AI Transforming the Financial Landscape

x9.org/x9ai-study-group-newsletter

View the X9 AI Study Group

X9 AI Study Group Newsletter - Issue No. 11(2026)

NIST to Test Frontier AI Models pre-deployment

The U.S. government AI security center will test frontier models before release. NIST plans pre-deployment evaluations of models from Google, Microsoft, and xAI. The goal is to find cybersecurity risks tied to advanced capabilities.The testing runs through the Center for AI Standards and Innovation. Evaluators will check whether model features create new attack options. Results will inform federal guidance.

This sets a precedent for government review of private AI systems. If you build on these models, track the findings. Expect security baselines to tighten as evaluations expand.

Continue Reading

MISMO introduces Wrapper Files for loan data standardization

MISMO introduced Wrapper Files to standardize loan boarding on May 28. The format gives lenders a consistent way to transfer loan data between systems. It targets a long-running source of cost in the mortgage chain.

Inconsistent loan boarding raises error rates and manual work. A shared file structure reduces mapping effort. MISMO also published a paper on fee standardization to cut complexity in lending.

Adopt the Wrapper File format to lower integration costs. Align your loan transfer process with the standard before partners require it. Standardized data improves accuracy when you move loans between servicers.

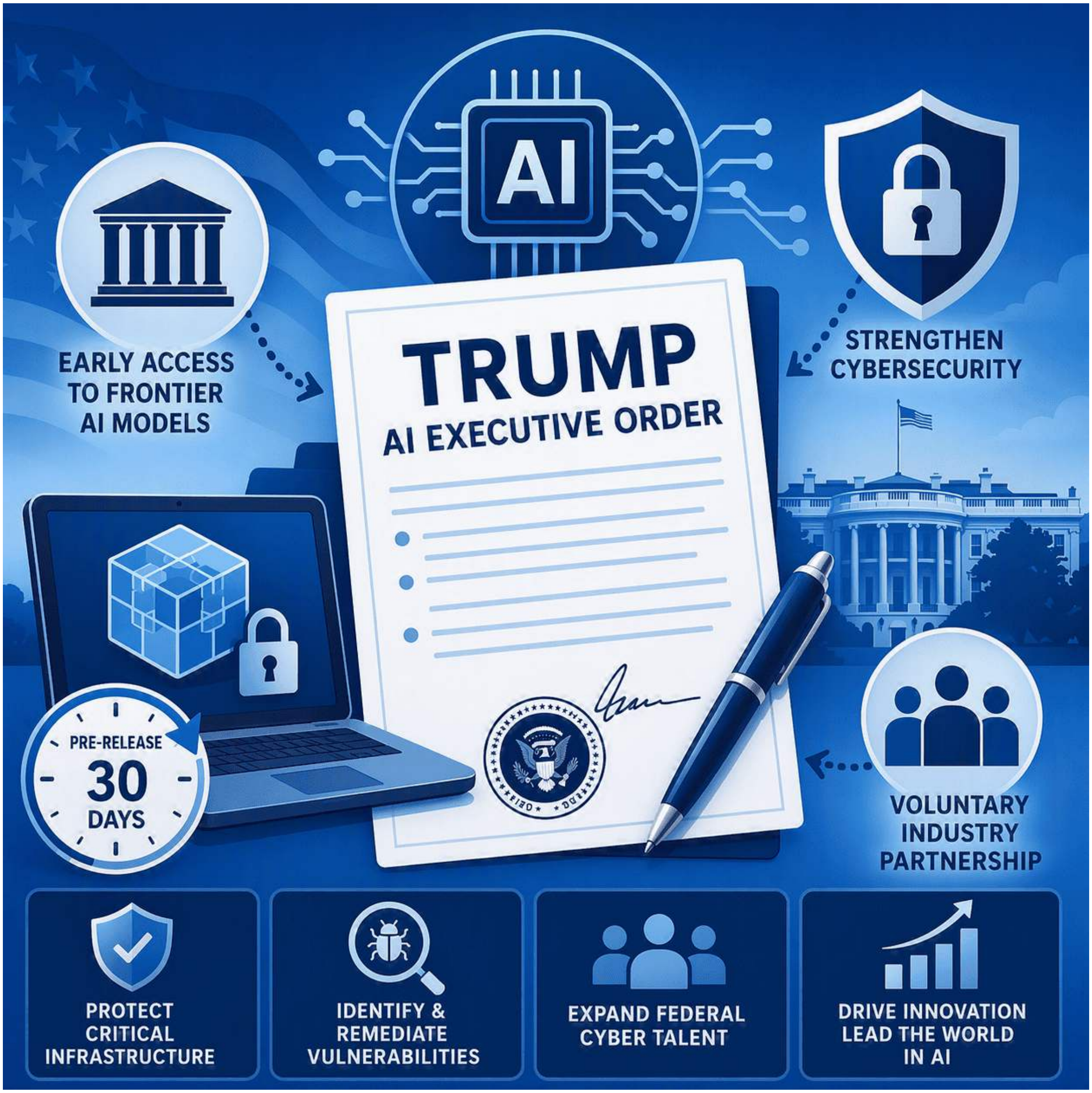
[Continue Reading](#)

Trump Signs Voluntary AI Executive Order Delaying Strict Rules

President Trump signed a scaled-back executive order on AI and cybersecurity on June 2. The order rejects mandatory licensing for new models, including frontier models. You get a voluntary framework instead of binding federal rules.The details show a compromise. Former

White House AI czar David Sacks secured a 30-day window for pre-deployment testing and kept the framework voluntary. Some officials pushed to make testing mandatory and lost.The backdrop is a fight inside the government. Commerce, intelligence agencies, and industry allies clashed after Anthropic's Mythos model showed offensive cyber capabilities. No binding framework exists weeks later, so federal AI policy stays unsettled going into summer.

[Continue Reading](#)



MISMO updates reference model for servicing and VA workflows

MISMO released Version 3.6.3 of its Reference Model on June 3. The update targets servicing, property data, and VA workflows. If you work in mortgage technology, this version changes the data standards you build against.The release adds concrete support. It covers the MISMO Federal Government Housing Agency Servicing Dataset, aligns property data with recent GSE updates, and adds structured data for VA workflows. The package ships XML Schema, JSON Schema, YAML files, and a logical data dictionary.The goal is cleaner data. MISMO President Brian Vieaux said the update reduces friction, improves data quality, and supports faster decisions across the mortgage system. Stronger alignment cuts the cost of variable interpretations between lenders, servicers, and investors.

Continue Reading

Regulators Prioritize AI, Stablecoins, and Digital Payments

AI ranks as the top fraud threat facing financial institutions in 2026. Fraudsters use generative tools to produce convincing content and automate attacks at scale. You face faster, cheaper, and more credible scams than a year ago.The data shows the scale. Consumers lost more than $12.5 billion to fraud in 2024. Voice cloning and vishing attacks now exceed 1,000 AI scam calls per day at major retailers. Deepfakes account for a rising share of global fraud activity.The methods keep shifting. Emotionally intelligent bots run romance and relative-in-need scams with no human operator. Cloned websites harvest credentials and feed identity theft. Your defenses need AI-based detection to match the speed of these attacks.

Continue Reading

AI-Driven Fraud Losses Surge Globally

AI ranks as the top fraud threat facing financial institutions in 2026. Fraudsters use generative tools to produce convincing content and automate attacks at scale. You face faster, cheaper, and more credible scams than a year ago.

The data shows the scale. Consumers lost more than $12.5 billion to fraud in 2024. Voice cloning and vishing attacks now exceed 1,000 AI scam calls per day at major retailers. Deepfakes account for a rising share of global fraud activity.

The methods keep shifting. Emotionally intelligent bots run romance and relative-in-need scams with no human operator. Cloned websites harvest credentials and feed identity theft. Your defenses need AI-based detection to match the speed of these attacks.

Continue Reading

Stay Ahead in Financial AI

Subscribe to our newsletter for the latest insights and updates on AI in financial services.

Subscribe Now