CLIENT UPDATE

AI IN FINANCIAL SERVICES GUIDANCE FROM TREASURY

Background

The U.S. Department of the Treasury (the "Treasury") published a report on December 19, 2024 on The Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services (the "Report"), based upon respondents' comments to a previous consultation. The Report provides background on the use of AI in financial services, builds on previous Treasury reports and summarizes key recommendations from respondent feedback, including an array of financial firms.

The Report provides useful guidance for Mexican financial firms to start preparatory steps that will make it easier and more expedient to implement future regulations governing AI in the financial services industry in Mexico.

Risks and Mitigation Measures

The Report notes that the last two years marked a major shift from traditional AI with an acceleration in the development of emerging AI technologies such as "Generative AI." Generative AI is characterized by its ability to create new content based on what is learned from the training data.

The Report contains information on six categories of potential risks related to AI and includes suggestions of measures to mitigate each risk.

• **Data Privacy, Security, and Quality Standards.** Respondents highlighted the need for high-quality data and noted that risks related to "data poisoning" can impair a model's performance.

Suggested mitigations: Respondents proposed that organizations use AI governance frameworks and technical solutions such as homomorphic encryption and federated learning to enhance data privacy.

• **Bias, Explainability, and Hallucinations.** The Report summarizes respondents' concerns in respect to (i) bias, which is generally when a model's results reflect human or data biases, whith potentially discriminatory outcomes, (ii) lack of explainability, which includes the difficulty of understanding how models generate output and may undermine trust and entail reputational risks, and (iii) risks associated with generative AI such as hallucinations where a model convincingly produces an incorrect output.

Suggested mitigations: Respondents highlighted how some financial firms are attempting to mitigate potential bias from using AI, including using alternative variables, like rent and utility payments, to decrease reliance on credit scores. Another alternative is to use retrieval augmented generation to ground outputs in verifiable data to improve explainability.

• **Impact on Consumers and Consumer Protections.** The Report notes respondents' concerns with risks for AI systems that interact directly with consumers, it underscores the importance of accuracy and disclosures in these use cases and the need to observe consumer protection laws.

Suggested mitigations: Varied views on mitigation measures included mandatory disclosure to improve transparency and accountability, prelaunch testing for AI models or regulatory pre-approval.

• **Concentration-related Risks.** Respondents identified the concentration risk of Generative AI model development by only a few firms and the resulting impact on market competitiveness for both providers and users of AI. Ensuing risks such as cyberattack and unfair competitive advantage may pose systemic vulnerabilities.

Suggested mitigations: Some respondents suggested open-source AI tools, and monitoring the concentration of AI providers. To reduce macro level risks, some respondents suggested developers to use incremental rollouts before full scale implementation to minimize the risk of widespread disruption.

• **Third-Party Risks.** Respondents expressed that due to high cost and technical expertise, financial firms will need to rely on AI models and systems developed by others.

Suggested mitigations: Respondents emphasized the need for financial firms to rely on vigorous third-party risk management ("TPRM") processes and conduct robust due diligence as we have previously discussed.

• **Illicit Finance Risks.** The Report conveys respondents' concerns about the growing use of AI tools by adversaries to enable illicit cyber activity and fraud.

Suggested mitigations: Respondents recommended digital identity solutions, such as biometrics-based multi-factor authentication, to address such risks.

Potential Next Steps

Financial Firms

• **Prioritize Review of AI Use Cases for Compliance with Existing Laws/Regulations Before Deployment.** The Report recommends that financial

firms prioritize their review of AI use cases for compliance with existing laws and regulations before deployment and that they periodically consider updates to their policies and procedures, and their AI models.

Government Agencies

• **Facilitate Financial Services-specific AI Information Sharing.** The Report recommends the financial services sector and government agencies continued collaboration on AI information sharing, in an appropriate AI cybersecurity forum to develop data standards, share risk management best practices, and support smaller firms , while monitoring concentration risks among providers.

• **Continued International and Domestic Collaboration.** The Report recommends continuing international and domestic collaboration among governments, regulators, and the financial services sector to promote consistent standards for uses of AI in the financial services sector. Of particular importance in the case of Mexico, is the need for enhanced interagency collaboration to cohesively address emerging AI risks.

Key Suggestion

• **Establishing a Generative AI Risk Assessment Program and Inventory.** Mexican financial firms should consider implementing a generative AI governance program that (1) identifies low risk AI uses cases that do not need a compliance review (e.g., summarization and translation of public documents), (2) identifies prohibited use cases and ensures that there are no such use cases in production (e.g., using a generative AI interview tool to decide whether to hire an employee based on what their body language indicates about their trustworthiness), (3) identifies the risks associated with other generative AI use cases, along with the appropriate mitigation measures to address those risks, and (4) keeps track of higher-risk generative AI use cases in production to ensure that their risks, including regulatory compliance risks, remain adequately mitigated.

* * *

Please do not hesitate to contact us with any questions.

Berdeja Abogados, S.C.

February 5, 2025