Response to

Request for Information Regarding

Artificial Intelligence Risks and Modernization in Financial Services

On Behalf of the

American Bankers Association

to the

House Financial Services Committee Democrats

August 14, 2026

On Behalf of the

American Bankers Association

to the

House Financial Services Committee Democrats

August 14, 2026

Via Online Submission

Re: Request for Information on AI Risks and Modernization in Financial Services

Dear Ranking Member Waters,

The American Bankers Association [1] (ABA) appreciates the opportunity to respond to the House Financial Services Committee Democrats' Request for Information on AI Risks and Modernization in Financial Services (RFI). [2]

The following comments are based on discussions with ABA's AI Working Group, which is an interdisciplinary body of data scientists, technologists, compliance, legal, risk, security, audit, and human resources experts representing banks of all sizes. This group routinely comes together to formulate policy positions as well as to discuss operational best practices. Our comments are also informed by the work of the Financial Services Sector Coordinating Council's (FSSCC) R&D Committee. [3]

Please see ABA's responses to the questions below. Please note that we elected not to respond to every question; instead, we focused on areas in which we could deliver the most value.

Submission Details

***Question #1**: Please provide your name and the name of your organization.*

The American Bankers Association, also known as ABA.

---

[1] *The American Bankers Association is the voice of the nation's $26.1 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $20.5 trillion in deposits and extend $13.7 trillion in loans.*

[2] https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=415374 and . https://democrats-financialservices.house.gov/uploadedfiles/ai_rfi.pdf.

[3] In 2026, FSSCC published a series of AI papers covering an AI risk management framework, identity & authentication controls, explainability, nutrition labels, and a lexicon; see https://fsscc.org/aieog-ai-deliverables/.

Question #2*: Supplemental data and reports are optional and welcome. Please email AIRFI_Data@mail.house.gov with your name, organization, and supplemental data and reports only. Please confirm below whether you have submitted additional materials.*

In lieu of separately emailing supplemental materials, we would note that ABA maintains a repository of AI resources, the vast majority of which are publicly available, on www.aba.com/AI.

Question #3*: Would you like to provide an email address, potentially allowing us to contact you for further details? If so, please include your email address below.*

In the event of any follow-up, please reach out to Chris Fisher, Vice President for Congressional Relations, at chrisf@aba.com.

White House Actions on AI

Question #4*: Please share your views on this federal review process, including recommendations for the Treasury and its role in the process.*

ABA believes the program represents a sound basis for additional action. However, it will ultimately be necessary for the executive branch to act pursuant to Congressional action in order to fully extend appropriate oversight mechanisms to developers of frontier AI models. Further, more public/private coordination is needed to deliver timely, actionable processes that balance innovation with controls.

ABA supports efforts to develop a sustainable national process to manage, prioritize, and control vulnerability disclosure, testing, and remediation at scale. This process should focus on high-impact findings affecting widely deployed software that supports critical systems. It should also include liability protections that enable firms to share the information necessary to accelerate confidential vulnerability remediation without fear of increased legal exposure. In addition, the process should focus on core service providers that deliver essential back-end infrastructure for banks, including transaction processing, account management, and digital banking platforms.

On July 14, the White House issued a press release announcing "Gold Eagle," which implements the AI cybersecurity clearinghouse outlined in the President's June 2 executive order, "Promoting Advanced AI Innovation and Security."[4] ABA and its member banks look forward to working with the Administration as it implements Gold Eagle.

It is critically important for the U.S. Congress to reauthorize the Cybersecurity Information Sharing Act of 2015 before it expires on September 30, 2026, to preserve privacy, liability, and

[4] https://www.federalregister.gov/documents/2026/06/05/2026-11415/promoting-advanced-artificial-intelligence-innovation-and-security.

antitrust protections so that banks can confidently share information about cyber threats, vulnerabilities, and incidents with other private-sector firms and U.S. government agencies.[5] ABA recommends that the U.S. government adopt a "whole-of-industry" approach to ensure that all entities have access to technical assistance, tools, or other support for patching and other cybersecurity activities.

The financial sector has a long history of collaborating internally and with the U.S. Department of the Treasury and financial regulators to prepare for and respond to AI and other emerging technologies. In collaboration with Treasury and the FSSCC, the sector recently released a suite of resources to help firms maximize the benefits of this technology while mitigating the risks posed by adversarial uses of AI (see the link in footnote 3). Financial institutions have significant experience defending against sophisticated cyber adversaries that are intent on disrupting the financial system and the infrastructure underlying the global economy. Responsibility for managing the resilience of critical services resides with financial institutions, which must meet the expectations of both their customers and regulators.

As a result, the sector has well-defined and routinely practiced disaster recovery, business continuity, and resilience plans for responding to cyberattacks and operational outages. These plans not only outline coordination and communication within the financial sector but also formalize financial institutions' long-standing collaboration across industry and government to better prepare for and manage risk.

The formation of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999 and the FSSCC in 2002 have substantially enhanced information sharing about threats facing the sector and enabled executive-level communication during crises. These mechanisms can be leveraged to address current threats affecting the entire sector.

Question #5*: How should the Administration ensure that the rollout of the NSPM-11 is done properly, especially when it comes down to humans maintaining control?*

ABA declines to respond to this question as outside the scope of its remit. Nonetheless, we generally observe that there are many forms of human oversight. For additional detail, please refer to the Financial Stability Board's (FSB) Consultation Report on Sound Practices for Responsible Adoption of Artificial Intelligence.[6]

Anthropic's Mythos and OpenAI's GPT-5.5-Cyber

Question #6: *What responsible AI frameworks have financial services and housing firms adopted and complied with prior to Mythos and GPT-5.5-Cyber developments? How should firms rethink these practices?*

[5] See joint trade association letter urging Congress to reauthorize CISA 2015; available at https://www.aba.com/advocacy/policy-analysis/letter-to-congress-on-cisa-september.
[6] See https://www.fsb.org/uploads/P100626.pdf, pages 41-44, particularly page 42 (45-48 of the PDF).

Historically, banks have established and maintained very strong cybersecurity programs to protect safeguard personal information and other sensitive data with which they are entrusted. However, the advent of advanced forms of AI pose a significant test that demands urgency, discipline, and rigor to identify and remediate vulnerabilities at speed and scale.

Banks are ultimately responsible for their own compliance programs, tuned to particular circumstances and overall risk appetite. Hence, while there are many frameworks they consult and leverage (e.g., the National Institute of Standards and Technology's AI Risk Management Framework (NIST AI RMF),[7] they must adapt to fit the three lines of defense within their institution.[8] Moreover, banks typically have technology-neutral approaches to risk mitigation. Thus, their cyber and IT teams are fully integrated into the apparatus, alongside other workstreams responsible for their own domains. Nonetheless, advances in frontier models require adaptation. In addition, agentic AI (which by its very nature has greater autonomy and is more difficult to constrain) may necessitate technical, hard-coded solutions.

The Cyber Risk Institute (CRI), with input from ABA, other associations, and more than 100 financial services companies, released the Financial Services AI Risk Management Framework (FS AI RMF) in 2026.[9] The framework provides practical, targeted guidance that evolves with AI technologies to support trustworthy, resilient deployment across the sector. Developed through industry-led public-private collaboration with input from U.S. and international agencies, the framework is structurally aligned with the NIST AI RMF (see footnote 7) and expands and operationalizes it through 230 control objectives tailored to financial services. It is designed to help institutions of all types and sizes manage and govern AI risk while supporting responsible innovation.

Specifically, the FS AI RMF:

- Translates high-level AI principles into actionable, sector-relevant control objectives and implementation guidance;

- Supports consistent evaluation, benchmarking, and maturation of AI governance across institutions and supply chains; and

---

[7] https://www.nist.gov/itl/ai-risk-management-framework

[8] The first line are business units, which are generally responsible for the risk associated with their business strategies. They are ultimately accountable for the risk and performance within the framework set by bank policies and procedures, and are responsible for ensuring processes are properly developed, used, and evaluated.

The second line is the control function. The responsibilities include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place. Control staff should have the authority to restrict business operations and order corrective action. Control work can be done in a way that prioritizes the greatest risk.

The third line is the bank's internal audit function. The third line's role is not to duplicate risk management activities but to evaluate whether risk management is comprehensive, rigorous, and effective. They should possess expertise and document findings while at the same time exercising independence and not be involved in the first or second line of work. The third line should also verify that acceptable policies are in place, owners and control groups comply with those policies, validation work is conducted properly, and appropriate degrees of effective challenge are being carried out.

[9] https://cyberriskinstitute.org/artificial-intelligence-risk-management/

- Helps organizations assess their current AI adoption, define target adoption stages, and prioritize controls to close gaps incrementally and responsibly.

Question #7*: What are examples of provisions or issue areas in financial services and housing firms' internal guidance frameworks that may now require amplified safety measures?*

As frontier AI models continue to evolve, banks need practical tools to evaluate how their core service providers identify and manage emerging cybersecurity risks. ABA prepared a tool to assist banks with remediating cyber vulnerabilities.[10] We incorporate this document by reference, which provides an overview of the types of issues presented by advanced frontier models such as Mythos.

Developed in collaboration with ABA member experts from cybersecurity, third-party risk, core provider, and AI working groups—and informed by input from partner organizations, including CRI and FS-ISAC—this questionnaire is designed to help banks assess providers' preparedness for risks associated with advanced AI models. The questionnaire enables ABA member banks to request information directly from core service providers and supports their third-party risk management efforts. It is organized into 11 sections and references established frameworks, standards, and regulatory expectations.

Question #8*: What factors and who should determine which firms participate in Project Glasswing or related initiatives?*

Securing early access to these advanced models is essential for large financial institutions so they can proactively identify zero-day vulnerabilities and protect customers before those models are broadly accessible. Protecting the critical infrastructure is the primary goal. If left unaddressed, vulnerabilities in code could pose a risk to the security of the encrypted information and ultimately threaten the safety and availability of the U.S. financial system.

When deciding what organizations should participate in initiatives such as Project Glasswing, members of the critical infrastructure, including Global Systemically Important Banks (GSIBs), must be included. Most non-GSIBs rely on service providers for their technology, and do not have a direct relationship in setting up or maintaining the code. As such, those banks would maximize their benefit by being consulted and informed as appropriate by relevant core service providers or industry groups.

Question #9*: What systems, protocols, or deliverables should be in place to ensure that such access to advanced AI systems does not create a competitive disadvantage to firms that do receive access?*

[10] Publicly available at https://www.aba.com/news-research/analysis-guides/ai-assisted-vulnerability-detection-and-remediation

Care must be taken to balance private property rights with pro-competitive outcomes. Moreover, given the sensitive nature of the information at hand, the disclosure of information should be meticulously managed to avoid it falling into the hands of bad actors. Ultimately, access to these systems should be tied to the business interest in using them (i.e., either directly or via a service provider) as well as the technological capability to identify and remediate software defects.

Model Fairness and Explainability

***Question #10**: What kinds of explainability standards should Congress and/or regulators establish to allow affected individuals to understand how AI systems used by the financial services and housing industries reach their decisions, such as in underwriting decisions that may result in credit denials?*

The Equal Credit Opportunity Act (ECOA) and its implementing regulation, Regulation B, along with the Fair Credit Reporting Act (FCRA) form the statutory backbone of consumer adverse action notice requirements. Under these statutes creditors must provide applicants with specific reasons for an adverse action, disclose key factor codes, and provide relevant credit score information whenever credit is denied or offered on less favorable terms. These statutory requirements apply equally regardless of the technology utilized to make an underwriting determination.

Explainability standards should be designed around what is meaningful and actionable for the consumer, not around technical disclosures that are unlikely to help consumers or that duplicate or conflict with existing legal frameworks. Rather than creating new legal frameworks, Congress should clarify that existing regulations apply to AI. Depository institutions have long complied with rigorous explainability and consumer disclosure requirements governing credit decisions. The same expectations should apply whether or not AI (however defined) is used in the decision-making process.

Indeed, that is the approach Congress has taken to date in laws that prohibit discrimination in credit and housing, and that require transparency in credit-related decisions. The ECOA requires creditors to provide the principal reasons for denial in writing to each credit applicant; and the ECOA and the Fair Housing Act prohibit discrimination in all types of credit and housing-related activities.[11] In addition, the FCRA requires creditors to explain adverse credit decisions and risk-based pricing decisions based on credit reports or credit scores, to applicants in writing.[12] These laws are technology neutral and apply to decisions and actions guided by AI. The ECOA and

[11] *See, e.g.,* 15 USC 1691 et seq. (the Equal Credit Opportunity Act); 42 USC 3601 et seq. (the Fair Housing Act). ECOA requires written adverse action notices with reasons in 15 USC 1691(d), which is implemented by the CFPB's Regulation B at 12 CFR 1002.9. In addition, mortgage lenders must report the reasons for denial for each application, to the CFPB under its Regulation C, 12 CFR 1003.4(a)(16), which implements the Home Mortgage Disclosure Act.

[12] *See* 15 USC 1681m(a), g(g) and m(h).

FCRA already provide a solid foundation for adverse-action explanations and consumer rights, and generally satisfy AI-specific considerations.

Question #11*: What pre-deployment and post-deployment controls should Congress and/or regulators require for AI models in connection with model inputs, weights, and other technical elements when used in the financial services and housing industries?*

Pre-deployment validation has long served as the industry standard for model governance. In conventional quantitative modeling, pre-deployment validation relies on evaluating a model's mathematical baseline by comparing inputs directly against deterministic outputs prior to the model's initial release. However, deep learning models (including generative and agentic AI) operate on probabilistic, non-deterministic structures where identical inputs can yield varied outputs depending on specific context, prompt engineering, or real-time data inputs. Consequently, forcing non-deterministic models into rigid, pre-deployment validation frameworks is inherently ill-suited and creates unnecessary supervisory friction without meaningfully reducing risk.

Policymakers should begin transitioning the governance of probabilistic models to a more dynamic, outcomes-based framework that prioritizes continuous monitoring and post-deployment auditing over pre-deployment assessments. Where necessary and appropriate based on risk profile, pre-deployment efforts may still be utilized to validate developmental and purpose soundness. However, a dynamic approach allows banks to oversee models in real-time as they interact with live data. Regulators could consider the value of automated red-teaming for post-deployment model auditing. This involves leveraging adversarial AI to continuously probe an already-deployed model for hallucinations, biases, or security vulnerabilities. The Treasury Department and CRI have underscored that as AI tools gain autonomy, the ability to conduct automated adversarial testing will be essential for maintaining sector-wide resilience.

By formalizing support of such mechanisms, policymakers can help provide banks with the operational clarity necessary to more confidently deploy innovative AI solutions while maintaining the integrity of the financial system.

Model Risk Management

Question #12*: What changes, if any, should regulators and Congress consider making for the Revised Guidance on Model Risk Management, in light of recent AI developments?*

ABA is supportive of the revisions made to the prudential agencies model risk management guidance. However, we also believe that the banking agencies should be encouraged to adopt additional guidance to provide a durable, credible framework to set forth sound practices for the risk management and governance of generative and agentic AI. This new guidance should build

on and be consistent with the materials currently under development by the FSB.[13] The issuance must be subject to public notice and comment, and should address items such as:

- Reinforce that controls and governance should be applied proportionately based on firms' risk assessment, and AI systems with a higher risk profile should be subject to proportionately higher controls;

- Revised language should be clearer on the expectations (or lack thereof) for lower risk activities (validation vs. control review vs. exclusion);

- Assessment of the conceptual soundness of generative AI models;

- Types and level of performance testing for various large language model types (foundational, purpose built, smaller and trainable open-source, Retrieval Augmented Generation-powered generative AI, etc.). Risk treatment may scale depending on the degree of the banks' involvement, and performance validation may require industry benchmark tests as well as specific use case benchmark tests;

- Expectations on the relationship of model risk management with respect to other control domains, such as data and technology risk, with banks permitting to leverage existing processes;

- Validation procedures should be flexible and risk-based with the recognition that traditional methods, like explainability, may not be necessary or practical for all AI tools. Validation should account for alternative methods, including AI-powered checks. Accordingly, the guidance should focus on the outcomes rather than specific methodology; and

- Delineate responsibilities for oversight of third-party AI models.

We would emphasize that the agencies made it clear that, even though out of scope of the revised model risk management guidance, banks should maintain "appropriate governance and controls for any tools, processes, or systems not covered in [the] document."[14]

Further, Congress and regulators should support modernized AI supervisory expectations, anchored in existing prudential, consumer, cybersecurity, privacy, model-risk, third-party-risk, and operational-resilience frameworks. Banking regulators are best positioned to supervise AI use in context, using their sector expertise and existing supervisory tools. Expectations should recognize that banks may use different controls for different AI systems, including traditional models, machine learning, generative AI, and agentic AI. Similarly, low-risk internal productivity tools should not be governed like high-impact consumer, credit, fraud, or trading applications.

Data Privacy and Disclosures

[13] Supra, note 6; https://www.fsb.org/uploads/P100626.pdf.
[14] https://www.federalreserve.gov/supervisionreg/srletters/SR2602a1.pdf at footnote 3, page 3.

***Question #13**: How should Federal laws relating to data privacy for the financial and housing industries be amended to address the privacy risks from AI? Do they need to be amended in any way to simultaneously ensure that financial institutions can conduct appropriate identity verification and financial crime compliance?*

In many respects, existing privacy laws applicable to banks (e.g., the Gramm-Leach-Bliley Act, or GLBA, and its implementing Regulation P) effectively govern the collection, use, and sharing of personal information. There may be certain targeted changes that can improve transparency of when and how AI tools are being used, but in general existing financial services privacy laws, when properly applied and enforced, generally address risks from AI.

***Question #14**: What steps can Federal regulators take, utilizing existing authorities, to improve data privacy in the financial and housing marketplace for the benefit of consumers? How can this be balanced, too, with the necessary access to data in areas like customer identification and financial crime compliance?*

Regulators should clarify that existing GLBA obligations apply to data shared for AI applications, as they would for any other type of nonpublic personal information. This includes personal data shared with service providers as well as for transactional and other exceptions pursuant to Regulation P (which includes "with the consent or at the direction of the consumer, provided the consumer has not revoked the consent or direction"). [15]

The real challenge has to do with a level playing field. Although banks and other depository institutions are supervised for compliance, other types of entities are not even though they also deliver financial products and services. In addition, GLBA has safeguarding requirements, such as "insuring the security and confidentiality of customer records and information, protecting against any anticipated threats or hazards to the security or integrity of such records, and protecting against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." [16] Ensuring these obligations are observed by all entities, regardless of what financial services they provide, would go a long way to protecting consumers and preventing data leakage and breaches.

Congress could also pass privacy legislation that would in many respects close these gaps and modernize existing law. This would include bills such as the House Energy & Commerce Committee's SECURE Data Act (HR 8413) and the House Financial Services Committee's GUARD Financial Data Act (HR 8398).

---

[15] https://www.ecfr.gov/current/title-12/chapter-X/part-1016/subpart-C/section-1016.13; https://www.ecfr.gov/current/title-12/chapter-X/part-1016/subpart-C/section-1016.14; https://www.ecfr.gov/current/title-12/chapter-X/part-1016/subpart-C/section-1016.15.

[16] 15 USC 6801(b); https://uscode.house.gov/view.xhtml?req=(title:15%20section:6801%20edition:prelim)%20OR%20(granuleid:USC-prelim-title15-section6801)&f=treesort&edition=prelim&num=0&jumpTo=true.

Question #15*: What customer notice and disclosure regimes should be applied to financial institutions and housing firms that utilize AI (either internally or provided by a third-party vendor) in providing a product or service to a consumer?*

As discussed, the ECOA and FCRA require written notices of adverse actions, including reasons and information about the use of credit reports and credit scores. ABA believes that existing notice and disclosures are adequate from a compliance floor perspective. However, some entities may elect to provide additional transparency as a competitive differentiator. Policymakers and firms should be mindful of disclosure fatigue.

Question #16*: What steps can Congress and/or regulators take to improve guidance relating to the mapping of data supply chains relating to the use of AI?*

Congress and regulators should make it clear that existing law, such as GLBA and FCRA applies to data relating to the use of AI where appropriate. In addition, downstream use by nonbanks remains inadequately scrutinized and should be bolstered by new or existing supervisory authorities. As ABA has consistently stated, agencies already possess sufficient powers; the key will be to apply them consistently across the ecosystem to nonbanks as well as traditional depository institutions.

Question #17*: Would it be helpful to provide financial institutions that wish to use vendor-provided Gen AI systems a standardized description that identifies what data was used to train a model, where it came from, and how any data submitted to the model will be incorporated? If so, what steps should Congress and/or regulators take in this regard?*

Absolutely, the answer is yes. This idea is related to model/system cards and would be invaluable.[17] In order to encourage use of such disclosures, Congress and/or regulators should include them as part of a larger standard-setting organization or AI center of excellence that include safe harbors.

Question #18*: What regulations should Congress establish that could standardize how publicly traded companies report the way they use AI?*

Such a disclosure is unnecessary. If AI use is relevant to the business's performance, it would be reported in due course.

Third-Party Service Providers

Question #19*: What steps should Congress and regulators take to heighten monitoring of emerging risks from the use of AI in the financial services and housing industries?*

[17] See, for instance, Anthropic's system cards; available at https://www.anthropic.com/system-cards.

The financial services industry is already subject to a mature risk management framework governing deployment of AI applications. Fragmented standards increase compliance costs, slow deployment, and can undermine the ability of banks to deploy AI safely and consistently across states and markets. Congress should therefore establish a nationally harmonized, risk-based federal AI framework for federally supervised banking activities that preempts conflicting state and local requirements while preserving strong consumer protection, fair-lending, privacy, cybersecurity, operational-resilience, and safety-and-soundness outcomes.

In a report, the House Bipartisan Task Force on Artificial Intelligence (from the 118th Congress) recommended a "sectoral approach […] to financial services regulation" that ensures "primary regulators" can "leverage their expertise."[18] There is an ongoing risk that states will adopt laws governing AI which will stifle innovation by imposing conflicting and unnecessary requirements on financial institutions. In some cases, these laws could impact the way many financial institutions have used AI for more than a decade. Therefore, any AI-specific federal laws or provisions must recognize banks' existing compliance framework and not impose duplicative or inconsistent requirements. Congress must pass comprehensive laws that builds on this established risk management framework with strong preemption of state requirements. These laws should create baseline standards that are not duplicative or inconsistent with the enterprise risk management obligations of banks.

Regulators should focus on substantive risks—such as model inputs, outputs, and outcomes—rather than technical minutiae. Improper supervisory practices can drive innovation away from regulated banks and to less regulated entities that do not provide the same degree of consumer protection and financial stability. As highly regulated entities, banks require clarity from the agencies conducting oversight. Each bank has its own risk appetite and process for making decisions, but the ability for the bank to take appropriate actions pursuant to that risk appetite is key for their ability to endure and flourish as financial activity becomes increasingly digital. Banks must be empowered to make decisions based on common sense and best practices, including in AI matters.

***Question #20**: The Trump Administration has generally reduced enforcement and supervision efforts by agencies. What actions can Congress take to ensure there remains adequate oversight of third-party vendors used by financial services firms, particularly during periods of reduced agency enforcement and supervision capacity?*

The federal banking agencies possess significant authority to supervise third-party service providers, including through the Bank Service Company Act (BSCA), and the CFPB has additional supervisory authority over certain larger participants. Congress should use its oversight function to better understand how regulators exercise these powers and whether service provider examinations are appropriately focused on the third parties that present the greatest risk to financial institutions, consumers, and the broader financial system.

[18] Report on Artificial Intelligence, Bipartisan H. Task Force on Artificial Intelligence, 118th Cong., at 240 (Dec. 2024), https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/6676530F7A30F243A24E254F6858233A.ai-task-force-report-final.pdf.

Specifically, Congress should evaluate:

- Whether the agencies are using their BSCA authorities as intended and whether the BSCA should be amended to reflect modern banking practices;

- Whether regulators have adequate visibility into emerging risks arising from fintechs, core service providers, cloud providers, and other critical third parties; and

- Whether regulators adequately monitor concentration risk among critical service providers.

Congress should also explore whether and how regulators should strengthen and modernize service provider examination programs. This could include:

- Updating the frameworks regulators use to determine which providers should be examined;

- Ensuring that examination resources are directed toward service providers that present the greatest risk;

- Evaluating service provider readiness to support bank compliance obligations; and

- Incorporating operational resilience, incident reporting, API security, and emerging technology risks into the scope of service provider examinations.

Finally, Congress should evaluate whether regulators provide banks with timely access to service provider examination findings, including actionable information that banks can incorporate into their own third-party risk management programs.

Question #21*: How can Congress ensure that a wide range of smaller financial institutions, including community development financial institutions (CDFIs) and minority depository institutions (MDIs), remain competitive in their ability to access and use AI provided by third-party vendors compared to larger entities that can develop AI systems internally?*

Demand for use cases should drive AI development, and in many cases banks of all sizes find vendor-provided AI fulfills their needs. Nevertheless, regulatory clarity and stability are needed to ensure that governance programs can continue to mature. Many smaller financial institutions are adept at cross-functional collaboration and have the right people embedded across their organizations. However, they would benefit from consistent messaging from examiners and policymakers as to which of their existing workstreams should be formalized and iterated upon.

Liability

Question #22*: What liability, if any, should be applied to financial institutions and/or third-party service providers used by financial institutions to the extent the use of AI contributes to violations of Federal law or regulation, especially where consumers are harmed? What law(s) should be amended to create this liability framework? Should there be safe harbors provided in certain circumstances? Please explain why any proposed changes may be warranted.*

Generally speaking, ABA believes this should be a technology-neutral consideration. However, ABA has become aware that some vendors are disclaiming any responsibility for the outputs of their AI products and services. This is especially concerning given a sizeable difference in market power/negotiating leverage between banks and frontier AI model developers, meaning financial institutions may not have full visibility into third-party systems. Third-party service providers should stand behind their AI products as they would outputs of other tools.

With this in mind, policymakers can focus on indemnification and liability cap provisions to avoid an unconscionable apportionment of liability away from developers and towards deployers. Banks primarily operate as deployers in the AI tech stack and face significant downstream exposure if a model failure causes losses; therefore, ensuring clear risk allocation and fair liability protections will be critical.

A federal framework should allocate obligations to the actors best positioned to manage them, while preserving banks' responsibility for deployment, governance, and use in context.

Capital Markets, Investor Protection, and Capital Formation

Question #23*: What standards should Congress and/or the SEC establish for the use of AI by issuers in preparing public company disclosures, periodic reports, and offering documents—including with respect to officer certifications under Sections 302 and 906 of the Sarbanes-Oxley Act, internal controls over disclosure, and liability under Sections 11 and 12 of the Securities Act of 1933 and Rule 10b-5 under the Securities Exchange Act of 1934?*

ABA declines to respond to this question as outside the scope of its remit.

Question #24*: How should regulators address risks that AI systems pose to market integrity—including AAI-driven trading strategies, AI-generated content used to influence prices, and synthetic-media-driven market manipulation? What additional tools, if any, do the SEC, Commodity Futures Trading Commission (CFTC), Financial Industry Regulatory Authority (FINRA), and Municipal Securities Rulemaking Board (MSRB) need to detect, prevent, and prosecute AI-enabled fraud, spoofing, and market manipulation,51 particularly when conducted across platforms or through autonomous agents?*

ABA declines to respond to this question as outside the scope of its remit.

Question #25*: What obligations should apply to investment advisers and broker-dealers that use AI in connection with recommendations and advice to retail and institutional clients, including with respect to fiduciary duty under the Investment Advisers Act, Regulation Best Interest, conflicts of interest arising from the use of third-party AI vendors, model and algorithm testing and validation, and supervision and recordkeeping?*

ABA declines to respond to this question as outside the scope of its remit.

Question #26*: What transparency, accountability, and disclosure standards should apply to the use of AI by proxy advisory firms, by asset managers and other institutional investors casting votes on behalf of clients, and by issuers in shareholder engagement and the preparation of proxy materials?*

ABA declines to respond to this question as outside the scope of its remit.

Question #27*: What disclosure, valuation, and risk management standards should apply to the use of AI by private fund advisers—including private equity, hedge fund, and private credit advisers—particularly in light of expanding retail access to private markets through private funds, so-called "alternatives," interval funds, BDCs, tender-offer funds, and similar vehicles, and the growing role of AI in valuation, due diligence, and underwriting of illiquid assets?*

ABA declines to respond to this question as outside the scope of its remit.

Question #28*: How can Congress and the SEC promote responsible AI-enabled capital formation that broadens access to capital for small businesses, startups, and underserved entrepreneurs—including through Regulation A, Regulation Crowdfunding, and other exempt offerings—while ensuring that AI tools used to evaluate, market, or match investors with offerings do not introduce new fraud, suitability, or disparate-outcome risks?*

ABA declines to respond to this question as outside the scope of its remit.

Question #29*: What evidence exists regarding the use of AI by investment advisers, broker-dealers, registered investment companies, and other market participants to reduce intermediation costs—including advisory fees, fund operating expenses, transaction costs, and execution costs—for retail and institutional investors? What steps, if any, should Congress and the SEC take to ensure that AI-driven cost savings are passed through to investors, supporting the long-term growth of retirement and other household savings, rather than retained as additional firm revenue?*

ABA declines to respond to this question as outside the scope of its remit.

***Question #30**: In what ways is AI being deployed—or how could it be deployed—to expand retail investor access to portfolio construction, personalized financial planning, tax-efficient asset location, risk management, research, and other capabilities historically available primarily to high-net-worth and institutional investors? What standards or guardrails would be needed to ensure that such AI-enabled services satisfy applicable fiduciary, suitability, supervision, and anti-fraud obligations while remaining accessible at low costs?*

ABA declines to respond to this question as outside the scope of its remit.

***Question #31**: What evidence exists regarding the use of AI to improve investment outcomes—through, for example, improved portfolio construction, execution quality, rebalancing, dynamic risk management, or tax optimization—for retail and institutional investors? How can Congress and regulators distinguish between substantiated AI-driven performance improvements and unsubstantiated marketing claims, and what disclosure or substantiation standards should apply to AI-related performance representations made to investors?*

ABA declines to respond to this question as outside the scope of its remit.

Housing

***Question #32**: What tenant protections should be ensured in PropTech?*

ABA declines to respond to this question as outside the scope of its remit.

***Question #33**: What is specifically needed to ensure transparency and clarity in algorithms used on online real estate platforms, automated valuation models, automated underwriting systems, electronic closing products and other PropTech so that regulators and Congress can promote responsible innovation while ensuring access to fair and affordable housing and prohibiting disparate outcomes and/or discriminatory practices?*

Congress and regulators should take care to preserve confidential commercial information, as protection of property rights encourages innovation. Nonetheless, many companies may find "open source" models to be highly valuable. In addition, as detailed above in the response to Question #17 model/system cards can provide assurances to both deployers and examiners. Finally, the supervisor and outcomes-based analysis can shed light on performance of the AI tools; however, evaluators must be mindful of what they are comparing against. For example, while the AI systems may not be perfect, they might perform more consistently than an aggregate of human employees.

***Question #34**: What actions should the FHFA and other similar agencies take to oversee PropTech and ensure its compliance with fair lending laws and regulations?*

There is already a proven blueprint for oversight as represented by the federal regulators with depository financial institutions. Encouraging development of the three lines of defense approach to operations (see footnote 8), coupled with effective supervision, would go a long way to creating a culture of compliance in the broader ecosystem.

National Security

Question #35*: How can Congress and regulators work with the financial services industry to address the threat of bad actors using smaller institutions to access and subsequently compromise the core banking infrastructure (traveling through the smaller institution's systems into partner entities)?*

Congress and regulators should build on the voluntary programs begun by the Administration to encourage strong cybersecurity baselines across the tech stack of AI vendors and core service providers. The creation of standard-setting organizations would help lead to this result.

Question #36*: Banks and technology firms are hesitant to invest heavily in the development or rollout of new technology, for example, to combat financial crime, without knowing whether regulators will accept the outcomes for use by financial services institutions. Yet regulators and lawmakers cannot enshrine such technology without understanding it fully and without the technologies' being deployable, following development and testing. What are ways in which the private sector and government may work together to bridge that gap without endangering, customer data, civil rights, or more, in the process?*

Cooperation between industry and government via public/private partnerships is needed to meet the challenges posed by advanced technologies in a way that not only enhances security, but also focuses on privacy, civil liberties, accessibility, and interoperability. Public/private partnerships can aid financial institutions in ascertaining the identity of customers transacting over an open network, and expand access to identity attribute validation services (see the linked report from FSSCC).[19] These tools help to reduce synthetic identity fraud and equip financial institutions to face the myriad new challenges in addressing identity, authentication, and authorization requirements as agentic AI applications begin to emerge.

Question #37*: How can examiners help financial institutions to adopt responsible AI technology that lowers financial crime risks affecting both the institutions and their customers? Specifically related to the yet-to-be-initiated "Testing Methods Rulemaking" mandated by the Anti-Money Laundering Act of 2020, what standards should the regulators promulgate in the rule for financial institutions to test and adopt new technology and internal processes?*

The prudential agencies have already begun to provide relief in this area with the clarifications to SR 26-2. Now, they should follow up with additional materials addressing generative and agentic AI.

[19] https://www.aba.com/news-research/analysis-guides/mitigating-ai-powered-attacks-policymakers

The most direct way for examiners to help banks innovate responsibly is to focus on things the bank can more easily control, such as inputs, outputs, and outcomes. Multiple ABA members report that, in recent memory, field examiners would stymie innovation efforts by needlessly focusing on granular matters (such as explaining the finer points of computer code) rather than areas of actual risk. This is true across all areas of innovation but is particularly the case with complex issues such as AI. Members share that, in some cases, field examiners who had no concerns with a particular workstream in one exam cycle raised issues subsequently, purely because the service provider supporting the workstream suddenly began to highlight "AI" in its marketing materials. Congressional and regulatory action could help to minimize this type of potential puffery by promoting a clear, legal lexicon of terms.

Question #38*: Some experts claim that methods of identifying the customer will shift dramatically due to AI models and tools, potentially changing how financial institutions create and execute their "Customer Identification Programs," as required for financial crime compliance and other purposes. Please describe those potential changes, the benefits and drawbacks to different stakeholders, and how law and regulation related to or impacted by customer identification may be adapted to capitalize on the new tools.*

ABA declines to answer this question as the response would vary widely among banks. Each bank has its own internal risk appetite and creates business operations that reflect it as well as their culture and organization. The interplay between these factors leads to a cat's cradle of business decisions.

Export-Import Bank

Question #39*: Regarding the ExportAI Initiative, recently launched by EXIM to, "strengthen U.S. global competitiveness and accelerate the export of American artificial intelligence technologies," are the typical EXIM statutory standards met or sufficient for exports from this industry (such as the specific transactions face private financing gaps or the exports support U.S. jobs and content)? What other standards might be considered, including those which may be new or unique to the AI sector?*

ABA declines to respond to this question as outside the scope of its remit.

Question #40*: EXIM appears to be contemplating the financing of domestic AI data centers and, perhaps, their utilities. Would doing so support EXIM mandates such as job creation, support to small business, support to American exporters, and leveling of the playing field against competition from companies backed by foreign ECAs? Why or why not?*

ABA declines to respond to this question as outside the scope of its remit.

Workforce and Training

Question #41*: How should AI developers and Congress best address workforce challenges with AI deployment, including potential inequalities resulting from job displacement?*

ABA declines to respond to this question as outside the scope of its remit.

Question #42*: There is evidence that the adoption of Gen AI by businesses has already resulted in a decline in employment for younger workers, with the unemployment rate increasing for new college graduates.64 What can be done to ensure that entry level workers are given the same opportunities for employment, experience, and growth as previous generations?*

ABA declines to respond to this question as outside the scope of its remit.

AI Data Centers

Question #43*: How do data centers affect grid capacity, water quality and usage, electric consumption, and other environmental impacts in different communities?*

ABA declines to respond to this question as outside the scope of its remit.

Question #44*: Some states have reportedly granted tax breaks to data builders and operators, and related companies, to encourage the growth of data centers in their communities. Can you describe how such tax breaks and financing mechanisms are structured?*

ABA declines to respond to this question as outside the scope of its remit.

Question #45*: In what ways are taxpayers subsidizing the presence of data centers in their communities, as well as long-term AI development in the U.S.?*

ABA declines to respond to this question as outside the scope of its remit.

Question #46*: Some state and local governments have announced moratoriums on new data centers in their communities. What federal safeguards should be established, in line with such moratoriums?*

ABA declines to respond to this question as outside the scope of its remit.

Question #47*: Would community benefits agreements alleviate potential concerns arising from data center presence? If so, what community benefits agreement should companies propose before establishing data centers and building AI infrastructure in communities?*

ABA declines to respond to this question as outside the scope of its remit.

Question #48*: In some communities, companies are converting Bitcoin mining facilities into AI data centers. Please describe potential challenges, risks, and benefits arising from such transitions. Additionally, how does AI data center consumption compare to Bitcoin mining consumption?*

ABA declines to respond to this question as outside the scope of its remit.

Financial Stability

Question #49: *What steps should regulators—including the Financial Stability Oversight Council (FSOC), Office of Financial Research (OFR), and banking regulators—take while utilizing their existing authorities to address financial stability concerns relating to AI?*

The most important action would be clarifying principles-based expectations for supervised entities, while expanding the supervisory footprint to entities of all types operating in the broader financial services ecosystem. These bodies already possess sufficient authorities to make a large impact.

Question #50*: What steps can Congress take to improve authorities or modify laws to address risks that AI poses with respect to financial stability?*

One area emerging is the price of AI tokens. The costs of AI deployment can balloon unexpectedly, which has implications for the overall performance of banks, capital rules, and resiliency. Congress should encourage additional clarity on pricing and terms in an evolving market.

More generally, Congress can use its oversight function to encourage the exercise of dormant authorities; for example, pursuant to the BSCA. If it takes action, it should be to create a consistent federal standard for all sectors while recognizing existing obligations for the financial services industry.

Question #51*: To what extent should regulators utilize AI to better monitor the financial system and mitigate financial stability risks? What benefits and risks are there in doing so?*

It is essential for regulators to familiarize themselves with technology if they are to effectively oversee it. Moreover, like the banks they supervise, regulators should articulate how they are

using it and ensure appropriate controls (such as data protection of confidential information) are in place.

International Development

Question #52*: How can and should International Financial Institutions (IFIs) like the World Bank and the IMF help developing countries access advanced AI systems or support their integration?*

International coordination is generally welcome but care must be taken to avoid overly broad and prescriptive approaches that discourage innovative practices such as fine-tuning existing LLMs. Instead, a flexible risk-based framework adapted from that used by banks would be far more effective at both continuing U.S. leadership and mitigating potential harm.

Question #53*: The World Bank often talks about "Small AI, Big Impact." What examples of this have you seen in developing countries that could serve as models for future development activities globally and what were some of the "pros" and "cons" experienced in the execution of such projects?*

ABA declines to respond to this question as outside the scope of its remit.

Question #54*: Financial services are global and bad actors are global, both crossing international borders. There has been a reluctance by the Trump Administration, however, to share access to AI tools that might improve security globally. In general, how might the U.S. and its AI firms work together to protect the financial ecosystem in a manner that preserves U.S. interests as well as those of America's allies and partners?*

Where possible, the U.S. should encourage the availability of open source models. Nonetheless, highly sensitive areas may not be able to offer this level of transparency. It is exceedingly difficult to have a one-size-fits-all approach to AI technology when so many aspects of it are use case-specific. Furthermore, the easier the access to frontier models, the more likely they will be employed by adversaries.

Conclusion

ABA truly appreciates the opportunity to provide feedback on this salient issue. We look forward to continued engagement as Congress shapes its policy objectives in the rest of the 119th Congress and beyond.

Respectfully submitted,

American Bankers Association