to formulate options for information or action. These systems should also be capable of integrating non-traditional and alternative data sources to enhance their applicability across diverse contexts and should be designed to be adaptable and economically feasible to ensure inclusive access and innovation."*

***A.2. What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?***

The extent and sophistication of AI usage across CDFIs vary significantly. Some CDFIs are making substantial progress in integrating AI technologies, but overall adoption remains limited due to resource constraints and the need for specialized expertise.

A few CDFIs have started using machine learning models for predictive analytics and credit risk assessment. These supervised learning models analyze historical data to predict future trends, which can be incredibly useful. However, not many institutions have widely adopted these technologies yet. On the customer service front, some CDFIs have implemented chatbots and virtual assistants powered by natural language processing. These tools provide 24/7 support and handle basic inquiries, but, again, they are not yet a common feature across the sector.

Predictive analytics and advanced fraud detection algorithms are being explored to enhance risk management and security, primarily in CDFIs that are more substantially resourced. These tools are helpful for identifying potential risks and detecting fraudulent activities, protecting both the institution and its clients. However, many CDFIs still rely on traditional methods due to limited access to advanced technologies and the necessary expertise to implement them effectively.

When it comes to capital markets activities, AI integration is minimal. CDFIs typically focus on community-level impact rather than large-scale investments, which limits the application of AI in investment analysis and trade execution. Some benefits are seen in internal operations through process automation, but many CDFIs still depend on manual or semi-automated processes.

Improvements in customer service through AI, such as chatbots and virtual assistants, are just starting. While these technologies have the potential to enhance customer engagement and satisfaction, broader implementation will take time and investment.

Regulatory compliance is another area where AI could be beneficial, but most CDFIs currently follow manual compliance processes. Automating compliance monitoring and reporting could offer significant efficiency gains, but adoption remains low. Similarly, AI-driven marketing efforts are not widely used; most CDFIs employ straightforward and less data-driven marketing strategies.

Looking to the future, CDFIs see the potential benefits of AI in enhancing financial inclusion, improving risk management, and achieving operational efficiency. However, substantial implementation is still months or years away. Incremental adoption of AI is expected as institutions invest in technological upgrades and build the necessary capacity. Enhancing

customer service and regulatory compliance through AI is a goal, but achieving widespread implementation will require overcoming significant challenges, including financial and technical resource limitations.

While there is growing interest and some progress in adopting AI among CDFIs, current usage is limited and varies across institutions. Many CDFIs are still in the exploratory phase, determining how AI can best serve their mission of providing financial services to underserved communities. Overcoming the barriers to adoption will be crucial for CDFIs to fully leverage AI's potential and enhance their impact.

***A.3. To what extent does the type of AI, the development of AI, or AI applied use cases differ within a financial institution? Are there additional use cases for which financial institutions are applying AI or for which financial institutions are exploring the use of AI? Are there any related reputation risk concerns about using AI?***

CDFIs are increasingly using a variety of AI technologies to enhance their services and streamline their operations. Machine Learning (ML) is one of the key tools CDFIs use. It helps with credit scoring, risk assessment, and customer segmentation by analyzing historical data to predict creditworthiness and identify high-risk applicants. Natural Language Processing (NLP) is used in chatbots and customer service platforms to handle inquiries and guide customers through various processes. Predictive Analytics plays a crucial role in financial forecasting and resource allocation, while Robotic Process Automation (RPA) takes care of repetitive tasks like data entry and compliance checks, allowing staff to focus on more strategic work.

The development of AI solutions in CDFIs varies depending on their size and resources. Larger institutions might develop their own AI models tailored to their specific needs, while many CDFIs turn to third-party solutions provided by fintech companies for their specialized expertise and cost benefits.

AI’s applications within CDFIs are diverse. For credit scoring and risk assessment, AI integrates data from various sources to create comprehensive credit scores for applicants with limited credit histories. Predictive models also help in assessing the risk of loan defaults, which supports informed lending decisions. AI also aids in financial inclusion and outreach by identifying underserved communities and tailoring financial products to meet their specific needs. Predictive analytics helps in designing targeted marketing campaigns to effectively reach potential clients.

However, integrating AI comes with its challenges. There are concerns about bias and discrimination, as AI models might unintentionally perpetuate biases present in historical data.

This can lead to unfair outcomes in credit scoring and lending decisions, affecting CDFI's reputation and possibly drawing regulatory scrutiny. Transparency is also an issue; complex AI models can be difficult to interpret, making it hard to explain decisions to customers and regulators. Data privacy and security are significant concerns as well, with any breaches or misuse of sensitive information potentially harming a CDFI's reputation. Over-reliance on AI might also overshadow human judgment, leading to decisions that don't fully consider unique customer circumstances.

To address these challenges, CDFIs should implement strong measures to detect and correct bias, develop clear and interpretable AI models, and establish robust data governance frameworks. Ensuring human oversight in AI decision-making processes will also help maintain a balance between automation and personalized service.

***A.4. Are there challenges or barriers to access for small financial institutions seeking to use AI? If so, why are these barriers present? Do these barriers introduce risks for small financial institutions? If so, how do financial institutions expect to mitigate those risks?***

Small financial institutions face several significant challenges and barriers when implementing artificial intelligence (AI) technologies. A major hurdle is the high initial investment required. Developing and deploying AI systems require substantial capital for technology, infrastructure, and talent acquisition. These institutions often lack the financial resources to make such investments, and the ongoing costs of maintaining, updating, and scaling AI systems can further strain their limited budgets.

Another critical barrier is the lack of technical expertise. Recruiting skilled AI professionals is both costly and highly competitive. Small financial institutions often find it difficult to attract and retain such talent, which is essential for the successful implementation and maintenance of AI technologies. Moreover, providing ongoing training for existing staff to keep pace with AI advancements adds to the challenge, as these institutions may not have the resources to invest in continuous professional development.

Infrastructure and technology limitations also pose significant obstacles. Many small financial institutions operate on outdated legacy systems that are incompatible with modern AI technologies. Upgrading these systems is both expensive and complex, requiring substantial financial and technical resources. Additionally, limited IT infrastructure can hinder the ability to handle the data processing and computational needs of advanced AI applications, further complicating efforts to adopt these technologies.

Data availability and quality is yet another challenge. Smaller institutions typically have less data available for training AI models, which can impact the accuracy and effectiveness of AI-driven insights. Ensuring data quality and consistency is also challenging without robust data governance frameworks in place, making it difficult for these institutions to leverage AI effectively.

These barriers introduce several risks for small financial institutions. Falling behind larger competitors that leverage AI for better decision-making and customer service can lead to a loss of market share, placing these smaller entities at a competitive disadvantage. Continued reliance on manual processes, due to an inability to adopt AI, results in higher operational costs and inefficiencies. Moreover, without AI, these institutions face higher risks related to fraud, cyber threats, and operational failures, as they lack advanced predictive and preventive measures. Limited ability to harness AI for data analysis also results in poor customer insights, negatively affecting customer satisfaction and retention.

To mitigate these risks, small financial institutions can collaborate with third-party AI service providers to gain access to advanced technologies without significant internal investment. Joining industry consortiums or alliances can also provide access to shared AI resources, helping to reduce costs. These institutions can also utilize cloud-based AI solutions. These platforms lower the barrier to entry by reducing the need for on-premises infrastructure and offering scalable, pay-as-you-go models. Seeking government grants or subsidies aimed at encouraging AI adoption in small businesses can also provide much-needed financial support. Further, focusing investment in specific AI applications that offer the highest return on investment or address the most critical challenges can help manage costs effectively. Similarly, these institutions might consider a phased approach to AI implementation to spread out costs and allow for gradual integration and scaling of AI technologies. Finally, investing in training programs to upskill existing employees in AI and machine learning builds internal expertise over time, reducing reliance on external talent.

**B.** ***Actual and Potential Opportunities and Risks Related to Use of AI in Financial Services***

> ***B.5. What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)? How has AI been used in financial services to improve fair lending and consumer protection, including substantiating information? To what extent does AI***

***improve the ability of financial institutions to comply with fair lending or other consumer protection laws and regulations?***

For CDFIs, a key benefit of AI is how it improves access to financial services. By analyzing large datasets, AI helps CDFIs pinpoint underserved areas and tailor products to meet the specific needs of low-to-moderate income consumers. In addition, AI significantly cuts costs and improves efficiency. Automating routine tasks, such as handling customer service inquiries and processing loan applications, reduces operational expenses and streamlines operations. AI chatbots and virtual assistants can manage a high volume of customer interactions without increasing staff workload, ensuring that CDFIs can serve more clients effectively.

AI enhances risk management by predicting potential defaults and financial risks more accurately through data analysis. This allows CDFIs to better manage risks and offer more sustainable lending products. For example, AI-driven risk assessment tools can detect early warning signs of financial distress, enabling proactive support for borrowers. Moreover, AI enables the creation of personalized financial products that cater to individual consumers' financial behavior and history. AI algorithms can design customized loan repayment plans that fit the cash flow patterns of small business owners in underserved communities. Additionally, AI-driven marketing tools can effectively target potential customers, helping CDFIs reach a broader audience, including those in rural or remote areas. By analyzing social media and other online platforms, AI can identify and engage with potential customers who might be missed by traditional marketing methods.

The benefits of AI are particularly significant for low-to-moderate income consumers and underserved communities. AI can help reduce human biases in lending decisions by relying on objective data and statistical correlations. For instance, AI models that use alternative data sources, like rental and utility payment histories, can provide a more accurate picture of a borrower’s creditworthiness, benefiting communities of color and other underserved groups. AI also promotes financial inclusion by offering tailored products to individuals with limited access to traditional banking services. Furthermore, AI enhances consumer protection by monitoring and detecting fraudulent activities more efficiently, protecting consumers from financial scams and identity theft. AI algorithms can spot unusual transaction patterns and alert consumers and CDFIs to potential fraud in real-time.

From a regulatory compliance perspective, AI is a major help. Automated compliance monitoring systems continuously oversee transactions to ensure they adhere to fair lending laws and regulations, reducing the risk of violations. AI tools can automatically review loan applications to ensure they comply with the Equal Credit Opportunity Act, ensuring non-discriminatory lending practices. AI models can identify and mitigate biases in lending decisions,

ensuring fair treatment for all applicants. For instance, AI-based compliance tools analyze loan approval data to detect patterns of discrimination and suggest corrective actions. Additionally, AI improves customer service efficiency and accuracy, ensuring consumers receive timely and accurate information about their rights and available financial products.

By leveraging AI, CDFIs can better serve low-to-moderate income consumers and underserved communities, fostering financial inclusion and equity.

***B.6. To what extent are the AI models and tools used by financial institutions developed in-house, by third-parties, or based on open-source code? What are the benefits and risks of using AI models and tools developed in-house, by third-parties, or based on open-source code? To what extent are a particular financial institution's AI models and tools connected to other financial institutions' models and tools? What are the benefits and risks to financial institutions and consumers when the AI models and tools are interconnected among financial institutions?***

Developing AI models in-house allows CDFIs to create solutions tailored to their unique needs and mission objectives. This approach gives them the flexibility to make immediate adjustments and fine-tune models as needed. It also enhances data security by keeping sensitive information within the organization, reducing the risk of data breaches. However, in-house development is resource-intensive, requiring significant investment in technology infrastructure, skilled personnel, and continuous maintenance. Smaller CDFIs, in particular, may face difficulties due to limited availability of specialized AI expertise, which can result in less effective models.

On the other hand, third-party development provides access to advanced AI capabilities and specialized knowledge without the need for substantial upfront investment. These solutions can be more cost-effective, especially for smaller CDFIs, and can be easily scaled to meet growing needs. However, this method introduces risks related to data privacy and security since sensitive information is shared with external entities. Additionally, reliance on third-party vendors can create dependencies, making CDFIs vulnerable to changes in vendor services, pricing, or quality. The solutions provided by third parties may also lack the necessary customization to fully align with the specific requirements of the CDFI.

Open-source development offers a cost-effective alternative, with AI models typically available for free or at a lower cost. The open-source community provides continuous improvements, bug fixes, and updates, benefiting from a broad user base. Transparency is another advantage, as open-source code allows for thorough vetting and modifications. However, the quality and reliability of open-source models can vary, and these models may be more susceptible to security

vulnerabilities if not properly managed. The lack of dedicated support and maintenance services may also require CDFIs to invest in internal capabilities to manage and update these models.

Interconnecting AI models and tools with other financial institutions can provide benefits but also propose risks. Such interconnections are often achieved through APIs, data-sharing agreements, and collaborative platforms. Access to a broader data set can significantly enhance the accuracy and robustness of AI models, leading to better insights and more informed decision-making. Collaborative efforts with other institutions can foster innovation by leveraging shared expertise and resources. However, these interconnections also increase exposure to data breaches and privacy violations, given that sensitive information is shared among multiple entities. The interconnected nature of these systems can create systemic risks, where failures or issues in one institution's AI models can propagate and impact others.

***B.7. How do financial institutions expect to apply risk management or other frameworks and guidance to the use of AI, and in particular, emerging AI technologies? What types of testing methods are financial institutions utilizing in connection with the development and deployment of AI models and tools? To what extent are financial institutions evaluating and addressing potential gaps in human capital to ensure that staff can effectively manage the development and validation practices of AI models and tools? What challenges exist for addressing risks related to AI explainability? What methodologies are being deployed to enhance explainability and protect against potential bias risk?***

CDFIs are in the early stages of establishing governance structures that provide oversight for AI projects. In some cases, the board of directors and senior management have begun to take an active role in aligning AI initiatives with institutional goals and ensuring compliance with regulatory requirements. However, the establishment of dedicated AI governance committees, which are more common in larger financial institutions, remains less prevalent among CDFIs due to resource constraints.

Risk management frameworks are critical in mitigating the potential risks associated with AI. CDFIs are gradually integrating AI-related risks into their Enterprise Risk Management (ERM) frameworks. This process involves identifying potential risks, assessing their impact, and implementing strategies to mitigate them. Model Risk Management (MRM) frameworks are also being adopted, although the extent of their implementation varies. Effective MRM involves robust model development practices, independent validation to ensure accuracy and compliance, and continuous monitoring to detect performance issues and emerging risks. Despite these efforts, many CDFIs struggle with the expertise and resources necessary to fully implement comprehensive MRM practices.

Data governance policies are essential for maintaining data quality, integrity, and security. Some CDFIs have implemented basic data governance policies, but these are often less formalized compared to those in larger institutions. Ethical AI policies, which define standards for fairness, transparency, accountability, and privacy, are also rare due to limited resources. Additionally, CDFIs frequently rely on third-party vendors for AI solutions, but robust risk management practices to oversee these relationships are often lacking.

Testing methods are vital to ensure the robustness and reliability of AI models. While the primary purposes of testing include verifying accuracy, performance, fairness, security, and compliance, the extent and rigor of these practices vary widely among CDFIs. Basic cross-validation techniques are used to evaluate model performance on unseen data, but advanced methods like stress testing, which simulates extreme scenarios to assess model robustness, are not typically conducted. Similarly, statistical methods for bias and fairness testing are applied to some extent, but advanced techniques are rarely employed.

Human capital is a major challenge for CDFIs in managing AI technologies. Investment in training programs to upskill staff in data science, machine learning, and ethical AI practices is limited by resource constraints. Recruiting specialized AI talent is also difficult due to budget limitations, leading many CDFIs to rely on external consultants or third-party vendors. Collaboration with academic institutions, industry groups, and AI consortia can provide valuable support and expertise, but such partnerships are not widespread.

While CDFIs are making strides in integrating AI into their operations and adopting risk management frameworks, they face significant challenges due to limited resources, expertise, and the complexity of AI technologies. The practices outlined represent goals that CDFIs are working towards but are not yet fully realized across the sector. It is essential for CDFIs to continue developing these capabilities to leverage the benefits of AI while mitigating its risks and ensuring compliance with regulatory standards and ethical guidelines.

***B.8. What types of input data are financial institutions using for development of AI models and tools, particularly models and tools relying on emerging AI technologies? Are financial institutions using "non-traditional" forms of data? If so, what forms of "non-traditional" data are being used? Are financial institutions using alternative forms of data? If so, what forms of alternative data are being used?***

Traditionally, CDFIs have relied heavily on established data sources like credit scores from major bureaus, financial data including bank statements and tax returns, and basic demographic

details for their credit assessment processes. However, more CDFIs are beginning to consider more non-traditional data sources. For instance, utility payment records and rental payment histories are becoming valuable tools for assessing financial responsibility. These data points can offer insights into an individual's payment behavior that traditional credit scores might miss. While not yet widespread, the use of such data signifies a move towards creating a more inclusive credit assessment framework.

In addition, a smaller percentage of CDFIs are exploring the use of alternative data. Detailed transaction histories from bank accounts provide a deeper understanding of spending behaviors and overall financial health. This transaction data, aggregated from various payment processors and financial apps, can identify patterns crucial for understanding an individual's cash flow and financial stability. Although still in the early stages of adoption, this data holds promise for making credit assessments more comprehensive and accurate.

Despite these advancements, using non-traditional and alternative data presents several challenges. Protecting the privacy and security of this data is a critical concern, given the sensitive nature of the information. Ensuring the accuracy and integrity of diverse data sources requires consistent practices and thorough cleaning processes. Addressing potential biases in AI models is an ongoing challenge, requiring continuous monitoring and testing to ensure AI algorithms do not perpetuate historical biases and discrimination.

***B.9. How are financial institutions evaluating and addressing any increase in risks and harm to impacted entities in using emerging AI technologies? What are the specific risks to consumers and other stakeholder groups, including low- to moderate-income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)? How are financial institutions protecting against issues such as dark patterns— user interface designs that can potentially manipulate impacted entities in decision-making—and predatory targeting emerging in the design of AI?***

The current practices among CDFIs reflect an awareness of AI's potential to enhance financial services but also reveal a sector still in the early stages of fully integrating robust risk management frameworks. In terms of governance and risk management, some CDFIs have started incorporating AI oversight into their existing governance structures. This includes forming committees specifically tasked with monitoring AI implementations. These efforts aim to ensure that AI systems align with the ethical standards and missions of the institutions. However, the extent to which these practices are standardized across the sector varies significantly. Leading CDFIs are also initiating model validation processes, involving regular

stress testing of AI systems to identify and mitigate potential risks. This approach ensures that AI models function as intended and do not introduce unforeseen vulnerabilities.

Bias and discrimination mitigation is another critical area where CDFIs are taking action. A few institutions are conducting comprehensive data audits to uncover and rectify biases within their datasets. This process is essential to prevent AI models from perpetuating historical biases that could lead to discriminatory outcomes in lending and other financial services. Some CDFIs have also started implementing fairness testing, utilizing techniques such as adversarial testing and Less Discriminatory Alternatives (LDA) testing to ensure their AI models treat all demographic groups equitably. However, these practices are not yet universally adopted across all CDFIs.

Transparency and explainability of AI models are emerging priorities for some CDFIs. Efforts are underway to make AI-driven decisions more interpretable, allowing both regulators and consumers to understand how these decisions are made. This is particularly important in areas like credit underwriting, where clear explanations can help build consumer trust and ensure compliance with regulatory requirements.

The ethical design of AI systems remains an area needing further development. While there is limited evidence of systematic efforts to avoid dark patterns in user interface designs, there is growing awareness of the potential for manipulative practices and the need for transparency in user interactions.

Data privacy and security are also a cause for concern for CDFIs using AI. Most institutions comply with basic data privacy standards, but the adoption of advanced techniques like anonymization and encryption specifically for AI systems is not yet widespread. Basic cybersecurity measures are generally in place, but comprehensive protocols tailored to protect AI systems from unauthorized access and data breaches are still in development.

There are also specific risks to consumers and stakeholders associated with AI use in CDFIs. AI models can perpetuate existing biases, leading to discriminatory practices in lending and insurance. Studies from broader fintech sectors indicate that minority borrowers may receive less favorable loan terms due to biased AI models, highlighting similar risks for CDFIs. Extensive data requirements for AI systems also increase the risk of data breaches and misuse of personal information. The reliance on alternative data sources, such as social media data, further raises significant privacy concerns.

There is also the risk of AI being used to target vulnerable consumers with high-risk financial products. Predatory lending practices, although not well-documented within CDFIs, remain a potential concern. Additionally, the complexity of AI models can obscure the decision-making process, reducing transparency and making it difficult for consumers to understand why certain financial decisions were made. This lack of explainability can undermine trust and prevent consumers from addressing issues related to denied loans or other adverse outcomes.

While some CDFIs are making strides in adopting practices to mitigate the risks associated with emerging AI technologies, comprehensive implementation of these strategies is not yet widespread. The sector is still in the early stages of integrating comprehensive risk management, transparency, and ethical design principles. Further development and broader adoption of these practices are necessary to ensure the responsible use of AI in serving low- to moderate-income and underserved communities effectively.

***B.10. How are financial institutions addressing any increase in fair lending and other consumer-related risks, including identifying and addressing possible discrimination, related to the use of AI, particularly emerging AI technologies? What governance approaches throughout the development, validation, implementation, and deployment phases do financial institutions expect to establish to ensure compliance with fair lending and other consumer-related laws for AI models and tools prior to deployment and application? In what ways could existing fair lending requirements be strengthened or expanded to include fair access to other financial services outside of lending, such as access to bank accounts, given the rapid development of emerging AI technologies? How are consumer protection requirements outside of fair lending, such as prohibitions on unfair, deceptive and abusive acts and practices, considered during the development and use of AI? How are related risks expected to be mitigated by financial institutions using AI?***

As stated, most CDFIs are still at an early stage in using AI, and the sophistication of their bias detection methods is often limited, if it exists at all. Advanced techniques like disparate impact analysis, which are crucial for spotting subtle or systemic biases, are not widely adopted due to a shortage of technical expertise and resources.

When it comes to governance throughout the AI lifecycle, few CDFIs have set up comprehensive ethical guidelines specifically for AI. Ethical considerations are often handled informally or on a case-by-case basis rather than being integrated into the development process. Additionally, development teams often lack the diversity needed to fully address ethical and legal issues. Smaller CDFIs, in particular, may not have the resources to bring together interdisciplinary teams that include ethicists, legal experts, and community representatives.

The validation phase also presents challenges. Independent third-party audits, which could provide the necessary rigor and independence, are rare. Instead, internal validation processes are more common but often lack the required rigor. Critical fairness metrics like demographic parity and equal opportunity are not standard practice, as many CDFIs do not have the capacity to implement these metrics effectively. Stakeholder engagement, crucial for gathering feedback and ensuring community needs are met, is inconsistent. Larger CDFIs might have more structured feedback mechanisms, but smaller ones often do not.

In sum, data privacy measures are prioritized but vary in implementation. Larger CDFIs tend to have more advanced protections compared to smaller ones. Regular updates to AI models and training programs are more common in larger institutions, while smaller CDFIs struggle to keep pace with rapid advancements. Stress testing and scenario analysis, essential for predicting and preparing for potential AI model failures or discriminatory outcomes, are not widely adopted due to technical and resource constraints.

***B.12. How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?***

Many CDFIs are still in the early stages of adopting AI-powered systems for fraud detection, relying mostly on traditional methods that don't fully utilize AI's potential. While a few have started using machine learning to identify unusual transaction patterns, this isn't widespread due to resource constraints.

On the data security front, CDFIs generally stick to standard practices like encryption and access controls to protect sensitive information. However, the adoption of advanced AI-specific security measures is limited because of the high costs and complexity involved. Some CDFIs have implemented multifactor authentication (MFA) to enhance security, requiring users to confirm their identity through multiple methods, such as entering a password and a code sent to their phone. Despite this, the use of biometric verification methods, like fingerprint or facial recognition, remains rare due to the significant barriers of cost and technical challenges.

Budget constraints present the biggest challenge. Many CDFIs operate with tight budgets, making it difficult to invest in advanced AI technologies and hire specialized staff for fraud prevention. There is also a significant expertise gap, with many CDFIs lacking in-house knowledge of AI and fraud prevention, leading them to rely heavily on external vendors.

Balancing security with user experience is another critical issue. Implementing security measures like MFA can negatively impact user experience, potentially leading to dissatisfaction and reduced adoption of digital services. Additionally, AI systems can sometimes flag legitimate transactions as fraudulent, requiring additional resources to review these cases—resources that many CDFIs lack.

Regular security audits and software updates are critical for maintaining sound fraud prevention systems. Conducting regular audits and penetration testing helps identify and address vulnerabilities, while keeping fraud detection systems updated with the latest security patches protects against new threats. AI's ability to mimic biometrics like photos, videos, and voices poses a significant challenge. Advanced biometric verification methods and continuous monitoring for inconsistencies in biometric data are necessary countermeasures. Managing third-party risks associated with AI technologies is also critical, requiring thorough due diligence, contractual safeguards, and ongoing monitoring of third-party vendors.

Thus, while CDFIs are taking steps to address and mitigate AI-related fraud risks, they face ongoing challenges. Limited resources, evolving fraud techniques, and the need to balance security with user experience remain significant concerns. Effective fraud prevention requires a comprehensive approach, including collaboration, regular updates, and comprehensive risk management frameworks. More support and resources are needed for CDFIs to effectively combat AI-driven fraud and protect their stakeholders.

***B.15. To the extent financial institutions are relying on third-parties to develop, deploy, or test the use of AI, and in particular, emerging AI technologies, how do financial institutions expect to manage third-party risks? How are financial institutions applying third-party risk management frameworks to the use of AI? What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions? How have these challenges varied or affected the use of AI across financial institutions of various sizes and complexity?***

Managing third-party risks in AI deployment poses challenges for CDFIs. While some foundational practices exist, many CDFIs are still developing comprehensive risk management frameworks.

When it comes to due diligence, many CDFIs find it difficult to thoroughly assess the technical capabilities of AI vendors. Often, they lack the in-house expertise needed to evaluate the complex technical aspects of AI solutions. While regulatory compliance checks are performed,

these tend to be superficial and do not cover a full evaluation of potential risks. Detailed security assessments, crucial for preventing data breaches and unauthorized access, are also often lacking.

In terms of contract management, CDFIs often include basic service level agreements (SLAs), but these often lack specific, enforceable performance metrics. Standard legal terms are generally present, but contracts can easily miss the mark in addressing the unique risks tied to AI deployment. Detailed provisions for data privacy, indemnification, and audit rights are usually not comprehensive, and termination clauses often fail to cover AI-specific scenarios adequately.

Monitoring and evaluation practices involve periodic performance reviews and regulatory audits, but these are usually high-level. Specific key performance indicators (KPIs) related to AI are not consistently tracked, and incident management tends to be reactive rather than proactive. This approach limits the ability to preemptively address potential issues and maintain continuous compliance.

Training and capacity-building efforts are generally focused on raising general AI awareness among staff. Vendor-led workshops occur, but they often lack critical scrutiny from the CDFI's perspective. There is a significant gap in specialized training on AI risk management and technical aspects, hindering the development of a thorough understanding of AI risks. Limited opportunities for knowledge sharing within the industry result in inconsistent practices and a lack of cohesive strategies.

Ethical considerations and governance around AI use in CDFIs are often handled with basic ethical guidelines. However, comprehensive frameworks are typically missing, leading to ad-hoc governance practices. Formal processes to detect and mitigate biases in AI models are notably absent, and governance structures for overseeing AI deployment are not robustly implemented.

Therefore, while CDFIs are making strides in managing third-party risks associated with AI, there are significant gaps in current practices. Comprehensive due diligence, detailed contractual agreements, proactive monitoring, specialized training, and robust ethical governance need substantial improvement. Many CDFIs are still building the capacity and expertise to effectively manage these risks, and current practices often fall short of ensuring safe and ethical AI deployment. Over the next several years, it will be critical for CDFIs to address these gaps in order to fully take advantage of AI's potential while safeguarding against its inherent risks.

***B.16. What specific concerns over data confidentiality does the use of third-party AI providers create? What additional enhancements to existing processes do financial institutions expect to make in conducting due diligence prior to using a third-party***

***provider of AI technologies? What additional enhancements to existing processes do financial institutions expect to make in monitoring an ongoing third-party relationship, given the advances in AI technologies? How do financial institutions manage supply chain risks related to AI?***

When considering the use of third-party AI providers, the possibility of data security breaches is a major worry for CDFIs. Third-party providers may not always uphold the stringent security measures that CDFIs need, making unauthorized access to sensitive financial and personal data more likely. To tackle this, it is necessary to enforce strict security requirements and carry out regular security audits.

Another critical issue is the potential misuse of data and unauthorized access. Data shared with third-party providers could be used for purposes beyond the agreed terms, including unauthorized sharing or selling. This not only breaches privacy laws but also erodes consumer trust. Establishing clear data usage policies and conducting regular compliance checks can help ensure that providers stick to the rules. The lack of transparency in how third-party AI providers handle and process data further complicates things. Many financial institutions, including CDFIs, struggle to see exactly how their data is being managed, which makes ensuring compliance with data protection regulations challenging. To address this, CDFIs must demand detailed documentation and transparency from their third-party providers about their data handling practices.

Data integrity and quality are also areas of concern. Poor data quality can lead to inaccurate AI model outputs and decisions, which can harm both consumers and the CDFI's reputation. While there's limited specific data on how well CDFIs manage these issues, maintaining high standards of data governance and conducting regular data quality assessments are recognized as best practices.

To improve existing processes for conducting due diligence, CDFIs are beginning to consider how best they can carry out comprehensive vendor risk assessments. These assessments should evaluate the provider's security practices, compliance history, and data protection measures, focusing on their capability to comply with relevant data privacy laws and regulatory requirements. Establishing detailed Data Protection Agreements (DPAs) is also crucial. These agreements should clearly outline the responsibilities and obligations of third-party providers regarding data confidentiality, security, and usage, including clauses on data encryption, access controls, and breach notification protocols.

For monitoring ongoing third-party relationships, continuous monitoring and reporting mechanisms are an obvious necessity for CDFIs. These mechanisms can help oversee the provider's data handling practices and compliance with security protocols, allowing for real-time detection of anomalies or potential breaches. Regular compliance reviews and assessments are also necessary to ensure that third-party providers continue to adhere to the agreed-upon data protection standards and to evaluate their response to any security incidents.

Incident response plans should be developed and maintained by CDFIs, including protocols for managing data breaches involving third-party providers. These plans should integrate third-party providers into the financial institution's broader incident response framework. Additionally, ongoing training and awareness programs for third-party providers on data protection, security best practices, and compliance requirements are important to foster a culture of security and vigilance. Diversifying AI providers is another strategy to reduce risk, though it may not always be practical for all CDFIs due to budget constraints. Enhancing transparency and traceability across the AI supply chain is also important. This can be achieved by using technologies like blockchain to monitor data flow and verify compliance at each stage.

***B.17. How are financial institutions applying operational risk management frameworks to the use of AI? What, if any, emerging risks have not been addressed in financial institutions' existing operational risk management frameworks? How are financial institutions ensuring their operations are resilient to disruptions in the integrity, availability, and use of AI? Are financial institutions using AI to preserve continuity of other core functions? If so, please provide examples.***

In identifying and assessing risks, CDFIs often focus on potential model risks, such as inaccuracies and biases that might emerge from AI algorithms. Larger and more technologically advanced CDFIs tend to conduct thorough risk assessments, while smaller institutions may still be developing these capabilities. Operational risks, such as the potential for AI system failures that could disrupt services, are recognized universally, though the extent of these assessments varies.

Compliance with regulatory requirements is another critical area, with more sophisticated CDFIs often having compliance frameworks that include AI, ensuring they adhere to regulations like the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA). Concerns about data privacy, particularly the protection of sensitive information used in AI models, are common, but the specific practices for managing these risks can differ significantly among CDFIs. Compliance programs tailored to AI applications are also more likely to be found in CDFIs with greater resources and technological infrastructure.

Investment in human capital is another key aspect of managing AI risks. Again, larger CDFIs are more likely to offer training programs to enhance staff understanding of AI technologies and associated risks. These larger CDFIs also tend to form cross-functional teams, including data scientists, risk managers, and compliance officers, to oversee AI projects.

Generally, CDFIs are beginning to consider the application of operational risk management frameworks to their use of AI, but the sophistication and extent of these practices vary. Larger and more technologically advanced CDFIs generally have more comprehensive risk management practices in place, whereas smaller CDFIs may still be in the early stages of implementation.

**C.** ***Further Actions***

***C.18. What actions are necessary to promote responsible innovation and competition with respect to the use of AI in financial services? What actions do you recommend Treasury take, and what actions do you recommend others take? What, if any, further actions are needed to protect impacted entities, including consumers, from potential risks and harm? What enhancements, if any, do you recommend be made to existing governance structures, oversight requirements, or risk management practices as they relate to the use of AI, and in particular, emerging AI technologies?***

To foster responsible innovation and competition in the use of AI within the financial services sector, a comprehensive and collaborative approach is essential. Treasury should begin by developing detailed governance frameworks for AI, providing clear guidelines on data quality, model validation, explainability, and thorough documentation. Financial institutions need these standards to ensure that AI model decisions are transparent and can be easily audited and regulated. Strengthening regulatory oversight is crucial, involving regular reviews and updates of AI-related regulations to keep pace with technological advancements and emerging risks.

Enhanced monitoring systems will help ensure compliance and identify potential issues early on.

Promoting inclusive and equitable access to AI technologies is another key priority, particularly for the CDFI industry. Treasury should support small financial institutions by providing technical assistance, grants, and training programs to help them adopt AI. Additionally, fair lending regulations must be enforced rigorously to prevent AI from perpetuating discrimination and bias. Regular audits and impact assessments can help ensure compliance and fairness and a strong effort to facilitate collaboration across sectors will drive innovation and address common challenges. Establishing public-private partnerships and organizing industry forums can encourage the sharing of best practices and collaborative solutions to emerging risks, serving as platforms for discussing AI governance and promoting a cooperative and diverse regulatory approach.

Treasury should also update data privacy regulations to safeguard consumer data used in AI models, including requirements for data anonymization and secure storage. Implementing strong cybersecurity standards tailored to AI systems will further protect these technologies from cyber threats. For their part, financial institutions, including CDFIs, must take proactive steps to implement robust risk management practices. Comprehensive AI-specific risk assessments can address potential biases, data privacy issues, and operational risks. Continuous monitoring and auditing processes are necessary to promptly detect and mitigate these risks.

Finally, transparency and accountability should be prioritized in AI deployment. Financial institutions should maintain detailed documentation of their AI models, including development processes, data sources, and decision-making logic. Clear communication with stakeholders about AI usage and mechanisms for feedback will enhance trust and accountability.

To ensure fairness and mitigate bias, financial institutions should regularly test their AI models and implement strategies to address any biases. Using diverse and representative data sources for training AI models can help avoid reinforcing historical biases. Strengthening consumer protection measures is also critical. Consumers must receive clear and understandable reasons for adverse actions taken by AI systems, in compliance with fair lending laws.

On the legislative front, enacting comprehensive data privacy laws that address the collection, storage, and use of data in AI systems is crucial. These laws should include provisions for consumer consent and data protection. Introducing an AI Accountability Act can hold financial institutions accountable for the outcomes of their AI systems, ensuring adherence to ethical and legal standards.

Regulatory improvements that allow financial institutions to test AI technologies in a controlled environment under regulatory supervision can increase demand for such technology, while ensuring new users remain in compliance with regulatory guidelines. Supervisory actions should include creating dedicated oversight bodies within regulatory agencies focused on AI technologies. These bodies would monitor and guide the use of AI in financial services. Providing specialized training for regulators will ensure they understand and can effectively oversee AI technologies and their applications in the financial sector.

By implementing these measures, Treasury and financial institutions, including CDFIs, can foster a financial system that leverages AI's potential while mitigating its risks. This approach

will maintain stability, protect critical infrastructure, and ensure that AI technologies serve the needs of all consumers and businesses, particularly those in underserved communities.

* * *

On behalf of the African American Alliance of CDFI CEOs, we thank you for the opportunity to provide input on the development of a national strategy on financial inclusion. Please do not hesitate to contact us for clarifying questions or comments.

Sincerely,

Lenwood V. Long, Sr.
CEO, African American Alliance of CDFI CEOs