AI Transforming the Financial Landscape

x9.org/x9ai-study-group-newsletter

Insights into AI's Role in Financial Services

This page provides a biweekly roundup of AI related news concerning US financial services including banking, capital markets, fintech, and corporate finance. Discover how artificial intelligence is reshaping banking, and capital markets driving innovation and efficiency across the financial sector.

View the X9 AI Study Group

X9 AI Study Group Newsletter - Issue No. 15 (2026)

NIST Releases AI Documentation Zero Draft for Public Comment

On July 30, NIST published an initial public draft titled Guidance and Templates for Public-Facing AI Documentation: An AI Standards Zero Draft. Authors Razvan Amironesei and Jesse Dunietz developed the draft under NIST's AI Standards Zero Drafts Pilot Project. The comment period closes September 16, 2026. NIST's approach gathers stakeholder input before work moves into formal standards bodies, helping accelerate standard development.

The Zero Draft provides templates for how AI system developers and deployers should document and communicate AI capabilities, limitations, and risks to the public. It addresses model cards, system cards, and other public-facing disclosure formats. NIST backed the project with $55 million in AI standards research funding. The AI Agent Standards Initiative, also under NIST, was updated August 14 and runs parallel to this documentation work.

Compliance and risk teams should track this document closely. Regulators across financial services are building AI transparency expectations from frameworks like this one. Documentation requirements for model cards and system cards could influence future examination expectations. Filing a comment by September 16 gives organizations a direct voice in how those expectations develop, with relatively low effort and potentially significant influence.

Continue Reading

OCC, Fed, and FDIC Replace SR 11-7 With Scaled, Principles-Based Model Risk Guidance

On April 17, the OCC, Federal Reserve, and FDIC jointly issued OCC Bulletin 2026-13, replacing SR 11-7, the Federal Reserve's 2011 supervisory guidance on model risk management, which has served as the banking industry's primary model governance framework for 15 years. The new guidance takes a risk-based, principles-driven approach and applies only to banking organizations with more than $30 billion in total assets. Community banks below that threshold are no longer subject to this specific guidance.

The revised framework explicitly excludes generative and agentic AI, classifying those technologies as "novel and rapidly evolving." Traditional statistical models and non-generative AI tools remain in scope. Fair lending expectations include disparity analysis across protected class segments, testing for proxy variables in model inputs, and ongoing monitoring for disparate impact throughout the model lifecycle.

The shift to a principles-based approach gives larger banks more flexibility in structuring model governance, but also increases responsibility for internal risk management teams. The exclusion of generative AI does not mean those systems are unregulated. Banking regulators have made clear that AI-specific guidance is forthcoming, and institutions should prepare accordingly.

Continue Reading

Federal Reserve Proposed AML/CFT Rule Opens Door for AI-Based Transaction Monitoring

On July 7, the Federal Reserve Board published a Notice of Proposed Rulemaking to modernize anti-money laundering and countering the financing of terrorism (AML/CFT) program requirements for Board-supervised banking organizations. The proposal, published in the Federal Register on July 9, runs parallel to similar rules proposed by FinCEN in April 2026. Comments are due September 8, 2026. Together, the proposals represent the most significant update to AML/CFT program requirements in years.

The proposed rule requires risk-based, written AML/CFT programs with board-level approval and enterprise-wide risk assessments tied to FinCEN's national priorities. A key provision updates supervisory expectations for technology-enabled monitoring and explicitly supports the adoption of AI and advanced analytics tools. The proposal seeks to remove perceived enforcement risks associated with deploying those tools, which regulators acknowledge have slowed AI adoption in compliance functions.

For institutions still relying primarily on rules-based transaction monitoring, the proposal signals a regulatory willingness to support AI-enhanced capabilities. The Fed intends the rule to reduce disincentives to AI deployment in AML/CFT programs, indicating that regulators expect monitoring programs to evolve. Organizations have until September 8 to submit comments and influence requirements before they are finalized.

Continue Reading

SEC Examiners Request Written Evidence of AI Governance, Marketing Claims, and Vendor Oversight

The SEC's Division of Examinations has begun sending information requests to financial firms focused on AI use, according to an August 7 analysis from FinTech Global citing Red Oak Compliance Solutions. Examinations target three areas: AI-driven portfolio management, algorithmic trading models, and marketing claims. The SEC is testing whether firms can substantiate public statements about their AI capabilities and avoid "AI washing", the practice of overstating, misrepresenting, or exaggerating the role and sophistication of AI in products, services, or business operations.

Examiners are requesting written, audio, and video materials that reference AI, including ADV Part 2 filings, websites, pitch materials, and video content. Many firms report having AI governance committees, yet some discovered AI tools were being used by IT teams without compliance oversight. Third-party vendors add complexity, requiring firms to document and monitor AI embedded in external products and services.

Red Oak recommends three immediate actions. Review public AI claims for accuracy and consistency across all channels. Build a complete inventory of AI tools, including those obtained through third-party providers. Assign clear governance ownership and document it through committee structures, training records, and meeting minutes. Examiners are specifically requesting those records. While no dedicated ADV field for AI disclosures exists

today, examinations are already driving detailed documentation expectations through direct information requests.

Continue Reading

Fannie Mae AI Governance Rules for Mortgage Lenders Took Effect August 6

Fannie Mae's Lender Letter LL-2026-04 became effective August 6. The framework requires seller/servicers using AI or machine learning in loan origination or servicing to maintain written governance policies covering the full AI lifecycle: development, deployment, operation, maintenance, and risk management. Fannie Mae issued the letter April 8 and provided lenders 120 days to comply.

The guidance applies to both internally developed and vendor-provided systems. Lenders must review AI governance policies annually and remain fully responsible for AI used by subcontractors. Vendor errors do not shift liability away from the lender. The guidance also applies broadly across origination and servicing functions, not just underwriting.

For organizations that sell or service loans for Fannie Mae, the framework is now a contractual obligation. Policies must address ethics, bias risk, regulatory compliance, and personnel oversight. Failure to comply may jeopardize seller/servicer status. If your compliance team has not reviewed AI systems against LL-2026-04 requirements, the August 6 effective date means those expectations are already in force.

[Continue Reading]

Synchrony Partners with OpenAI to Advance Agentic Commerce

Providing one of the clearest examples yet of how agentic commerce could move from concept to real-world deployment, Synchrony announced an enterprise collaboration with OpenAI to help bring financing, rewards, and loyalty programs into AI-native shopping and checkout experiences.

A key element is a Synchrony ChatGPT plugin that will allow consumers to discover offers, promotional financing, and rewards within conversational shopping experiences.

Synchrony also plans to deploy OpenAI models across its enterprise and expand AI training and tools for employees. The company views the collaboration as part of a broader strategy to support agentic commerce, where AI systems increasingly help consumers discover products, evaluate options, and complete transactions.

Synchrony emphasized maintaining consumer choice, merchant flexibility, and secure experiences as commerce becomes more AI-driven.

One of the largest U.S. consumer financial services companies, Synchrony operates at the intersection of shopping, payments, financing, and rewards. Its co-branded credit cards, installment lending, financing, and loyalty programs make it a significant indicator of how agentic commerce may evolve.

Continue Reading

NIST RFI: Modernizing the National Vulnerability Database in the Age of AI

On August 12, NIST issued a Request for Information (RFI) seeking input on modernizing the National Vulnerability Database (NVD), the U.S. government's primary repository for vulnerability management data. Comments are due October 13, 2026.

NIST says the vulnerability management ecosystem is being reshaped by artificial intelligence, increasing numbers of disclosed vulnerabilities, machine-readable security data, and the need for faster, more automated analysis. The agency is seeking recommendations on AI-enabled automation, vulnerability prioritization, data quality, interoperability, automated remediation, governance, and modernization of vulnerability standards.

The RFI also asks how the NVD should evolve over the next five years to better support analysts, developers, researchers, policymakers, and security tools while maintaining transparency, accuracy, trust, and accessibility. Responses will help guide future NVD strategy, architecture, standards development, and community collaboration efforts.

The RFI builds on NIST's April 2026 update of NVD operations, which introduced risk-based prioritization and other measures to address record CVE growth. The latest request seeks input on how AI, automation, and machine-readable security data should shape the next generation of vulnerability management.

Continue Reading