



August 21, 2026

Center for AI Standards and Innovation (CAISI)
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899

Re: Barriers to AI Adoption in Finance

1. Introduction

The National Fair Housing Alliance (NFHA) leads a coalition that works to build inclusive, well-resourced, and resilient communities; expand equitable opportunities; and end housing discrimination. It has extensive consulting and compliance experience with regulated financial entities such as major banks and insurance companies. The organization works on solutions to mitigate the negative effects of AI-driven financial products on consumers while promoting and advancing the beneficial use of the technology within the financial industry. NFHA's position is that the primary barrier to effective AI adoption in financial services, and across high-stakes sectors is the *absence* of clear, consistent, civil-rights-grounded federal guidance for sound and safe use of the technology in financial services. This brief reflects expert views from our partners in industry, law, and civil rights.

2. AI Use Cases in Financial Services

1. AI can allow small businesses to expand into larger markets and serve their customers. For example, AI tools can allow more frequent compliance monitoring in place of periodic loan sampling, thereby improving risk management with the same resources. On the other hand, while high-stakes decision systems including credit scoring, mortgage underwriting, and insurance pricing carry the greatest civil rights exposure, a range of algorithmic fairness techniques exist to mitigate this exposure, including distribution matching, adversarial debiasing, exponential gradient reduction, prejudice remover, rich subgroup fairness.
2. Additionally, GenAI-powered automation can greatly increase efficiency and compliance in financial services through virtual chatbots, workflow automation, and agentic trading assistants.

2. Barriers and Enablers

1. **Talent and cost barriers create an access gap for small-to-mid-sized institutions (up to \$50B in assets), threatening their long-term viability.** These institutions often rely on ad hoc tools in place of vetted, scalable AI systems, and are wary of adopting AI absent established fairness standards and regulatory guidance. Smaller/regional institutions also have less AI sophistication, meaning they are **disproportionally exposed to regulatory risks compared to** larger competitors.
2. **Market concentration compounds the access problem.** AI capability is concentrated among a small number of large banks relying on a handful number of frontier model developers. This creates a widening competitive gap and risks accelerating consolidation from community-based and mission-driven lenders.
3. **Regulatory fragmentation and uncertainty chill responsible adoption.** Institutions face fragmented federal lending rules and are conflicted about testing obligations. Lenders understand their continuing obligation to red-team AI models under state and local law, but conflicting federal guidance makes it difficult to assess the cost-effectiveness of an AI solution against potential legal and reputational risk. Third-party due diligence requirements (IT security, vendor vetting) also remain non-standardized across regulators, adding to this uncertainty.
4. **Internal governance gaps create reputational exposure.** Many institutions lack clear internal lines of AI authority (e.g., no designated AI officer), reflecting a basic corporate governance shortfall. This creates an unresolved question of who owns AI governance processes and liability. Customer-facing AI carries a liability exposure that no institution is yet to solve.
5. **Existing frameworks leave key risk categories uncovered.** Evaluation guidance to date focuses on capability and neglects consumer risks, leaving institutions vulnerable to reputational and legal exposure when those risks go unmitigated. Current cybersecurity frameworks do not adequately address financial-sector-specific threats and testing guidance for possible attack vectors needs to be sector-specific and keep pace with model releases.

3. Strategies and Interventions

1. **Establish clear, durable standards and benchmarks.** NIST could set fairness tolerance ranges for AI in finance, giving institutions regulatory certainty across administrations, and develop metrics/guardrails that let smaller institutions adopt safely without disproportionate compliance burden. NIST should encourage domain-specific benchmarks and evaluation approaches crowdsourced from lenders' actual use cases. A recurring public report on AI trends in finance, akin to the CFPB's discontinued supervisory highlights, would build smaller-player confidence in adoption.
2. **Restore and standardize regulatory guidance.** Regulators, including the Federal Financial Institutions Examination Council (FFIEC) and the Consumer Financial Protection Bureau (CFPB), should issue guidance requiring lenders to conduct and document consumer safety testing with clear procedures for contestability for example in automated valuation models (AVMs) and automated underwriting systems (AUS) powered by AI. In addition, a plain-language AI systems taxonomy (e.g., dynamic vs. static models) would help resource-constrained institutions procure safe and sound third-party tools. Financial regulators should jointly standardize a single third-party AI vendor questionnaire to replace the current fractured and duplicative vetting process, paired with a clear vendor disclosure obligation to force parity in transparency across vendor size and feed a shared cross-agency reporting standard.
3. **Make consumer safety an explicit, structural component of AI evaluation.** Consumer safety and institutional soundness must be built into the rules governing AI adoption in finance. This involves centering lived experience in oversight to ensure meaningful participation by affected communities. Technical and regulatory reforms must be grounded in the experiences of those most likely to be harmed, particularly low-income households, families with children, people with disabilities and single mothers.
4. **Extend testing transparency beyond frontier labs.** NIST's frontier model testing work is valuable, but its secretive nature leaves AI companies outside that testing regime in the dark. NIST should publish frontier testing guidance made concrete for financial services use cases and should issue safety and soundness testing and evaluation guidance for institutions that develop or rely on open-source AI.

