Statement for the Record

On Behalf of the

American Bankers Association

Before the

House Financial Services Committee

July 23, 2024

Building Success. Together.

Statement for the Record

On Behalf of the

American Bankers Association

Before the

House Financial Services Committee

July 23, 2024

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, *AI Innovation Explored: Insights into AI Applications in Financial Services and Housing*. The ABA is the voice of the nation's $24 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19 trillion in deposits and extend $12.4 trillion in loans.

Banks are a model for how other industries can explore AI-enabled use cases in a safe and sound manner. The compliance requirements, model risk management expectations, and supervision by specialized regulators has resulted in an environment of trust and responsible innovation. Accordingly, the financial services sector can be a leader alongside government to encourage the proliferation of these features. We urge Congress to apply those same standards to non-bank participants, and we look forward to working with this Committee, your colleagues in the House and Senate and other policy makers and stakeholders to ensure that outcome.

Introduction

Financial institutions have a long history of deploying and controlling risk related to novel technologies, and this includes both the traditional and generative iterations of the Artificial Intelligence (AI) spectrum. Moreover, just like other technologies banks' use of AI is subject to a strong foundation of compliance to manage risks, including: three lines of internal risk-management defenses; application of technology-neutral laws, regulations, and guidance; and validation of the effectiveness of the framework through regular examinations by the bank regulatory agencies.

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, 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 R&D Committee (FSSCC R&D), which the ABA Co-Chairs. Last year, the FSSCC R&D Committee convened a series of meetings with financial sector experts to explore the role of AI in cybersecurity and fraud which resulted in a six page report that the US Treasury included in its March 2024 report on AI and cybersecurity.[1] The US Treasury report was one of the many taskings in the October 2023 Executive Order on AI.

As discussed in greater detail below, ABA's comments are organized into four sections: (1) Regulation of AI; (2) How Banks Use AI; (3) Risk Management of AI; and (4) Recommendations for Policymakers.

I. Regulation of AI

AI is an umbrella term for various enabling technologies and is not a standalone program, product, or service. Rather, it is embedded into various bank operations, including security and products and services provided to our customers. While it is useful to attach definitions to AI for purposes of framing the discussion, ABA strongly believes that any legal or regulatory requirements must be technology-neutral and tied to a specific use case (for example, fair lending consumer protection laws applying whether or not AI is used in the provision of products and services).

There is a complex overlay of applicable laws, regulations, and supervisory guidance that is relevant to 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).[2] Technically, these do not apply to AI as such, but rather to models, but the guidance provides that "[w]hile outside the scope of this guidance, more qualitative approaches used by banking organizations— i.e., those not defined as models according to this guidance—should also be subject to a rigorous control process." 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).[3]

It is 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

[1] See, *Appendix*, https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf

[2] SR 11-7, OCC Bulletin 2011-12, and FIL-22-2017, respectively. The OCC also released a booklet for its examiners to use as an aid when supervising banks' model risk management programs; *see* https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.

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

FDIC on third-party risk management is integral.[4] 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.

Several agencies have issued materials that are relevant for stakeholders evaluating risks stemming from AI usage:

- A release by joint agencies clarified that consumer protection and anti-discrimination laws continue to apply whether or not AI is utilized.[5]
- The Consumer Financial Protection Bureau (CFPB) issued guidance documents pointing out risks of AI present in chatbots[6] as well as the importance of explainability in complying with Regulation B.[7]
- The Treasury Department and the Department of Homeland Security have issued reports that are likely to be useful to banks and other financial institutions in identifying, assessing, and mitigating certain forms of risk presented by AI-enabled use cases.[8]
- Finally, the National Institute of Standards and Technology (NIST) has developed a voluntary, industry-agnostic, and customizable AI Risk Management Framework (AI RMF) that has proven invaluable to banks in standing up and maturing their AI governance programs.[9] NIST recently unveiled its initial public draft of a generative AI supplement to the framework.[10] In a comment letter, ABA expressed support for the initial public draft and made several recommendations on how it could be improved.[11]

---

[4] 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.

[5] Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[6] CFPB, Advisory on chatbots in consumer finance, https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/.

[7] CFPB, Circular 2023-03, "Adverse action notification requirements and the proper use of the CFPB's sample forms provided in regulation B."

[8] *See* Treasury Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, https://home.treasury.gov/news/press-releases/jy2212; *see also* DHS Report on Mitigating AI Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators, https://www.dhs.gov/publication/safety-and-security-guidelines-critical-infrastructure-owners-and-operators.

[9] NIST AI RFM, https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF.

[10] NIST AI 600-1, https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf.

[11] *See* https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf.

Banks gather these various threads and form them into comprehensive governance structures that are iterated upon and matured over time, and strengthened by feedback received from bank examiners.

II. How Banks Use AI

Banks have a long history of using traditional AI within the risk management framework outlined above. "Traditional AI" can be thought of as a system designed to respond to a particular set of inputs. It "learns" from the data and makes decisions or predictions based upon the data, but does not create anything new. Some examples include chess programs, voice assistants such as Siri and Alexa, recommendation engines on Netflix, or Amazon or Google search algorithms. Traditional AI is generally predictable and has been vetted through years of usage and supervisory feedback. Typical traditional AI use cases by banks include fraud detection and prevention, marketing, cybersecurity, anti-money laundering activity, and credit underwriting.

Banks and regulators do not face the same challenges with traditional AI as is the case with "Generative AI," which can be thought of as a form of AI that can create something new from information it receives. Generative AI models are "trained" on a set of data and learn the underlying patterns to generate new data that mirrors the training set. This can include images, music and computer code, among other things.

Generative applications are still in the nascent phase; there is much more work to be done to fully understand and trust the technology, as well as the regulators' attitudes towards it. Further, there is a need to identify the right stakeholders to build proper guardrails. In the interim, banks are proceeding very cautiously with generative AI, particularly with regard to customer-facing applications. Banks would need to see significant improvement in performance to justify the additional costs and risks presented before making a switch from traditional AI applications to those powered by generative AI.

Examples of AI Use Cases

Banks are using traditional and generative forms of AI in the following ways:

- Cybersecurity- AI is used to detect and respond to potential cyberattacks more quickly and efficiently than human intelligence could accomplish alone. AI-based network security software can monitor incoming and outgoing network traffic to identify suspicious patterns to aid security analysts in their initial classification by reducing the number of false positives. Banks may also utilize generative AI to pinpoint malicious code as well as aide internal developers in identifying vulnerabilities in their own code.

- Fraud Prevention- AI models using predictive analytics help banks proactively find anomalies in transactions and identify outliers that do not conform with customers' past patterns or payment activity. AI models not only improve the performance of fraud detection capabilities, but also help catch fraudulent activity before it impacts customers.

- Lending- Banks use AI across lending processes to help identify accounts that can be approved for credit, as well as loan amounts and pricing. AI assists banks with evaluation of creditworthiness and improves efficiency in decision-making. It can also provide metrics around key life indicators such as attrition rates for mortgages.

- Customer Service- AI assists banks with learning how customers interact with their products and services. In addition, AI can perform sentiment analysis to gain insight into satisfaction. This data can be used to better understand customer interactions and how to improve them. Generative AI will also likely assist contact center personnel to understand customers' prior engagements when following up.

- Chatbots- Chatbots powered by traditional AI are commonly used and can respond with static responses to certain keywords. Customers gravitate towards these channels due to ease of use and preference for self-service. In fact, in certain circumstances many customers would rather interact with a chatbot rather than a human. Thus, routine questions could be handled by the chatbot, with referral to human beings for more complex issues. Moreover, they can also be leveraged for simulations to train employees on how to deal with complaints or other eventualities. Generative AI may further expand Chatbot capabilities.

- Marketing- Traditional and generative AI may help personalize content to optimize relevance for customers, but it must be tempered with strong privacy controls consistent with the banks' values, as well as legal and regulatory requirements.

- Risk Management- Banks can potentially use generative AI to generate a first draft of policies and procedures, or to summarize a description of applicable controls for the three lines of internal risk-management "defenses" (see Part III below). It can also aid in creating uniform formats that can make it easier to comprehend information submitted from various sources (for example, vendor information for due diligence purposes).

- Internal Document/Knowledge Management- One of the most intriguing use cases is connecting bank resources into an internal document management system. There are tools to gather necessary information across disparate sources and compile necessary information for employees (for example, contact center representatives). Moreover, the nature of generative AI makes it easier to ingest policies and procedures.

- Coding- The potential for generative AI to assist with routine coding is very promising.

III. Risk Management of AI

While there should not be a separate system for evaluating AI applications, use cases should be assessed through a robust framework to flag any inherent risks. A material feature of generative AI is its prompt-based nature, which lowers the barrier to access and expands the pool of potential users. This democratization requires cross-functional teams to identify, assess, and mitigate risks stemming from particular applications.

ABA members are confident that banks have constructed, or will be able to construct, a mature governance framework to mitigate AI risks. There has been a long history of banks incorporating emerging technologies into their operations. This is testament to the "three lines of defense" model used by banks, coupled with agency supervision.

Three Lines of Defense

The three lines of defense refers to the division of roles and responsibilities within a bank in order to identify, assess, and mitigate risks, which is provided in the model risk management expectations guidance, SR 11-7,[12] issued by the bank regulatory agencies.

- 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 be independent and document findings. The third line should possess expertise but should 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 is being carried out.

[12] SR 11-7, see pp. 18-19.

Risk-Mitigation Examples

Some examples of the risks that financial institutions mitigate through the governance framework are:

- Cybersecurity and Fraud- banks must identify vulnerabilities in their own systems caused by AI (such as potential data leakage or backdoors). They must also defend against increasingly sophisticated AI usage by bad actors.

- Privacy and Data Governance- the training data used to power foundational large language models is of questionable quality. Moreover, it is unclear whether proper consents are in place to use it. In addition, banks are mindful about how personal information is used by AI and whether there is sufficient disclosure and transparency.

- Bias and Fair Lending- Financial institutions are committed to ensuring that credit decisions are made in a fair and non-discriminatory manner. One of the most cited risks in the use of AI is the potential of historical data used to train models that may perpetuate societal harms. In order to combat this, banks utilize a rigorous validation process to allow them to understand a model's inputs, outputs and outcomes. They then conduct a statistical analysis as to performance in meeting their business needs. An exhaustive compliance review is a crucial step prior to deployment.

- Third-Party Risk Management- Given that vendors are an essential element of the AI ecosystem, banks have to conduct proper due diligence to understand how third parties deliver AI-enabled services, as well as how AI affects the third parties' own operations. Banks must then negotiate contractual provisions to mitigate risk and delineate responsibilities. Banks must be able to understand and explain third-party solutions in order to inform their customers and satisfy regulatory expectations.

- Illicit Finance- Many banks use AI and machine learning technologies as part of their risk-based approach to BSA and sanctions compliance. In order to adopt an effective risk-based approach, banks must have an accurate understanding of the actual risks associated with their business practices. Banks also need refined and accurate models to avoid expending unnecessary resources investigating false positives; while ensuring they do not miss important red flags. In addition, generative AI can be used by bad actors to create realistic identity documents. Treasury's Financial Crimes Network has warned about the dangers posed by fraudulent identity documents, for example, fraudulent passport cards.

Rather than bank use of AI, the most pressing danger for policy makers is how entities without such supervision, such as Big Tech developers, will safeguard consumers and preserve financial stability.

IV. Recommendations for Policymakers

ABA makes the following recommendations for Congress and other policymakers to consider in legislation, regulation or other policy decisions with respect to the use of AI:

Avoid a Patchwork of Laws and Regulation. ABA encourages international and multijurisdictional cooperation to enact technology-neutral, industry-focused laws with strong preemptions of existing laws that recognize banks' mature risk management framework. 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 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. In particular, by including an entity-level exemption for those subject to the Gramm-Leach-Bliley Act (GLBA), while creating a national technology-neutral framework to establish baseline standards for "same activity, same risk, same treatment."

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

Focus on the Risks of Third-Party AI Platforms. Any legislation related to AI should include focus on third-party non-bank AI models, tools, and platforms to impose the same obligations directly on such third parties and to require such providers to furnish sufficient credible, reliable information if used by financial institutions or in the financial services market, such as an independent certification of fitness and compliance with applicable laws. Requirements for banks to examine and monitor third-party AI algorithms, training data, or performance are not possible without third party cooperation. Regulators should focus on non-banks and technology companies that provide financial services or support financial services 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 currently the only industry with model risk management guidance in place from regulators.

Adopt Legislation to Implement Consistent and Flexible Industry Standards. Legislation should be developed by Congress that creates an environment for consistent nomenclature and flexible industry standards that will be key to ensuring that organizations are able to continue to develop and adopt emerging technologies. Legislation should also encourage updates to model risk management guidance to clarify the connection with AI-enabled use cases, subject to notice and comment from industry stakeholders.

Collaborate on Standardized Strategies for Managing AI-Related Risk. Finally, the financial services sector and policymakers should collaborate to develop standardized strategies for managing AI-related risk. This includes development of standardized disclosure templates for generative AI systems, and creating sector-specific guidelines based on AI frameworks to lead to more effective mitigation of emerging threats and ensure alignment with regulatory requirements and supervisory expectations. Cooperation between industry and government via public/private partnerships is also needed to meet the challenges posed by advanced technologies.

Conclusion

As demonstrated above, banks are a model for how other industries can explore AI-enabled use cases in a safe and sound manner. While emerging technologies, such as AI, are exciting and can open new possibilities for the human condition, it is essential that they are used in a way that fosters trust, accountability, and safety. Banks stand ready to work with policymakers and other industries to spread this culture that combines compliance and innovation with respect to the use of AI.

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