August 12, 2024

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

Response to Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector
(Docket ID TREAS-DO-2024-0011)

We appreciate the opportunity to share some insights about Responsible AI (RAI) use at PayPal. PayPal is committed to promoting responsible technology use and to using AI technology in a manner consistent with regulatory guidance, industry best practices, and our overall risk management framework. AI holds much promise to deliver benefits to our customers and other stakeholders, and we believe these benefits can come from ethical development and use. Our approach is guided by internal principles and governance that emphasizes our responsibility to protect our customers in this rapidly evolving space. Senior leadership across the company is engaged and aware of the opportunities and risks of AI. Our commitment to RAI use continues to evolve to keep pace with the rapidly changing AI landscape. For example, in 2023, we expanded our RAI framework, further incorporating human oversight requirements into PayPal's AI use, including generative AI ("GenAI"). We also strengthened our AI governance by embedding model and AI risk assessment into our existing Risk and Compliance programs, such as new product review and third-party onboarding processes. Additionally, we formed an internal Center of Excellence focused on the responsible implementation of GenAI across the company. We appreciate that AI technology will require us to continue to monitor and enhance our approach to mitigate risks and leverage opportunities for our customers.

We are committed to using only the best-in-class techniques for AI, which includes Predictive AI, a machine learning type of AI capability that classifies input data in terms of expected outcomes, as well as GenAI, another machine learning type of AI that focuses on creating new content and ideas in various formats. At PayPal, we use these types of AI to advance several business objectives. Specifically, we carefully leverage these tools to detect suspicious, unlawful, or fraudulent activity, improve customer experiences, personalize offers for products and services,

automate back-end processes and manage business risks. We believe the benefits of AI are achievable so long as we practice responsible innovation and continue to invest in our governance, risk management and controls. PayPal takes these matters seriously not only as a matter of compliance, but as an investment in sustaining trust with our customers and other stakeholders.

Our RAI framework incorporates five core principles - Privacy, Security, Fairness, Transparency and Explainability – that inform systems and processes to help ensure safe, transparent and accountable use of AI technologies. These five core principles and underlying pillars below help us ensure ethical, transparent and accountable use of AI technologies in a manner consistent with user expectations, organizational values and societal laws and norms. This is key to retaining our customers' trust and to becoming industry leaders in promoting state-of-the-art, responsible application of AI.

- Privacy and the protection of customer personal data must be managed throughout the life cycle of PayPal's AI Systems. This includes both the personal data directly provided by users, and user information generated by their interactions with PayPal's AI Systems.

- Security risks associated with PayPal's AI Systems must be managed in accordance with the level of risk to PayPal and its users. This includes ensuring resiliency of these systems, both on an individual basis and with respect to interconnection / interdependence; managing risks posed by these systems to the confidentiality, integrity, and availability of PayPal systems. Business-critical automated decision-making systems must be protected from compromise and manipulation by malicious actors.

- Fairness is the absence of any prejudice or favoritism toward an individual or a group, based on their being a member of a protected class or their protected characteristics in the context of decision making, such as product and service offering.

- Transparency refers to the documentation and disclosures around AI applications. All AI documentation should be accurate and complete to ensure the entire AI program is replicable, traceable and auditable. When applicable, transparency also requires that customers be made aware of interaction with an AI system, its limitations, and risks.

- Explainability refers to the human interpretability of the decision-making process of the AI system. Decisions made by AI often need to be justified and understood by a range of internal & external stakeholders.

These RAI principles inform PayPal's AI risk management approach which aims to unlock the benefits of AI use while properly identifying and mitigating risks that stem from use. To guide the continuous improvement of our enterprise risk management approach, PayPal leverages existing legal requirements, emerging regulatory expectations, industry best practices, and relevant portions from AI risk management frameworks by impartial bodies, such as National Institute of Standards and Technology (NIST).

- Human Oversight, Governance Practices and Testing: Human oversight is critical to the AI lifecycle and in line with effective model risk management practices. PayPal's diverse team of cross-functional subject matter experts continuously assess things such as data quality and relevance, testing to ensure that model components are functioning as expected, and model limitations and assumptions.

- Emerging Security Risks: PayPal continues to be committed to the ongoing safety and security of its customers. Our approach to AI safety and security is consistent with NIST's benchmarks in its AI Risk Management Framework and Cybersecurity Frameworks. We maintain internal policies, procedures and controls to address security risks unique to AI, such as data poisoning, model thefts, data leakage, model integrity compromise and prompt injections.

- Third Party Risk Management: In some cases, PayPal relies on external parties for model development. We hold partners and suppliers to required standards to ensure safe and reliable deployment, requiring each partner and supplier to undergo comprehensive evaluation and due diligence assessments. Our agreements with these third parties document relevant roles and responsibilities regarding risk and compliance requirements, as well as expectations regarding AI integrity, availability and responsible usage.

- Data Use, Governance, Privacy and Security: PayPal takes a proactive approach to data protection that prioritizes responsible use of data and customer empowerment through transparency, education, privacy-by-design and product innovations. To achieve this, PayPal has established robust, enterprise-wide standards to safeguard our customers and drive consistency in the management and execution of processing personal information. This includes controls and oversight for data collection, use, minimization, storage, disposal and sharing.

In addition to managing the risks in AI throughout the life cycle, AI also presents enterprises with opportunities to improve their capabilities and achieve efficiencies in the delivery of their services. As two examples of how AI can be utilized to augment enterprises' operations, PayPal leverages AI tools to enhance its capabilities to

combat fraudulent activity and to improve processes related to our anti-money laundering/countering the financing of terrorism (AML/CFT) program.

- Fraud: For financial institutions, AI poses significant additional potential to help combat fraud and safeguard customers from bad actors. PayPal has successfully leveraged traditional AI for more than a decade to combat fraud. However, the democratization of AI, and specifically GenAI, is likely to enhance fraudsters' capabilities, and PayPal has already seen instances of GenAI being used for fraud. For example, criminals may use GenAI to create text inputs during interaction with organizations, upload fake images as ID documents and place robot calls trying to social engineer customer service agents. To keep up with the rapid developments emerging in this space, PayPal continues to conduct research and deploy new AI initiatives to combat such fraud. Employing AI-driven fraud detection tools and analytics helps financial services firms employ a more nuanced risk management approach that is more targeted and accurate. This allows a greater focus on true bad actors while enabling good transactions. As policymakers move forward with creating new laws and regulations for AI, it is important to consider, evaluate and hopefully mitigate the potential implications such laws and regulations may have on curtailing the ability of companies to leverage these important fraud tools, which help enhance and protect customer safety.

- AML/CFT: AI tools also have significant potential to help mitigate financial crimes, such as money laundering. PayPal is seeing increased potential for using AI in this context, including onboarding, customer screening, transaction monitoring, pattern recognition, case management optimization, investigation streamlining, suspicious activity reporting and quality assurance.

PayPal appreciates the opportunity to share some insights related to its Responsible AI program and how it helps us unlock the benefits of AI innovation. This is an important moment for our industry, and while AI comes with risks, it has significant potential to help financial institutions serve customers with best-in-class experiences. We recognize the responsibility of industry to build guardrails to ensure that we can achieve these objectives ethically and that the Treasury Department's Request for Information is an important step forward in this effort.

For further information please contact Fabrice Coles, PayPal Government Relations Senior Manager for Global Public Policy at facoles@paypal.com.