May 15, 2026

Via Electronic Mail

Financial Stability Oversight Council
U.S. Department of Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Dear FSOC Secretariat:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to provide supplemental comments following the April 27 Financial Stability Oversight Council (FSOC) Innovation Series Roundtable focused on cybersecurity and risk management considerations associated with artificial intelligence (AI).

ICBA appreciated the thoughtful discussion during the roundtable and welcomes Treasury's continued engagement with the financial services sector on the opportunities and challenges associated with AI adoption in community banking. As the only national trade association dedicated exclusively to serving the interests of community banks, ICBA represents the voice of thousands of community banks of varying asset sizes across the United States. Our member banks play a critical role in supporting small businesses, local communities, and rural economies.

ICBA has previously submitted several letters to the Administration regarding AI policy, cybersecurity, regulatory harmonization, and AI risk management considerations, including comments related to the Administration's AI Action Plan, Treasury's AI Request for Information (RFI), and the National Institute of Standards and Technology (NIST) Center for AI Standards and Innovation's request for information regarding security considerations for AI agents (*refer to enclosed letters*).

ICBA is writing to highlight how these institutions are already leveraging AI to strengthen operations and resilience, while also outlining key risks and practical implementation challenges that warrant further attention. In particular, this letter offers recommendations to ensure a risk-based, proportionate policy framework; strengthen coordination across critical infrastructure sectors; promote public-private collaboration to address emerging AI-enabled fraud risks; and maintain regulatory harmonization to avoid undue burden on smaller institutions. ICBA believes these steps are essential to supporting responsible AI adoption while preserving the ability of community banks to serve local communities, small businesses, and rural economies.

---

[1] *The Independent Community Bankers of America ® has one mission: the create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovation offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at icba.org.*

Community banks have long been adopters of technology to improve operational efficiency, strengthen cybersecurity, expand access to financial services, and support fraud mitigation efforts. Additionally, many community banks are already leveraging AI-enabled technologies across fraud detection, cybersecurity monitoring, operational automation, customer engagement, and underwriting functions.

As Treasury and FSOC continue evaluating AI adoption and resilience considerations, ICBA encourages additional focus on the interdependencies between the financial sector and other critical infrastructure sectors. Community banks are increasingly evaluating operational redundancies and continuity planning in response to evolving cyber and AI-enabled risks. This includes exploring backup power strategies such as generators and solar capabilities, as well as alternative telecommunications solutions including satellite internet connectivity to strengthen operational resilience during disruptions.

Financial sector resilience cannot be viewed in isolation from the broader critical infrastructure ecosystem. The operational availability of energy, telecommunications, cloud infrastructure, and data center capacity will increasingly shape the resilience posture of financial institutions, particularly smaller and rural community banks that may have fewer operational redundancies available to them.

ICBA also wants to highlight our longstanding partnership with the Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), the U.S Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), to help community banks strengthen cyber preparedness and operational resilience. Through this partnership, ICBA regularly works with Treasury and CISA to conduct cybersecurity tabletop exercises designed to battle test community bank incident response plans against evolving threats, including AI-enabled cyber and fraud scenarios. Most recently, ICBA and CISA hosted an AI-readiness tabletop exercise that garnered participation from more than 400 community bankers across over 30 states. These exercises help institutions identify operational gaps, strengthen coordination, and improve preparedness in an increasingly complex threat environment. ICBA believes these public-private partnerships are critical to ensuring community banks remain resilient, battle tested, and AI-ready.

At the same time, community bankers are increasingly expressing concerns regarding the rapid expansion of AI-related data center infrastructure across the country. While ICBA recognizes the importance of expanding compute capacity and maintaining American leadership in AI innovation, community banks are concerned that accelerated data center development could contribute to rising land values, increased utility costs, commercial real estate pressures, and increased competition for local infrastructure resources in some markets.

In some communities, these trends may unintentionally impact the ability of community banks to expand branch footprints, maintain affordable operational infrastructure, or manage rising utility expenses. ICBA respectfully encourages Treasury and FSOC to remain mindful of the Administration's commitment to enforcing the *Ratepayer Protection Pledge* as AI infrastructure expands. Policies supporting AI growth should ensure that increased electricity demand, utility modernization costs, and regional infrastructure pressures do not disproportionately impact local communities, small businesses, or community financial institutions.

ICBA also encourages continued dialogue regarding practical implementation challenges facing smaller financial institutions as AI adoption accelerates. Community banks remain interested in responsibly leveraging AI to improve fraud detection, cybersecurity operations, operational efficiency, and customer

service, but require practical, scalable, and risk-based guidance that reflects the realities of smaller institutions.

Community bankers are also increasingly concerned about the misuse of generative AI tools to facilitate fraud. Through independent testing and industry observations, it remains possible in many cases to prompt certain AI platforms to generate realistic synthetic checks and related fraudulent financial documents that could be used to facilitate check fraud and financial crimes.

ICBA strongly encourages Treasury, FSOC, and other relevant federal agencies to engage directly with leading generative AI developers to encourage voluntary restrictions and safeguards prohibiting the generation of synthetic checks and similar financial instruments. We believe this represents an opportunity for meaningful public-private collaboration that could help reduce fraud risks before they scale further across the financial sector. ICBA would welcome the opportunity to work collaboratively with Treasury, FSOC, financial regulators, and AI developers on practical mitigation approaches related to synthetic financial document generation and broader AI-enabled fraud risks.

ICBA also continues to emphasize the importance of regulatory harmonization and avoiding duplicative AI requirements that may disproportionately burden smaller institutions. Existing frameworks related to privacy, cybersecurity, third-party risk management, anti-money laundering, and consumer protection already provide important guardrails for the responsible use of AI in banking. As noted in prior ICBA submissions, future AI-related policies should prioritize harmonization, operational flexibility, and scalable implementation approaches for community banks.

Through initiatives such as the ICBA ThinkTECH Accelerator, ICBA continues working to connect community banks with innovative fintech and AI-driven solutions designed to support responsible modernization across the banking sector. As part of the ThinkTECH Accelerator program, ICBA also hosts a Regulator Day, which brings together regulators, policymakers, fintech leaders, and community bankers to discuss emerging technologies, operational risks, and innovation trends impacting the financial sector.

ICBA would like to extend an open invitation to representatives from the Department of the Treasury and FSOC to participate in the next ThinkTECH Accelerator Regulator Day in Atlanta, Georgia. The event provides an opportunity to engage directly with community bankers and discuss emerging issues impacting the sector, including AI governance, cybersecurity, fraud, operational resilience, and innovation.

Thank you again for the opportunity to provide supplemental input and for Treasury's continued engagement with the community banking sector on these important issues.

Respectfully,

/s/

Anjelica Dortch
Vice President, Operational Risk & Cybersecurity Policy
Independent Community Bankers of America (ICBA)

Enclosures:

ICBA Comments on Treasury RFI on Uses, Opportunities, and Risks of AI in Financial Services (August 12, 2024)
ICBA Comments on the Development of an Artificial Intelligence Action Plan (March 12, 2025)
ICBA Comments on Regulatory Reform on Artificial Intelligence (October 27, 2025)
ICBA Comments on Security Considerations for Artificial Intelligence Agents (March 9, 2026)