# AI Study Group Newsletter | Accredited Standards Committee X9

x9.org/x9ai-study-group-newsletter

**Insights into AI's Role in Financial Services**

## AI Transforming the Financial Landscape

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. 7 (2026)

### AI Chip Export Licenses Stack Up at the Commerce Department

The Bureau of Industry and Security faces a major backlog of AI chip export license applications. Thousands of requests sit unprocessed, slowing projects across allied countries. The gap between policy goals and licensing capacity creates direct risk for U.S. technology firms. BIS now handles added duties, including tariff investigations and reviews of Nvidia export requests to the Middle East and China. Staffing losses worsened the strain, even with a 23 percent budget increase approved for Fiscal Year 2026.

If your organization depends on export approvals for advanced semiconductors, expect delays. Set longer timelines and inform customers and internal teams early. Industry groups confirm the backlog and do not expect quick relief. Non U.S. suppliers are already stepping in to fill demand while U.S. exports stall.

Continue Reading

## AI cyber threats: open letter to business leaders

The UK government warns business leaders that AI is rapidly accelerating cyber threats by lowering the expertise needed to find software vulnerabilities and generate exploits at scale. Testing by the AI Security Institute found that frontier model cyber capabilities are now doubling every four months, significantly faster than previously observed. Recent advances by multiple AI firms indicate this trend is system-wide, not isolated. While government capacity through the AI Security Institute and the National Cyber Security Centre is expanding, officials stress that resilience depends on businesses strengthening basic cyber hygiene, board-level oversight, and preparedness, as government action alone will not be sufficient.

Continue Reading

## Fifth Third Says AI Lets Banks Build Compliance Capabilities Faster Than Vendors

Fifth Third Bank reports a shift in how banks manage compliance technology. AI enables internal teams to build analytical tools faster than vendor update cycles. Continuous monitoring replaces annual exam preparation, turning compliance into an ongoing process. AI systems analyze large data sets to identify loan risk, flag underwriting issues, and reduce repurchase exposure.

The bank has moved development in house rather than waiting on vendor releases. This gives earlier visibility into compliance risks and faster response times. Review where your institution depends on vendor tools. Internal AI development gives more control and aligns with examiner expectations, which now focuses on continuous oversight rather than periodic review.

Continue Reading

## Microsoft Releases Tools to Address AI Compliance and Security Gaps at Banks

Financial institutions face growing risk as AI systems handle sensitive data. Issues include data leakage, manipulated inputs, and unreliable outputs. These risks intersect with obligations under laws such as the Gramm Leach Bliley Act and Sarbanes Oxley.  Regulators now examine AI governance as part of standard oversight.

Microsoft released tools designed to address these risks within existing enterprise environments. The tools target data exposure, prompt injection, and output validation. They align with regulatory requirements and support existing oversight programs. If your organization uses Microsoft infrastructure, run a gap assessment against examiner expectations before your next review. Documentation and control evidence will face direct scrutiny.

Continue Reading

## NACHA Phase 1 Fraud Monitoring Rules Are Now in Effect for Large ACH

## Originators

Phase 1 of NACHA fraud monitoring rules took effect on March 20, 2026. Large ACH originators and certain financial institutions must now implement risk-based processes to detect unauthorized transactions and payments made under false pretenses. The rule applies to organizations with more than 6 million originated entries or 10 million received entries in 2023. Phase 2 expands coverage to all other originators on June 22, 2026.

The rules add false pretenses as a formal fraud category, including business email compromise and vendor impersonation. Standardized transaction labels such as PAYROLL and PURCHASE now support targeted monitoring. If your organization meets the Phase 1 threshold, confirm your monitoring program meets NACHA guidance. If not, use the remaining time before Phase 2 to build a defensible framework with documented risk-based controls.

Continue Reading

## Stay Ahead in Financial AI

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

Subscribe Now

## Archive of Newsletters

AI and Financial Services Insights