AI and the Industry

Anjelica Dortch

Vice President, Operational Risk & Cybersecurity Policy

Destin, Florida| June 11, 2025

ICBA

Agenda

- **Overview of ICBA**
- **Background on Artificial Intelligence**
- **Use cases in Community Banking**
- **AI: Opportunities and Threats**
- **Cybersecurity Threat Landscape in the Age of AI**
- **Responsible Use & Risk Mitigation**
- **AI Policy Landscape – State & Federal**
- **AI & Cyber Policy Expectation: The Trump Administration**
- **Recommendations for Community Banks**

ICBA Advocacy

About Me

Professional Background

Joined ICBA in December 2024

- SAP & IBM
- 10 years of federal service, White House, Department of Energy, Food and Drug Administration, and the Department of Justice
- Co-authored the following policies under President Trump's first term:
  - U.S. Federal Cloud Computing Strategy (Cloud Smart)
  - Report on Artificial Intelligence
  - EO on Strengthening America's Cybersecurity Workforce

Mission

The Independent Community Bankers of America® has one mission: to 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.

What is Artificial Intelligence?

AI refers to computer systems that can perform tasks that typically require human intelligence, such as learning reasoning, problem-solving, and decision making. It involves creating machines that can think or act like humans.

Legal Definition (FY 2021 National Defense Authorization Act, Sec. 5002):

"A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."

AI in Everyday Life

Generative AI (GenAI)

- ChatGPT (OpenAI), Copilot (Microsoft), Claude AI (Anthropic)

Autonomous Systems

- Waymo, Tesla, and Cruise

Recommender Systems

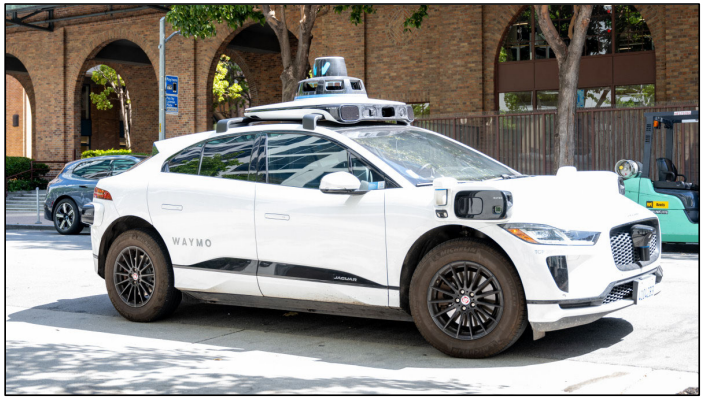
- Netflix, YouTube, and Spotify

Predictive AI

- Google Maps
- Credit scoring

Conversational AI

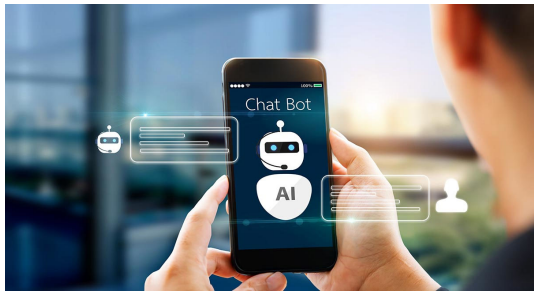
- Siri and Alexa

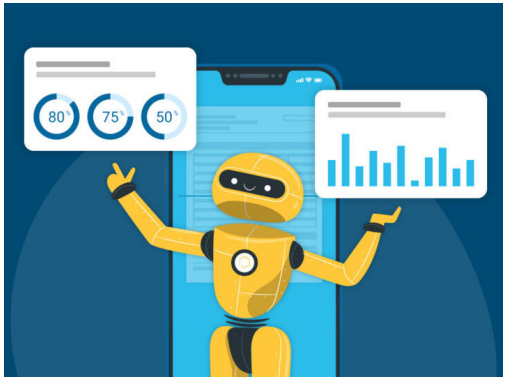


Computer Vision

- Smartphones & Security Systems

AI in Community Banking – Use Cases





Artificial Intelligence: Opportunities & Threats

Opportunities

- AI-driven fraud detection models that monitor real-time transactions.
- Streamlining KYC (Know Your Customer) & KYA (Know Your Adversary) programs using AI automation.

Threats

- Rise of AI-powered cyberattacks: attackers use AI for spear-phishing and voice cloning to gain access to bank credentials.
- AI model vulnerabilities: adversarial attacks that compromise the integrity of AI systems.
- Additional threats: AI-powered chatbots, credential stuffing, AI-enhanced reconnaissance, and malicious GPTs

Future Considerations

- Banking data is an extremely sought after asset in the age of AI.
- Evaluate your tech stack and leverage cybersecurity solutions that infuse AI capabilities with threat detection.

Cybersecurity Threat Landscape in the Age of AI

- **Threat Environment:**

  Cyberattacks on financial institutions rose by **38%** in 2024

  Financial services accounted for **23%** of all cyber incidents, making it the most targeted industry.

  Adversary Speed: The fastest observed breakout time has dropped to **51 seconds**, a sharp contrast from over 9 hours in 2018, underscoring the urgency of proactive defense.

  442% increase in voice phishing (vishing).

- **Cost of Cybercrime:**

  Global cybercrime costs are predicted to hit **$10.5 trillion** annually by 2025

- **Regulatory Pressure:**

  Enhanced scrutiny under FDIC's Cybersecurity Incident Notification Rule

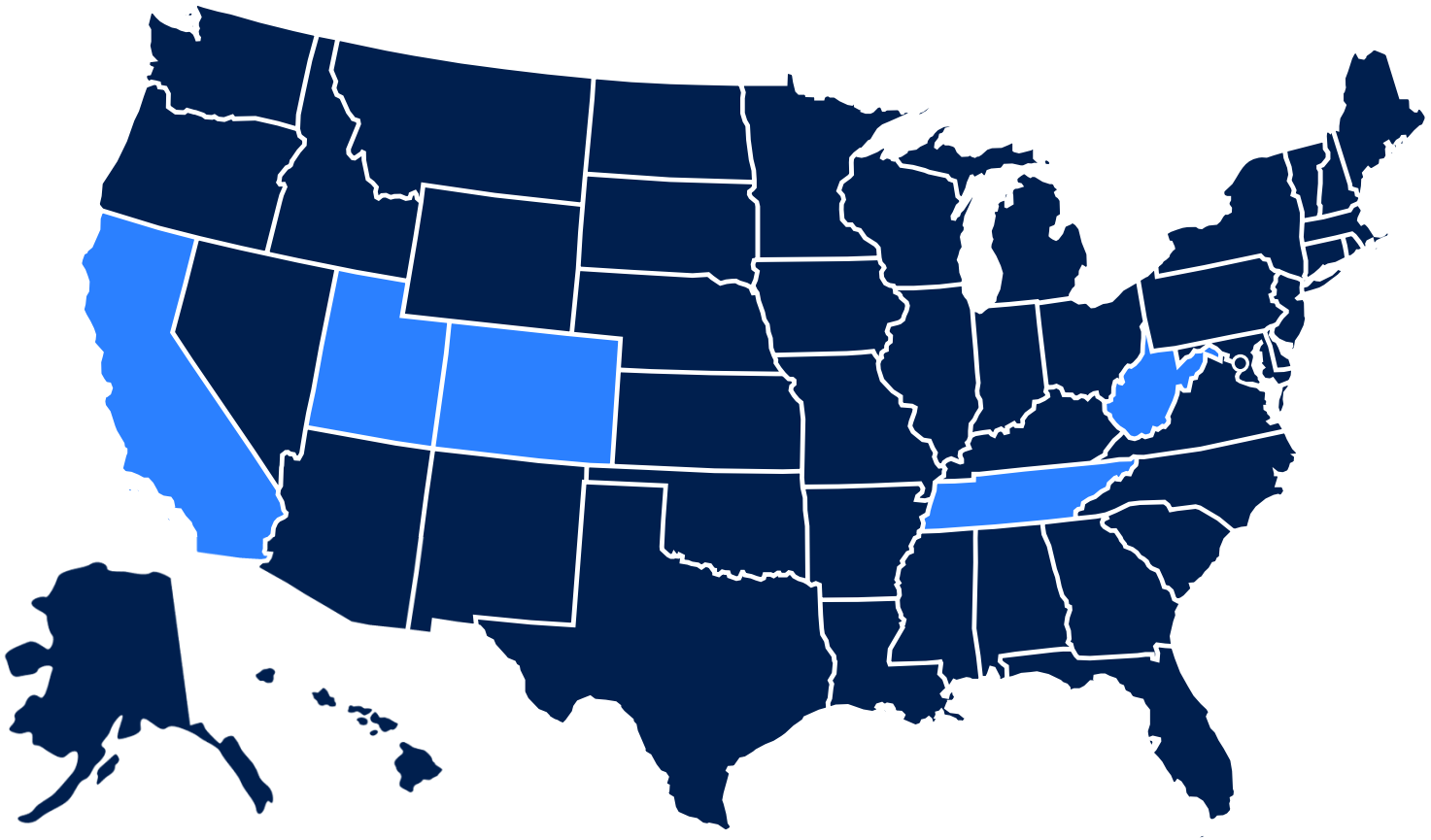
ICBA

Responsible Use & Risk Mitigation

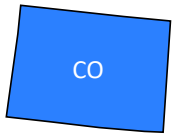
- Transparency: Ensure AI decisions are **explainable** to stakeholders.
- Fairness: Regularly audit AI systems for **bias** and discriminatory outcomes.
- Accountability: Establish clear **governance** structures for AI oversight.
- Security: Implement robust **cybersecurity** measure to protect AI systems.
- Compliance: Align AI practices with existing **laws and regulations**.

AI Policy Landscape – State Level

As of early 2025, over 700 AI-related bill have been introduced across 45 states



SB 24-205 – Colorado Artificial Intelligence Act



First comprehensive AI regulation in the U.S. that mandates risk assessment and documentation for developers & deployers of high-risk AI systems.

AB 2013 - AI Transparency Act

Requires developers of GenAI to disclose training data used.

Ensuring Likeness, Voice, and Image Security (ELVIS) Act

Protects individuals from unauthorized AI-generated replicas of their voice, image, or likeness.

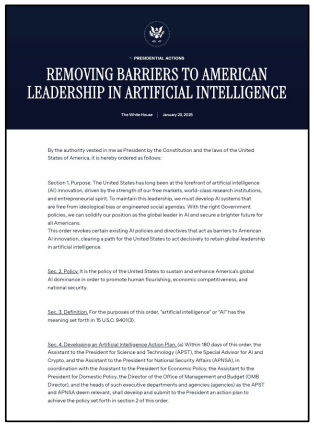
SB 149 – Artificial Intelligence Policy Act

Introduces a regulatory sandbox allowing organizations to test AI technologies under regulatory supervision.

ICBA Advocacy

AI Policy Landscape – Federal Level

Executive Order



PRESIDENTIAL ACTIONS

REMOVING BARRIERS TO AMERICAN LEADERSHIP IN ARTIFICIAL INTELLIGENCE

The White House | January 23, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The United States has long been at the forefront of artificial intelligence (AI) innovation, driven by the strength of our free markets, world-class research institutions, and entrepreneurial spirit. To maintain this leadership, we must develop AI systems that are free from ideological bias or engineered social agendas. With the right Government policies, we can solidify our position as the global leader in AI and secure a brighter future for all Americans.
This order revokes certain existing AI policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in artificial intelligence.

Sec. 2. Policy. It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security.

Sec. 3. Definitions. For the purposes of this order, "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3).

Sec. 4. Developing an Artificial Intelligence Action Plan. (a) Within 180 days of this order, the Assistant to the President for Science and Technology (APST), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (APNSA), in coordination with the Assistant to the President for Economic Policy, the Assistant to the President for Domestic Policy, the Director of the Office of Management and Budget (OMB Director), and the heads of such executive departments and agencies (agencies) as the APST and APNSA deem relevant, shall develop and submit to the President an action plan to achieve the policy set forth in section 2 of this order.

President Trump signed the Executive Order on May 1, 2025, directing agencies to prioritize American leadership in AI development, safety, and innovation through coordinated policies. An AI Action Plan is required within 180 days, due by mid-July.

NIST & Treasury

NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector

U.S. Department of the Treasury

March 2024

The NIST AI RMF offers a voluntary framework for managing AI risks across sectors, promoting trustworthy AI. Treasury's document specifically addresses AI-driven cybersecurity risks within the financial services sector, highlighting unique challenges and recommending tailored risk management practices for financial institutions.

Community Bank Responsible AI Strategy

AI Policy Principals

ICBA

Under Development

AI & Cyber Policy Expectations: The Trump Administration

Key Focus Areas for Trump 2.0

- Trump AI Action Plan (expected mid-July)
- New National Cyber Strategy EO (signed June 6)
- Review & Repeal
  - Biden AI Executive Order
  - Biden Cyber Executive Order
  - SEC Cyber Incident Disclosure Rule
  - National Security Memorandum-22
- Federal spending & workforce cuts
- Expect implementation delays with Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
- Changes to Public-Private Partnerships
- CAT Sunset on August 31, 2025

Recommendations for Community Banks

- **Start Small and Focus on Specific Use Cases:**
  Identify pain points to address existing challenges and/or create clear value
  Customer service and marketing tools are the most popular

- **Build Internal Capabilities and Foster a Culture of Innovation:**
  Invest in training employees and customers to enhance AI literacy & awareness

- **Engage and Evaluate Third-Pary Vendors:**
  Due diligence should include identification of ”AI capabilities” in your tech stack and alignment with NIST AI RMF

- **Stay Ahead of Regulatory Changes:**
  Partner with compliance and audit consultants for AI and cyber readiness

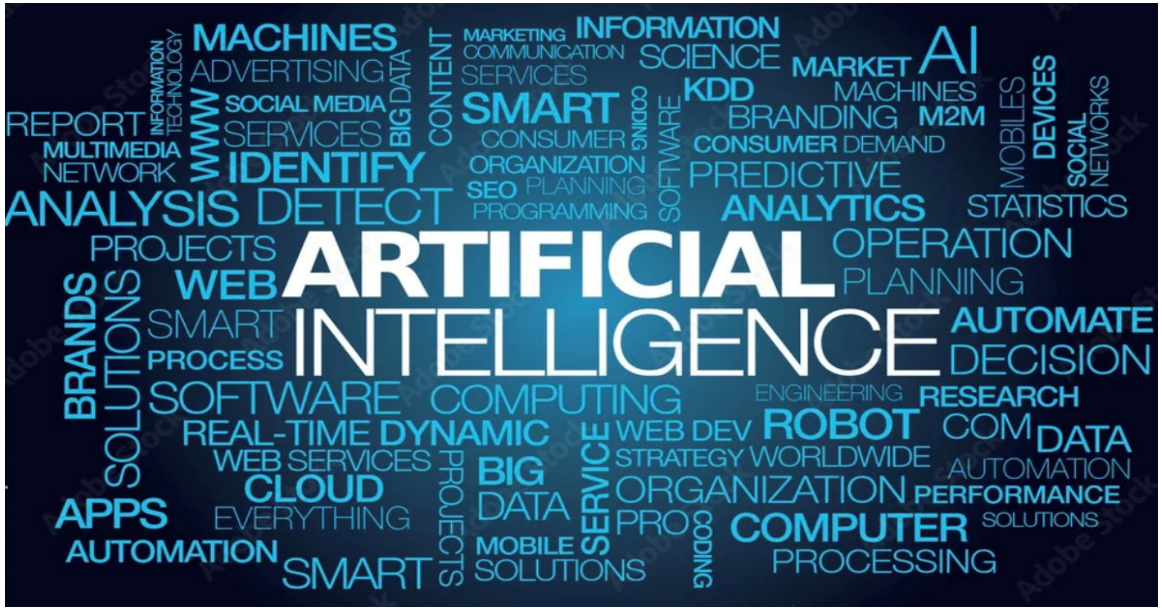
- **Align AI Strategy with Institution Goals:**
  Clear vision with an ROI focus

Closing Thoughts

Responsible AI adoption is a **strategic imperative** for community banks.

Proactive investment in AI, cybersecurity, and fraud prevention is vital.

Develop and **adopt an AI strategy** that is right sized to your institution.



Q&A

Anjelica Dortch
Vice President, Operational Risk & Cybersecurity Policy
Anjelica.Dortch@icba.org
Washington, D.C.