Emerging Regulatory Risks in Financial Services: Spring 2026 Update

Monica Bolin

Halfway through 2026, a picture is forming. Federal priorities are shifting, state regulators are moving to fill the space, and the risk environment is more distributed than it was a year ago — across jurisdictions, vendor stacks, and every function where AI is embedded without a formal governance framework.

For compliance and risk professionals at financial organizations, here are the emerging risks to monitor right now.

Fair Lending in Flux

The CFPB's April finalization of changes to Regulation B removed disparate impact liability from the Equal Credit Opportunity Act (ECOA), narrowed the discouragement standard, and restricted the use of race, sex, and national origin as eligibility criteria in Special Purpose Credit Programs.

But that doesn't mean the underlying obligation has changed. The Fair Housing Act still carries disparate impact liability. State fair lending laws in Massachusetts, California, New York, and New Jersey remain fully in force, and state enforcement is moving independently of federal posture. Massachusetts reached a $2.5 million settlement tied to AI-driven disparate impact outcomes this year, and litigation challenging the Regulation B rule is widely anticipated.

With the July 21 compliance deadline fast approaching, financial organizations should update their fair lending programs to distinguish ECOA intentional-discrimination analysis from FHA disparate impact analysis, audit existing Special Purpose Credit Programs against the new eligibility restrictions, and keep statistical monitoring intact.

Consumer Complaints Are a Supervisory Signal

Regulators are using complaint data to scope examinations, and the volumes are rising. According to the FDIC's 2026 Consumer Compliance Supervisory Highlights, the agency processed 32,128 written complaints and inquiries in 2025 — a 21% increase from 2024. Third-party providers were identified in nearly 6,400 of those cases, a 48% jump from the prior year. The Federal Reserve flagged unresponsive customer service and improper error resolution as the primary drivers of direct escalation.

Financial organizations that map internal logs against regulator data and extend monitoring to vendor-serviced functions have a clearer picture of where compliance gaps may be forming.

AI Risk Is Cutting Across Every Category

Three significant publications from early 2026 reframe what AI risk looks like for financial organizations. In February, the U.S. Department of the Treasury — working with over 100 financial institutions — released the Financial Services AI Risk Management Framework, built around 230 control objectives spanning governance, data, model development, validation, monitoring, third-party risk, and consumer protection. Two months later, the Federal Reserve, FDIC, and OCC jointly released revised interagency model risk management guidance, replacing SR 11-7 and explicitly bringing vendor and third-party models into scope. Frameworks like these have historically become the scaffolding for regulatory examinations.

The threat side of AI is moving just as fast. In April, the FS-ISAC issued a sector risk advisory warning that AI frontier models can rapidly detect and chain vulnerabilities and generate working exploits. Vulnerability backlogs managed through compensating controls now function as a roadmap for targeted attacks. The advisory recommends compressing remediation timelines, hardening perimeters, and deploying AI defensively to triage and respond to security alerts.

Vendor AI Is Your Risk Too

Many vendors have added AI capabilities to their platforms without proactive disclosure. The AI running inside your organization's loan origination systems, fraud detection tools, transaction monitoring, and BSA/AML platforms may never have been part of a formal vendor review. Regulators are clear on this: financial organizations are responsible for their vendors' AI use.

That accountability is concrete. When a vendor's fraud detection model incorrectly blocks account access, Regulation E consequences land with the financial organization. When an AI-driven transaction monitoring system misses suspicious activity, so does the regulatory exposure. Building an AI inventory that captures which vendors use it, how it's deployed, and what decisions it influences — and ensuring due diligence questionnaires and contracts reflect that — is where oversight starts.

Nacha ACH Fraud Monitoring: Phase 2 Is Here

If your organization originates or receives Automated Clearing House (ACH) transactions, Phase 2 of Nacha's new fraud monitoring rules went into effect on June 22 — and the shift it requires goes beyond adding a compliance checkbox.

Prior ACH fraud controls focused primarily on unauthorized debits. The new rules require risk-based processes designed to identify entries initiated through fraud, including cases where payments are technically authorized but induced through deception, such as business email compromise and payroll redirection. Phase 2 covers all remaining ODFIs, non-consumer originators, third-party senders, and RDFIs regardless of volume.

Noncompliance carries fines up to $500,000 per month and potential suspension from originating ACH entries. If compliant monitoring isn't yet in place, a gap analysis and verification of Company Entry Description labeling requirements are the starting point.

The Pattern is Worth Watching

Each of these developments has its own deadline and its own regulatory home, but taken together, they point in the same direction. Federal priorities are shifting, state regulators and private litigants are filling the space, and AI is expanding exposure across vendor stacks, cybersecurity, and compliance functions simultaneously.

The second half of 2026 won't slow down. Staying current on where the risk is moving is the work.