ELECTRONIC TRANSACTIONS ASSOCIATION

1300 Connecticut Avenue
Suite 475
Washington, DC 20036

202.828.2635
800.695.5509
electran.org

August 12, 2024

Submitted Electronically via
http://www.regulations.gov

Ms. Jeannette Quick
Deputy Assistant Secretary
U.S Department of the Treasury
1500 Pennsylvania Avenue N.W.
Washington, D.C. 20220

Re: **Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector RFI TREAS-DO-2024-0011-0001**

Dear Ms. Quick:

The Electronic Transactions Association ("ETA") hereby submits this information in response to the Treasury Department's Request for Information ("RFI") on artificial intelligence ("AI") in the financial services sector. ETA is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S and in more than a dozen countries around the world. ETA members make commerce possible by processing approximately $47 trillion annually in purchases worldwide and deploying payments innovation to merchants and consumers. Because ETA has members that are engaged in the development and deployment of AI technology in the payments industry, it is pleased to have this opportunity to provide feedback to the Department on its requests for information.

Background

The payments industry is at the forefront of safely deploying new technologies—including AI and machine learning. These technologies improve the consumer experience by making payments more secure and frictionless. The payments industry has developed and deployed AI tools to make payments faster and more secure, while unlocking numerous benefits for consumers, businesses, and the payments industry alike.

ELECTRONIC TRANSACTIONS ASSOCIATION
1300 Connecticut Avenue
Suite 475
Washington, DC 20036
202.828.2635
800.695.5509
electran.org

ETA encourages policymakers to review how the payments industry has used AI over the years to better understand the scope, scale, and impact that these tools have in fostering a stronger and more secure payments ecosystem. ETA believes use of AI by ETA members is well covered by existing laws and regulations.

To the extent new laws and regulations are needed, ETA suggests policymakers consider how the payments industry has leveraged AI responsibly under the robust oversight of federal and state policymakers and regulators. Any new laws and regulations should also complement and clarify, rather than duplicate, obscure, or conflict with the existing laws and regulations to which the payment industry already adheres. This requires recognizing how AI is currently being utilized to benefit consumers and the marketplace, alike, in payments today and acknowledging the rapid advances in this field.

U.S. payments companies employ robust, risk-based processes to assess and use AI and machine learning ("ML"). They have policies, procedures, and governance to ensure they understand the technology they use, and any potential risks and benefits, before deploying them. With a risk-based framework, payments companies are required to assess the risk of their AI/ML use and apply appropriate safeguards based on risk level and the nature and extent of their business. The applicable federal and state regulations are largely principles-based and agnostic as to the exact AI/ML being used. This type of regulation, adapted to the nature of the payments industry appears to be the proper style of regulation and be least likely to create conflicts/duplication in an area of technology that is constantly and rapidly changing. It would also ensure continuous growth and innovation, while protecting consumer and company interests in security.

AI presents opportunities to further strengthen protection for consumers against financial crimes, to streamline payments, to promote regulatory compliance, to improve customer service, and to support fair lending decisions. The payments industry is enthusiastic about harnessing AI to enhance transactional experiences, while at the same time establishing methods for maintaining security and assisting in preventing the violation of law.

Finally, it is essential that we distinguish traditional AI/Machine Learning from generative AI. While generative AI can be a useful tool for a host of use cases, it's still in its infancy and raises concerns, such as the risk of hallucinations, that differ from traditional AI/ML. For ETA members, this distinction currently limits the use of generative AI. For these reasons, it's important that regulations do not lump together traditional AI and generative AI.

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? To the extent possible, please provide specific suggestions on the definitions of AI used in this RFI.

ETA supports a principles-based approach. To encourage innovation, maintain national economic competitiveness, and combat financial crimes, it is crucial for policymakers to promote rules that leverage existing policies, are technology-agnostic, and are principles and risk-based. It is also important that they consider industry-led standards that strike a balance in promoting innovation, protecting consumers and businesses, advancing U.S. economic and national security interests, and ensuring the continued development of secure and inclusive financial services.

While there are many varying definitions of AI, attempting to come up with a "perfect" definition that is not overly broad or narrow will quickly become outdated or subject to scrutiny. Instead, if the aim is to focus on certain principles, then it does not matter as much that there is a "perfect" definition of AI and enhance existing frameworks.

Further, the appropriateness of any definition of AI depends on the extent it does or does not preempt other regulation. ETA members already subject to strict state and federal regulations as well as ongoing supervision. ETA's strong preference is inclusion of a federal preemption clause to prevent state, local, and sector-specific AI regulations that are increasing compliance challenges and create different treatment of its customers depending on where they live.

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?*

ETA's response to question 2 is included in our answer to question 3, below.

3. *To what extent does the type of AI, the development of AI, or AI applied use cases differ within a financial institution? Please describe the various types of AI and their applied use cases 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? If so, please provide specific examples.*

The payments industry uses AI models to enhance internal and external operations. Traditional AI is deployed in the payments sector for data analysis, assistance with predictive texting, transcribing audio, enhancing document search functions, verifying user identities during password reset processes, and for authorizing payments while checking for fraud. In contrast, Generative AI is harnessed to craft original content from existing data, generate document summaries, create unique and secure passwords, personalize recommendations using point-of-sale information, and to

establish more accurate fraud detection and response mechanisms. Payment companies also synthesize the use of traditional and generative AI for certain functions. The result of this synthesis helps to provide a more highly personal, secure, and streamlined payment experience. It is essential that policymakers understand the fundamental differences between traditional AI and generative AI as they consider legislation and/or regulation in this space.

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? Please describe specific benefits with supporting data and examples. 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? Please be as specific as possible, including details about cost savings, increased customer reach, expanded access to financial services, time horizon of savings, or other benefits after deploying AI.

The appropriate use of AI provides significant benefits to consumers and payment companies, as well as the overall marketplace, alike. AI systems can assist with identity verification and protection, personalization of services and recommendations, and fraud detection. Compliance with fair lending and consumer protection laws is of the utmost importance to ETA and its member institutions. The proper use of AI can enhance payment companies' ability to comply with fair lending and consumer protection laws. Model risk management and compliance programs are an essential aspect of how payment companies now operate. Although AI itself requires the kind of risk-based management described above, it may also itself be used to structure effective risk management.

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?*

The level of connectivity and extent of AI use vary among payment companies. This variation is a result of the diverse business functions that compose the payments sector as well as the size, scope, and complexity of the underlying activities. To meet industry needs, AI models and tools are being developed and deployed by a variety of stakeholders across the payments industry. As is the case

with other products and service providers, distinctions need to be drawn depending on the nature of the product, the risks and importance of the activities affected, and the identity of the provider of the product (third-party or in-house).

Existing Model Risk and third-party service provider guidance from the Federal banking regulators establishes considerations that must be considered when for the use of third-party models are used by payment companies or third parties provide equivalent services. This guidance requires both the relevant institutions and the third parties to consider the nature of the underlying business and the aspects of the products that can create risk. In general, ETA supports the development of federal guidelines for the integration of AI systems with existing payment infrastructure, and the creation of standards for interoperability between different AI systems and payment platforms. A regulatory focus on interoperability principles helps ETA's members contribute to a more seamless user experience across various AI-powered payment services.

There are also intellectual property risks when using AI models and tools. Most of the intellectual property ("IP") risks, if not all, derive from the fact that the data training the model or tool involves large amounts of information for the mode or tool to work efficiently and properly. Such information may belong to or be proprietary to another entity. The following are the main risks associated with using AI models or tools:

1. Copyright Issues: Generative AI systems can produce content that closely resembles or incorporates copyrighted material. In the financial sector, this might involve generating reports, trading algorithms, or marketing content. Organizations must ensure that the AI's outputs do not infringe on the copyrights of others and address any issues of derivative works. This is single-handedly the largest IP risk, and the most difficult to manage/mitigate.
2. Patent Infringement: Generative AI models may inadvertently infringe on existing patents related to algorithms, methods, or technologies. Financial institutions deploying these models must conduct thorough patent searches and risk assessments to ensure they do not violate patent rights held by others.
3. Trade Secret Concerns: The payments industry often uses proprietary algorithms and data as trade secrets. If generative AI models are trained on or interact with sensitive internal data, there is a risk that the AI could inadvertently expose or replicate trade secrets, potentially leading to unintended disclosures or competitive harm.
4. Data Ownership and Licensing: The use of generative AI involves vast amounts of data, which raises questions about data ownership and licensing. Payment companies must clarify the rights to data used in training and the ownership of AI-generated content to avoid disputes over intellectual property rights.

5. Model Ownership and IP Claims: The creation of generative AI models may lead to disputes over the ownership of the underlying intellectual property. Financial entities need to address who owns the model, its outputs, and any related innovations, particularly when collaborating with third-party AI providers.
6. IP Protection Strategies: Companies should develop comprehensive IP protection strategies, including securing patents, trademarks, and copyrights for their innovations, while also negotiating clear IP agreements with technology partners and ensuring robust internal policies for managing AI-generated IP.

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? Please describe the governance structure and risk management frameworks financial institutions expect to apply in connection with the development and deployment of AI. Please provide examples of policies and/or practices, to the extent applicable. What types of testing methods are financial institutions utilizing in connection with the development and deployment of AI models and tools? Please describe the testing purpose and the specific testing methods utilized, to the extent applicable. 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?*

ETA members aim to implement risk management frameworks that are adapted to the exact nature, extent, and complexity of the services they provide and the type of regulation to which they are subject. Consequently, it is difficult to generalize without becoming superficial. Among other things, members hire internal and external experts to advise about the acquisition and use of AI, conduct tests under a variety of conditions to uncover unexpected behavior, de-bug software, purchase insurance to cover risks and create management positions and structures to supervise and evaluate all of these activities.

While AI can be used to prevent fraud, it can also become a target of fraudulent activity. The National Institute of Standards and Technology (NIST) has published a detailed AI Risk Management Framework, with several principles that ETA supports. The NIST framework begins by calling for developers and designers to frame the AI technology's potential risk by seeking to understand future impacts and challenges. Additionally, NIST notes that the audience of the AI should be considered across its lifecycle when considering risk-management tactics. Additionally, in compliance with the NIST framework, ETA seeks to embody trustworthiness and effectiveness principles throughout AI operations.

Specific guidance and existing risk management policies being weighed by ETA members include the Federal Reserve letter SR 11-7 (Model Risk Management), and similar guidance from other agencies, along with ongoing work that is designed to align with the current AI and model risk management guidance. The Federal Reserve letter SR 11-7 requires U.S. banks to have robust programs in place to assess the validity and risks of "models" as defined by such guidance. Future guidance developed by policymakers should clearly delineate when use of AI is subject to SR 11-7 versus not.

Explainable AI refers to the idea that humans should be able to understand and explain how AI models come to the inferences that they do. But AI may generate outputs where the basis for why one or more of the outputs were generated is difficult to define. Practices around data input, human involvement, decision-making criteria and weighting of those criteria, assurance review and others are being developed to ensure that validation processes keep pace with technology, along with ways to trace how AI models process inputs into outputs, to understand the states of the models before and after processing.

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? Please describe the data governance structure financial institutions expect to apply in confirming the quality and integrity of data. 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?*

ETA member companies use various types of input data for the development of their AI models and tools. The requisite input data is dependent on the intended function of the AI technology it supports. Since ETA members cover the payments industry, both "traditional" and "non-traditional" input data are being used to innovate and train AI across the payments sector, including continued evolution to better utilize AI.

Generative AI models frequently train on publicly available data, which may fall under the umbrella of "non-traditional" data. To craft original content, generative AI must access huge amounts of data; therefore, datasets are often sourced from internet content. ETA affirms that ethical considerations must be considered when training AI, and that AI technologies should to some extent be supervised by a human.

9. *How are financial institutions evaluating and addressing any increase in risks and harms 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? Please describe specific risks and provide examples with supporting data.

AI technology presents an increased risk of discrimination to consumers if it is not developed and deployed responsibly. ETA suggests policymakers consider how the payments industry has leveraged AI responsibly while undergoing robust oversight from federal and state policymakers and regulators. New laws and regulations should also complement and clarify, rather than duplicate or conflict with the efficacy of existing rules that the payment industry adheres to. To facilitate responsible AI technology, ETA members seek to minimize the risk of bias and discrimination at all stages of the AI technology's lifecycle. From early design and development to post-deployment, ETA believes that AI technology should be monitored for potential harmful impacts.

One strategy that ETA has adopted to avoid reliance on AI technology within the payments sector is to frame AI as a form of enhancement technology, not as replacement technology. ETA promotes keeping humans in the loop to provide oversight monitor process and evaluate and key decisions. Among other things, rigorous testing using data sets not used in training the relevant AI should be conducted to detect potential forms of discrimination that are illegal, or, if legal, are contrary to the declared business purposes of the relevant company.

ETA also supports the notion that hiring diverse AI technicians can help companies identify discrimination. To the extent a company serves different nations, it should also conduct tests to determine whether patterns perhaps relevant in one nation are inappropriately being used in another. Payments sector companies engaged with AI are expected to participate in routine impact assessments, with an eye for discrimination.

Finally, ETA members are subject to all existing anti-discrimination laws. ETA believes that any new laws geared towards preventing discrimination should be drafted with an awareness of how much existing laws already cover.

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?

ETA and its members care deeply about maintaining consumers' trust and promoting non-discriminatory, unbiased practices. AI use has not and will not alter this commitment. ETA members already comply with anti-discrimination laws and are committed to maintaining and improving non-discriminatory practices. As previously discussed, ETA also supports technology-neutral policies designed to prevent discrimination based on race, gender, age, or other protected characteristics.

To ensure that AI use does not result in discriminatory outcomes, ETA supports continuous evaluations and impact assessments to monitor the effects of AI. Additionally, ETA believes that efforts to increase explainability will, if ultimately successful, help combat discriminatory outcomes. For example, when an AI developer provides clear documentation on how the algorithm contributed to a decision, AI developers and users alike can more easily identify the factors that may lead to a potentially discriminatory outcome. Generative AI is a very new evolution of AI, and as mentioned, some outcomes cannot be fully explained. Due to these concerns, Gen AI is not currently used in underwriting.

11. *How are financial institutions addressing any increase in data privacy risk related to the use of AI models, particularly emerging AI technologies? Please provide examples of how financial institutions have assessed data privacy risk in their use of AI. In what ways could existing data privacy protections (such as those in the Gramm-Leach-Bliley Act (Pub. L. No. 106-102)) be strengthened for impacted entities, given the rapid development of emerging AI technologies, and what examples can you provide of the impact of AI usage on data privacy protections? How have technology companies or third-party providers of AI assessed the categories of data used in AI models and tools within the context of data privacy protections?*

Payment companies bear responsibility for protecting consumer data and maintaining consumer privacy. Currently, there is a wide-ranging federal and state data privacy framework already in place. From the federal Fair Credit Reporting Act and the Gramm-Leach-Bliley Act to the California Consumer Privacy Act and the Connecticut Personal Data Privacy and Online Monitoring Act, existing federal and state data privacy frameworks protect consumers. ETA takes the position that new laws and regulations relating to data privacy should not target AI specifically because ETA members' use of AI is already covered within existing legal frameworks. Thus, regulatory targeting of AI and data privacy would duplicate existing compliance efforts without providing robust additional protection for consumers.

To build trust with consumers and to ensure legal compliance, payment companies follow data privacy laws and keep abreast of new legal developments. Based upon industry experience, ETA believes that the use of traditional AI does not undercut payment companies' compliance with the federal and state data privacy laws, and in many instances further supports and enhances those efforts. Finally, ETA continues to support a technology-neutral uniform national standard for privacy. This standard would replace, not duplicate, the existing framework and would provide predictability to both consumers and payment companies.

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)?*

It is crucial that the payments sector address fraud risks amidst the widespread adoption of AI technologies. To minimize potential fraud risks arising from AI, ETA members will continue to apply existing company practices to all new AI technologies. For example, if a company uses multifactor authentication technology to manage fraud, it should continue to use such technology even once AI technology is introduced. Further, existing third-party confidentiality policies should also carry over into management of AI technology when applicable to minimize fraud risk.

Additionally, ETA acknowledges a growing fraud risk arising from opt out provisions regarding the processing of personal information in AI technology the use of automated decision-making ("ADTs"). ETA believes that the scope of opt outs needs to be clarified, and restricted, to ensure fraudsters cannot use opt out provisions as a means of facilitating financial crime. ETA recommends policies that do not allow for opt outs. In formulating this opposition to opt outs, ETA members consider contracts with and among third-party partners requires compliance with a consumer's request to delete the consumer's personal information. ETA believes that in specific circumstances it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information to help to ensure security and integrity. Broadly, ETA opposes giving consumers an option to opt out of interlayered technologies.

ETA further disapproves of any policy that mandates companies to disclose notifications to consumers at the time ADT machine learning is being used to prevent fraud, because such notification requirements could alert bad actors and hinder prevention efforts.

13. *How do financial institutions, technology companies, or third-party service providers expect to use AI to address and mitigate illicit finance risks? What challenges do organizations face in*

adopting AI to counter illicit finance risks? How do financial institutions use AI to comply with applicable AML/CFT requirements? What risks may such uses create?

AI is integral to maintaining the safety and security of payment systems, which include consumer information and resources. ETA believes that AI 's ability to work faster, identify more patterns, and respond more quickly than humans is an asset in protecting consumers from financial crimes. For example, payments companies use their technological capabilities and unique industry insights to detect, track, and stem the flow of fraud schemes.

AI can be used to comply with applicable AML/CFT requirements by enhancing the companies' ability to respond to risks and implement new requirements. Companies in the payments sector may use AI to monitor transactions and to filter out scenarios that require additional investigation. AI should be deployed as a complement to human supervision of AML/CFT processes to avoid machine errors going unchecked.

As the volume and complexity of fraud in transactions have risen, the importance of identifying, preventing, and deterring fraud in payments has likewise increased. Given the rise of criminals exploiting new AI technologies such as deepfakes to commit more complex fraud, payment companies will increasingly rely on AI capabilities to enable timely detection and combating increasingly sophisticated fraud schemes.

14. *As states adopt the NAIC's Model Bulletin on the Use of Artificial Intelligence Systems by Insurers and other states develop their own regulations or guidance, what changes have insurers implemented and what changes might they implement to comply or be consistent with these laws and regulatory guidance? How do insurers using AI make certain that their underwriting, rating, and pricing practices and outcomes are consistent with applicable laws addressing unfair discrimination? How are insurers currently covering AI-related risks in existing policies? Are the coverage, rates, or availability of insurance for financial institutions changing due to AI risks? Are insurers including exclusions for AI-related risks or adjusting policy wording for AI risks?*

NO RESPONSE AT THIS TIME

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?

Payments companies rely on third parties to aid with a variety of business functions. Payment companies manage third-party risks from emerging AI technologies by applying existing risk management frameworks, and any additional AI risk management mechanisms that the company chooses to implement internally. Instances of third-party misconduct should be handled in accordance with company policy and relevant legal infrastructure.

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?*

Payments companies abide by both internal data confidentiality policies and the external data privacy legal framework. The external legal framework extends to third-party data providers and users. ETA supports this and similar technology-neutral efforts to equally protect consumers from the risks associated with third-party providers.

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.*

Payment companies use their existing operational risk management frameworks in the application of AI. Successful operational risk management frameworks, like the NIST framework, rely on corporate commitments to maintain teams of AI technology professionals with clearly defined roles. ETA encourages its members to hire and maintain teams of individuals capable of performing risk management and looking critically at AI technology for potential adverse impacts. Additionally, ETA emphasizes the importance of designating priority tasks to developers and deployers to ensure risk management maintenance.

AI risks remaining in the payments sector include exempting deployer's required impact assessments from public records laws to protect confidentiality and maintaining trade secrets relating to AI technology. ETA hopes that for transparency and explainability purposes companies will share information, but that such exchanges will not be done at the expense of confidentiality. Also, user information collected in impact assessments should be protected from being made public without consumer consent.

ETA members undertake extensive efforts to enable their operations to be resilient to disruptions in the integrity, availability, and use of AI by maintaining corporate commitments to human oversight. ETA members do not intend to rely solely on AI technology, rather they hope to harness it to enhance normal business function and internal supervision. Without a total reliance on AI technology, ETA members will hopefully be subject to less harm in the event of disruptions in AI use.

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 harms? Please provide specific feedback on legislative, regulatory, or supervisory enhancements related to the use of AI that would promote a financial system that delivers inclusive and equitable access to financial services that meet the needs of consumers and businesses, while maintaining stability and integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats. 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?*

ETA and its members recognize both the benefits and risks associated with AI use. Since industry stakeholders are best acquainted with these benefits and risks, ETA recommends that regulators allow these stakeholders to assist in setting standards for AI use and development. It is essential that industry standards are considered during policy development to encourage innovation, maintain national economic competitiveness, and combat financial crimes. Industry considerations are essential in helping regulators strike a balance in promoting innovation, protecting consumers and businesses, advancing U.S. economic and national security interests, and ensuring the continued development of secure and inclusive financial services.

Federal and state regulators have also expressed concern about data protection and privacy. ETA supports replacing the patchwork of state and federal laws with a uniform national standard of privacy that applies broadly, to establish consistency for consumers and payment companies alike.

If further regulation of AI is provided, it should be designed to level the playing field with under-regulated businesses across the whole AI supply chain, including non-banks and technology companies that provide financial services or support financial services, and data providers. ETA supports working to develop model certification techniques, standards, benchmarks, and certification agencies. Certification is possible where there are widely accepted and proven methods and benchmarks. Other advanced AI/ML areas need time to evolve. Legislation should

recognize those limitations. This is an area where support and funding from agencies can ensure feasibility before regulations are enacted.

Regulators outside of the banking space should establish similar risk-based standards for the development and use of AI systems outside the financial industry, and similarly oversee the use of AI systems. These standards should address common AI issues such as data privacy, IP ownership (including of input, model changes, and outputs under various use cases), bias, transparency, explainable decisions, algorithm validation, audit, and data security along each point of the AI supply chain.

Regulators should focus on where risks are concentrated (and are currently unaddressed), including on businesses outside the financial industry because they do not have the same prudential regulatory framework as banks and are more likely to create and use AI without guardrails. In fact, banks are the only industry with Model Risk management guidance from regulators. When evaluating whether to create new rules, regulators should consider both current and future use cases involving the use of AI with higher and lower risks, and the requirements that already apply to the activity being performed.

Overall, ETA hopes federal and state regulators will fill any regulatory gaps in a technology-neutral manner instead of adopting AI-specific laws or regulations. AI-specific laws or regulations are likely to risk duplicating existing legal requirements without providing meaningful additional protections for consumers and becoming obsolete or outdated as the technology evolves.

19. *To what extent do differences in jurisdictional approaches inside and outside the United States pose concerns for the management of AI-related risks on an enterprise-wide basis? To what extent do such differences have an impact on the development of products, competition, or other commercial matters? To what extent do such differences have an impact on consumer protection or availability of services?*

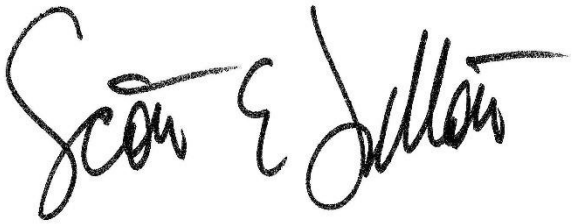
ETA is in favor of a common framework governing AI technologies. ETA anticipates that if companies are forced to comply with a patchwork of conflicting state and international laws, there would be negative consequences for consumers, inconsistences in the way information is handled and national security implications. ETA's strong preference is inclusion of a federal preemption clause for payments companies to prevent additional state, local, and sector-specific AI regulations that are increasing compliance challenges. Ultimately, ETA's overarching preference is for any new laws or regulations to acknowledge the statutory and regulatory frameworks currently in place in financial services and offer entity-level exemptions for those subject to the Gramm-Leach-Bliley Act, especially where there is an existing supervisory relationship.

1300 Connecticut Avenue
Suite 475
Washington, DC 20036

202.828.2635
800.695.5509
electran.org

In this moment of emerging AI regulation, ETA's members seek to comply with all relevant rules. Our members understand that AI regulation remains subject to changes in political leadership, especially since many existing AI policies are nascent and controversial given their questionable value. During this period of AI growth and development, ETA appreciates opportunities like this to collaborate with the government on behalf of the payments sector to improve the broader ecosystem and benefit consumers. ETA hopes that any AI framework developed is standardized and flexible.

Respectfully submitted,



Scott Talbott
Executive Vice President, Government Affairs
Electronic Transactions Association
1300 Connecticut Ave, #420
Washington D.C. 20036
stalbott@electran.org