Statement for the Record

On Behalf of the

American Bankers Association

before the

House Financial Services Committee

December 10, 2025

Statement for the Record

On Behalf of the

American Bankers Association

before the

House Financial Services Committee

December 10, 2025

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, *From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services*. The ABA is the voice of the nation's $25.1 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $19.7 trillion in deposits and extend $13.2 trillion in loans.

Banks are a unique sector already subject to an extensive compliance regime covering nearly all risks associated with artificial intelligence (AI), including fair lending and cybersecurity requirements. Federally regulated financial institutions undergo supervision, examination, and enforcement of their use of any technology, including AI. As such, the financial services sector is a model for how other industries can responsibly and effectively deploy AI at scale.

Introduction

There is a complex overlay of applicable laws, regulations, and supervisory guidance that is relevant to banks' AI usage. The most important of these are model risk management expectations issued from the Federal Reserve (Fed), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC).[1] In 2021, the Fed, the OCC, and the FDIC issued interagency guidance addressing model risk management to support Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Compliance (BSA/AML and OFAC).[2]

[1] SR 11-7, OCC Bulletin 2011-12, FIL-22-2017. Bank Secrecy Act/Anti-Money Laundering Compliance-specific guidance motivated the release of SR 21-8, OCC Bulletin 2021-19, and FIL-27-2021. The OCC also released a booklet for its examiners to use as an aid when supervising banks' model risk management programs. Links to all the model risk management materials can be found on www.aba.com/AI.

[2] SR 21-8, OCC Bulletin 2021-19, and FIL-27-2021, respectively.

It is also important to note that most banks are primarily reliant on vendors to supply their models and AI functionality. Accordingly, the interagency guidance issued by the Fed, the OCC, and the FDIC on third-party risk management is integral.[3] The document is principles-based and technology-neutral, which is entirely appropriate given the diversity of stakeholders and issues in the financial services ecosystem. This optimizes the ability of banks to identify concerns germane to their business model as they conduct due diligence on vendors and mitigate at a scale commensurate with their size and sophistication.

While the highly regulated nature of banks necessitate careful implementation to ensure compliance with consumer protection and safety & soundness requirements, banks should be empowered to make decisions based on common sense and best practices, including in AI matters.

Bank operations occur within a robust risk management framework often dubbed the "three lines of defense," which refers to the division of roles and responsibilities within a bank in order to identify, assess, and mitigate risks. The three lines of defense are discussed in the aforementioned model risk management guidance.[4]

- 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.

---

[3] Guidance on Third-Party Relationships: Risk Management, https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.

[4] *Supra,* note 2. *See:* SR 11-7, pp. 18-19.

Recent Regulatory Reform Efforts

We would like to acknowledge several recent actions by the Trump Administration that are positive steps towards promoting responsible innovation. For example, on October 6, 2025 the OCC issued Bulletin 2025-26—Model Risk Management: Clarification for Community Banks.[5] This bulletin recognizes that community banks use models for a broad range of activities, including underwriting credit; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; and determining capital and reserve adequacy.

Although it does not directly reference AI, the use of AI applications generally fits under the model risk management supervisory framework. The bulletin clarifies that community banks are to have flexibility in tailoring their model risk management practices, including the appropriate frequency and nature of validation activities, commensurate with the bank's risk exposures, its business activities, and the complexity and extent of its model use. The OCC does not require community banks to perform model validation on an annual basis, and the agency will not provide negative supervisory feedback solely for the frequency or scope of model validation as long as such is reasonably tailored.[6]

The OCC stated that the "bulletin is just the first step in refining model risk management guidance for all of the OCC's regulated institutions."[7] The bulletin, and the sentiment motivating it, are certainly welcome. ABA supports the OCC's efforts to enable innovation by community banks, and we look forward to engaging in additional efforts for banks of all sizes.

ABA has called on the prudential agencies to update the model risk management guidance, subject to notice and comment, in recent advocacy materials.[8] The nature of these updates are to make the guidance more reflective of bank operations, clarify applicability (or non-applicability) to particular AI usage, and to delineate the responsibilities when banks use third-party AI.

Additionally, the prudential banking agencies are taking steps to formalize examination reform. In pursuit thereof, the OCC issued Bulletin 2025-24—Examinations: Frequency and Scope for Community Banks on October 6, 2025.[9] Further, on October 30, 2025 the OCC and FDIC published a Notice of Proposed Rulemaking regarding Unsafe or Unsound Practices, Matters Requiring Attention that "would continue their effort to focus supervision on material financial

---

[5] https://www.occ.gov/news-issuances/bulletins/2025/bulletin-2025-26.html. By community banks, the OCC means national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations with up to $30 billion in assets.
[6] *Id*.
[7] https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-95.html.
[8] https://www.aba.com/advocacy/policy-analysis/letter-to-ostp-on-ai-reform.
[9] https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-24.html.

risks."[10] The Department of the Treasury and the Fed have also focused on innovation in financial services, particularly for community banks, which will have the effect of widening and deepening AI adoption in the provision of financial products and services.[11]

Recommendations for Congress

In a report, the House Bipartisan Task Force on Artificial Intelligence (118th Congress) recommended a "sectoral approach […] to financial services regulation" that ensures "primary regulators" can "leverage their expertise."[12] 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 the last several decades. Therefore, any AI-specific federal laws or provisions must recognize banks' existing compliance framework within the three lines of defense and not impose duplicative or inconsistent requirements.

Congress must pass comprehensive laws establishing an AI risk management framework with strong preemption of state requirements. These laws should create baseline standards that are not duplicative or inconsistent with current compliance obligations of banks.

Specifically, legislation should adhere to the below principles:

Avoid a Patchwork of Laws and Regulation. ABA encourages international and multijurisdictional cooperation to enact industry-focused laws with strong preemptions of existing laws. For AI, it is important for policymakers to avoid the patchwork of state data privacy laws that have been enacted given the potential adverse consequences for consumers, the economy, and national security.

Acknowledge Current Legal and Regulatory Framework for Financial Services. Any additional AI regulatory requirements should be practical, support innovation, and align with existing compliance practices. For example, any new AI legislation must acknowledge the statutory and regulatory frameworks already in place for the financial services sector such as the model risk management guidance and Gramm-Leach-Bliley Act (GLBA) protections.

---

[10] https://www.federalregister.gov/documents/2025/10/30/2025-19711/unsafe-or-unsound-practices-matters-requiring-attention; *see also* https://www.fdic.gov/news/press-releases/2025/agencies-issue-proposal-focus-supervision-material-financial-risks; *see also* https://www.fdic.gov/news/board-matters/2025/board-meeting-2025-10-07-1open for additional materials.

[11] *See* https://bankingjournal.aba.com/2025/10/bessent-outlines-policy-agenda-to-boost-community-bank-business-model; *see also* https://www.aba.com/about-us/press-room/press-releases/treasury-fed-regulatory-changes.

[12] 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.

Focus on Field Examination Reform. Congress should support the efforts of the prudential agencies in reforming field examination, including training supervisors to 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.

Fight Fraud and Combat Cybercrime. ABA strongly supports government actions that (1) create stricter penalties for use of AI to conduct criminal activity or financial crimes, (2) enhance identity and authentication; (3) support research activity that would help detect and prevent cyberthreats and fraud, (4) support workforce development efforts to ensure the workforce keeps pace with technical advances (e.g., AI-related training and certifications), and (5) strengthen public/private partnerships to increase awareness of cyber and fraud threats.

With respect to enhancing identity and authentication, it's important to emphasize that the emergence of generative artificial intelligence (Gen AI) has helped to supercharge the ability of attackers to fake likenesses and identities. Attacks that were once resource-intensive and difficult to execute have now become commoditized – with cheap or free deepfake tools powered by generative AI now able to spoof video, images, and voices. Paired with generative AI-composed phishing emails, financial institutions and their customers are now seeing a new wave of attacks that are largely indistinguishable to human perception – and can also fool many automated security tools. Deepfake incidents in the fintech sector are increasing. Financial institutions and their security partners are not able to address these threats alone; doing so will require assistance from and partnership with government.

There are two reasons why government needs to play a role. First, identity and authentication are heavily regulated in the financial services sector, with rules governing how financial institutions verify the identity of new customers, as well as how they authenticate customers signing into their accounts online. Some of these rules need to be updated – or in some cases, regulators need to clarify their intent – for financial institutions to feel comfortable in embracing newer tools such as passkeys or mobile driver's licenses that can thwart generative AI-powered attacks. Second, government – through a mix of Federal, state, and local agencies – is the only authoritative issuer of identity credentials in the United States. While those credentials can be used by customers in-person at a financial institution, there is in most cases no digital counterpart to those paper and plastic credentials that are suited for the online world. At a time when many industry security tools that try to predict whether someone is who they claim to be are coming under attack from generative AI, the need is greater than ever for government to help close the gap between physical and digital credentials.

Broadly speaking, federal and state governments can play an important role by prioritizing the development of next-generation remote identity proofing and verification systems, promoting the

use of strong authentication, coordinating with other countries and harmonize requirements and educating consumers and businesses about better identity and emerging identity threats.

Encourage Development of AI Centers of Excellence.[13] Congress should encourage the development of voluntary strategies for managing AI-related risks. One example would be a standardized disclosure template (model cards) shared for validation exercises, which would not require the transfer of confidential commercial information. Another avenue would be industry certifications to provide evidence of compliance for a baseline of fairness, transparency, and explainability; such programs would aid banks of all sizes and give AI developers incentives to build controls.

As touched on above, 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 (such as the Social Security Administration's Electronic Consent-based Social Security Number Verification Service, or eCBSV).[14] 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.

This coordinated approach could ultimately evolve into sector-specific AI Centers of Excellence like that suggested by the Trump Administration's AI Action Plan.[15] Although regulatory sandboxes are also contemplated by the Plan, these do not translate as well for highly regulated industries such as banks except in specific instances due to laws for consumer protection and safety & soundness. While most use cases therefore cannot be scaled in production, sandboxes could be of some utility to banks for scenarios that do not impact customers or existing regulatory requirements.

However, a collaborative open source environment such as an AI Center of Excellence could prove beneficial, allowing banks to centralize resources, including governance documents, due diligence materials, validation scenarios, and more as appropriate. Ultimately, this approach

---

[13] As used in this Statement for the Record, "AI Center of Excellence" borrows the language employed by President Trump's AI Action Plan (see footnote 15) and refers to a consortium of financial institutions, service providers/ other third parties, regulators, academia, and more collaborating on a common cause. The term can also be applied to standalone programs established within the respective participants themselves. Encouragement of the wider AI Centers of Excellence as contemplated by the AI Action Plan in no way precludes these individual initiatives, which are currently found at scale in many ABA members.

[14] https://www.ssa.gov/dataexchange/eCBSV/.

[15] "Winning the Race: America's AI Action Plan," https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf at page 8.

could lead to explainability methodologies that leverage a suite of coordinated risk management practices, including but not limited to data governance, weighted decision-making criteria, assurance and testing, and continuous risk monitoring. Sector-specific profiles mapped to relevant National Institute of Standards and Technology Risk Management Frameworks (NIST RMF) (e.g., NIST AI RMF and the NIST Privacy Framework[16]) would provide a strong foundation. An AI Center of Excellence could also include the sharing of certain information regarding supervisory findings to aid others in the ecosystem.

This holistic approach should include all participants in the AI ecosystem, including technology companies and non-financial industry actors, particularly because the economics of large language model production prevents internal development thereof and drives adoption of third-party offerings. Such work could be the foundation of interoperability across sectors and jurisdictions and would allow the entire ecosystem to innovate confidently. However, in order to gain sufficient adoption, the concept of creating an AI Center of Excellence would have to receive significant support from Congress and the relevant banking agencies.

Conclusion

As demonstrated above, the financial services sector has a robust risk management framework for deploying AI safely and soundly, which can be a model for nonbank industries. Prudential regulators are already taking steps to foster adoption, and Congress can lend its considerable weight and moral authority behind this development. Banks stand ready to work with policymakers and other industries on making improvements to this compliance regime.

Thank you once again for allowing us to provide our views on this very important topic.

[16] https://www.nist.gov/itl/ai-risk-management-framework; https://www.nist.gov/privacy-framework.