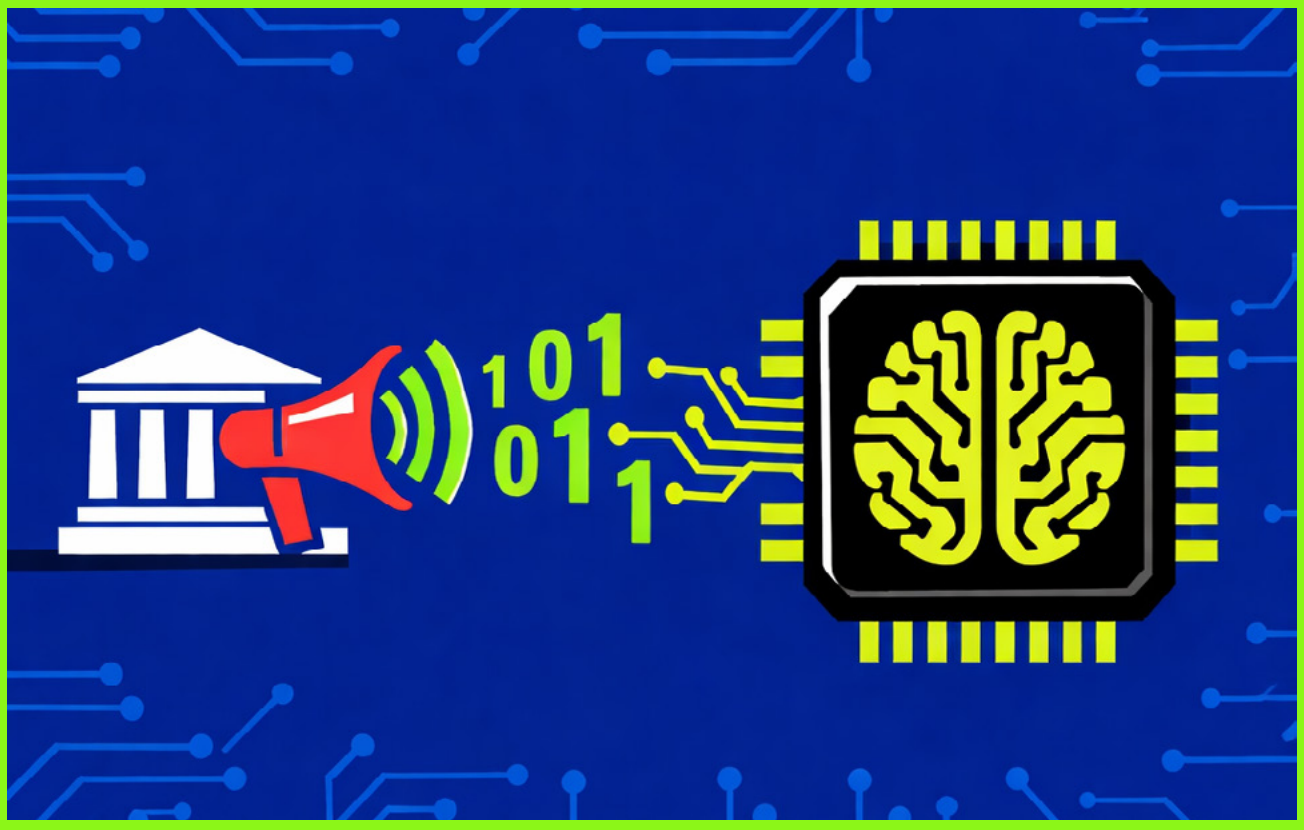
ACAMS TODAY™

AI in AML:

A guide to governance and implementation



The transformation from rule-based to artificial intelligence (AI)-driven anti-money laundering (AML) systems is not just inevitable—it is essential. Current systems intercept less than 1% of an estimated $2 trillion laundered globally each year.[1] Despite financial institutions (FIs) spending roughly $206 billion annually on compliance efforts, the case for change is clear.[2] Both regulators and FIs recognize that AI offers superior pattern recognition, greater accuracy and significant efficiency gains.

Federal regulators have been actively encouraging AI adoption. The Office of the Comptroller of the Currency's acting comptroller emphasized that "AI has the potential to strengthen safety and soundness, enhance consumer protections, [and] improve the effectiveness of compliance functions."[3] Former Federal Reserve (Fed) vice chair, Lael Brainard noted that machine learning-based fraud detection tools can "identify suspicious activity with greater accuracy and speed."[4] Furthermore, the Financial Crimes Enforcement Network (FinCEN) has been promoting innovative technologies for anti-money laundering/Bank Secrecy Act (AML/BSA) compliance since 2018. Research organizations like FinRegLab are also exploring advanced collaborative approaches such as federated learning, which could enable FIs to develop more robust AML models while preserving data privacy and competitive considerations.[5]

The regulatory message seems to encourage thoughtful AI adoption in AML, rather than simply permitting it. These governance requirements are manageable extensions of existing model risk management frameworks. Regulatory momentum alone, however, does not explain why AI has become so central to modern AML programs. As transaction volumes grow, typologies evolve faster and false positives continue to strain compliance teams; FIs are under pressure to demonstrate not just compliance, but effectiveness. This shift sets the stage for a deeper question: What is it about AI-driven approaches that make them uniquely suited to today's AML challenges?

This article provides a complete road map for responsible AI implementation in AML.[6] It will first examine the evidence demonstrating why AI works and where it delivers the greatest impact. Then the article will translate regulatory guidance into practical governance requirements, showing you exactly what to implement and how to de-risk your adoption. Finally, it will address the critical foundations of data quality and explainability that determine whether your AI initiative succeeds or fails. By the end, you will understand not just whether to adopt AI in AML—but how to do it confidently and compliantly.

Why AI works for AML

Proven benefits across multiple use cases

AI and machine learning have demonstrated measurable improvements in financial crime detection and operational efficiency.[7] The evidence base for AI's effectiveness in AML has grown substantially, moving beyond theoretical promises to documented results in production environments.[8]

McKinsey's research identifies AI-powered compliance as one of the most impactful use cases for FIs, noting that despite banks increasing know your customer/AML spending by up to 10% annually in some advanced markets, current systems detect only about 2% of global financial crime flows—making AI adoption not just beneficial but essential to address this fundamental ineffectiveness.[9]

Enhanced detection capabilities

According to Guidehouse's validation study, 61% of FIs reported risk reduction after implementing AI and machine learning solutions in their AML programs.[10] This improvement stems from AI's superior pattern recognition capabilities, which can identify complex relationships and behavioral patterns that are not evident to human analysts reviewing cases individually.[11]

In addition, unlike traditional rule-based systems, AI models can process both structured transaction data and unstructured information—such as news articles, beneficial ownership documents and adverse media—at scale, synthesizing insights across diverse data sources.[12] Perhaps most significantly, AI enables real-time detection capabilities that legacy rule-based systems simply cannot match, allowing institutions to identify and respond to suspicious activity as it occurs rather than discovering it weeks or months later during periodic reviews.

Operational efficiency

Beyond improved detection, AI delivers substantial operational benefits that address the resource constraints facing compliance departments. FIs implementing AI-powered transaction monitoring have achieved significant reductions in false positive rates, with many reporting improvements of 50-70% compared to their previous rule-based systems.[13] For a typical compliance team of 50 analysts at $60,000 per head—representing $3 million in annual labor costs—a 50-70% reduction in false positives can translate to cost savings or redeployment opportunities in the range of $1.5 to $2.1 million annually.

Automated alert prioritization directs analyst attention to the highest-risk cases first, ensuring that limited investigative resources focus on matters most likely to represent genuine money laundering activity.

AI systems can also generate prepopulated investigative summaries that accelerate case resolution by assembling relevant transaction history, relationship networks and risk indicators before an analyst begins their review. These efficiency gains translate directly to cost savings, allowing institutions to maintain or improve their detection effectiveness while managing compliance expenses more sustainably.

Key applications delivering results

Transaction monitoring: AI-powered transaction monitoring goes beyond static rules to deliver intelligent risk detection. AI systems can analyze both structured transaction data and unstructured information (such as payment narratives and communications), generate contextual explanations for each alert, autonomously prioritize investigation queues and continuously adapt to emerging typologies based on investigator feedback—creating a responsive system that improves with use.

Customer risk assessment: Machine learning enables continuous risk scoring updates as new information emerges, moving beyond the periodic reassessments typical of traditional systems. Behavioral profiling considers actual customer activity rather than relying solely on static demographic factors, while network analysis reveals

hidden relationships and beneficial ownership structures that might otherwise remain obscured.

Sanctions screening: Natural language processing significantly improves name matching accuracy, reducing the false positives that plague traditional fuzzy matching approaches. Entity resolution capabilities consolidate fragmented customer records across systems and contextual analysis helps distinguish between sanctioned individuals and innocent parties who happen to share common names.[14]

Typology detection: Supervised learning models identify known money laundering patterns with high accuracy when trained on historical suspicious activity report (SAR) data and confirmed cases. Unsupervised learning surfaces emerging typologies before they are formally documented in regulatory guidance, while graph analytics detect complex layering schemes that span multiple accounts and entities.

While these technical capabilities demonstrate AI's power in financial crime detection, their practical value depends on regulatory acceptance and supervisory comfort with these approaches. Understanding how regulators view these AI systems is essential to designing governance frameworks that satisfy both compliance obligations and business objectives. The regulatory perspective shapes not only what institutions can do with AI, but how they should structure their implementation and oversight processes.

The regulatory perspective

Federal regulators view AI as a solution to current AML system ineffectiveness. As former Fed vice chair Brainard noted, firms see AI as having "superior ability for pattern recognition" and "better predictive power" compared to traditional approaches.[15] The Fed's research shows that machine learning models consistently outperform conventional forecasting methods in identifying risk patterns.

Regulators also recognize AI's potential to expand financial inclusion by enabling institutions to serve higher-risk customer segments with appropriate controls—reducing the "de-risking" phenomenon where banks exit entire market segments due to risk and compliance concerns. Across these use cases, institutions that succeed treat AI models as governed assets rather than experimental tools, subject to the same rigor as credit or capital models.

Understanding governance requirements

Familiar frameworks applied to new technology

With regulatory support established, the question becomes: What do regulators actually require? The good news is that AI model governance for AML builds existing regulatory frameworks rather than creating entirely new requirements. The Fed's SR 11-7 Guidance on Model Risk Management,[16] dating from 2011 and issued jointly with the Office of the Comptroller of the Currency,[17] provides the foundational principles—though regulators acknowledge it needs adaptation for modern AI applications.

The SR 11-7 foundation

The three core components remain relevant for AI and machine learning models in AML:

1. **Conceptual soundness:** Understanding how the model works, its underlying theory, and why it is appropriate for its intended use case
2. **Ongoing monitoring:** Tracking performance over time to ensure the model continues to perform as expected and identifying when recalibration may be needed
3. **Validation:** Independent review of model effectiveness, limitations and assumptions by qualified personnel not involved in the model's development

FIs already apply these principles to credit models, stress testing models and capital adequacy models. AML AI models fit within this established framework, allowing institutions to leverage existing model risk management infrastructure, governance committees and subject-matter expertise.

What is different for AI?

The complexity and "black box" nature of some AI models create specific considerations that extend beyond traditional model governance:

- **Explainability:** While traditional rules state "if X > threshold, then alert," AI models weigh hundreds of features simultaneously through complex nonlinear relationships. However, modern techniques like SHapley Additive exPlanations (SHAP) values,

feature importance rankings, Local Interpretable Model-agnostic Explanations (LIME) and model-agnostic explanations can illuminate decision-making processes sufficiently to meet regulatory expectations for transparency.[18]

- **Dynamic learning:** Models that continuously retrain new data require different validation approaches than static rule sets that remain unchanged for months or years. Performance monitoring must be more frequent and validation protocols should account for model drift. But this is a manageable difference, not an insurmountable obstacle. Governance should also address model retirement and challenger models, defining criteria for when a model must be replaced, and how alternative approaches are evaluated and, if superior, promoted into production.
- **Data dependency:** AI models are highly sensitive to training data quality, completeness and representativeness—requiring robust data governance frameworks that many institutions are already building for other regulatory and business purposes. Data lineage, quality controls and bias testing become critical components of the governance framework.

Regulatory clarity emerging

While there is not yet comprehensive AI-specific AML guidance, regulators have provided directional clarity that allows responsible innovation:

- The Federal Reserve acknowledges SR 11-7 needs updating for modern AI and is actively engaging with industry experts and technology providers to develop appropriate adaptations.
- FinCEN, the Financial Conduct Authority, the Monetary Authority of Singapore, and the Australian Transaction Reports and Analysis Centre have issued statements supporting responsible AI use in AML with appropriate controls.[19]
- Examiners increasingly understand AML/machine learning technology through dedicated training programs, industry consultation and hands-on review of pilot implementations.

Given the benefits, the industry consensus is moving toward implementing AI with appropriate guardrails rather than waiting for regulatory clarity that may be years away.

The LLM question

Uncertainty remains around large language model (LLM) governance requirements in AML contexts.

While there is not yet comprehensive AI-specific AML guidance, regulators have provided directional clarity that allows responsible innovation

Current guidance focuses primarily on predictive models and classification algorithms. For LLMs used in AML contexts (e.g., SAR narrative generation, document analysis, customer communication review), institutions should:

- Document use cases clearly and specify decision-making authority (advisory vs. determinative)
- Maintain human oversight for all compliance-critical decisions, with qualified personnel reviewing and approving outputs
- Apply existing model governance principles while actively monitoring for emerging regulatory guidance specific to generative AI
- Participate in industry working groups shaping future standards and sharing best practices for LLM governance in financial crime compliance

Institutions should explicitly control LLM access to sensitive data, enforce strict prompt and response logging, and ensure red-teaming or adversarial testing is performed to uncover hallucinations or unsafe recommendations before production use.

Understanding the regulatory framework provides direction, but institutions need concrete practices to implement these principles effectively. The governance requirements that follow represent the nonnegotiable foundation—the baseline every institution must establish regardless of AI maturity or deployment scope. These fundamentals enable responsible innovation while satisfying regulatory expectations.

Ready to implement? Here is your road map

We have covered the business case for AI in AML, demonstrated where it delivers measurable value and mapped the regulatory landscape. The message is clear: AI adoption is not only permitted but encouraged by regulators who recognize its potential to address the fundamental ineffectiveness of legacy AML systems.

Understanding the framework, however, is not the same as implementing it. Knowing that SR 11-7 applies to your AI models does not tell you what to log, how to validate or when to deploy.

The second installment of this series provides the operational playbook: the specific governance practices you must establish before production deployment, proven strategies for de-risking your rollout, and practical approaches to the data quality, bias testing and explainability challenges that determine success. If Part 1 answered "why AI?" and "what do regulators expect?", Part 2 answers "what exactly do I need to build?" and "how do I deploy it safely?"

Look for part 2 of this article on acams.org under *ACAMS Today* Perspectives for the complete implementation framework, including audit trail requirements, validation protocols, phased deployment strategies and explainability techniques that satisfy both investigators and examiners.

Dustin Eaton, CAMS, CGSS, CAFCA, CAMS-RM, CTMA, CAFS, CKYCA, principal, AML & Fraud, Taktile, dustin.eaton@taktile.com,

Maximilian Eber, co-founder & CPTO, Taktile, maximilian.eber@taktile.com,

1 "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes," *United Nations Office on Drugs and Crime*, https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf

2 "Global Financial Crime Compliance Costs Continue to Rise," *LexisNexis Risk Solutions*, September 26, 2023, https://risk.lexisnexis.com/about-us/press-room/press-release/20230926-global-financial-crime-compliance-costs

3 "Artificial Intelligence and Bank Supervision," *Federal Reserve Bank of Richmond*, 2023, https://www.richmondfed.org/publications/research/econ_focus/2023/q2_federal_reserve

4 Lael Brainard, "Supporting Responsible Use of AI and Equitable Outcomes in Financial Services," *Board of Governors of the Federal Reserve System*, January 12, 2021, https://www.federalreserve.gov/newsevents/speech/brainard20210112a.htm

5 "Proposed Research: Assessing Federated Machine Learning's Potential for Transforming KYC/AML," *Financial Regulation Innovation Lab (FinRegLab)*, https://finreglab.org/research/proposed-research-assessing-federated-learning-for-bsa-aml/

6 Throughout this article, the term "AI" is used to encompass both classical machine learning techniques applied to structured data and generative AI technologies including LLMs.

7 "How Agentic AI Can Change the Way Banks Fight Financial Crime," *McKinsey & Company*, August 7, 2025, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-agentic-ai-can-change-the-way-banks-fight-financial-crime

8 Venkata Raja Ravi Kumar Gelle, "Enhancing Financial Security: AI-Driven Anti-Money Laundering (AML) and Compliance Monitoring in the Banking Sector," *World Journal of Advanced Research and Reviews*, https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-0365.pdf

9 "How Agentic AI Can Change the Way Banks Fight Financial Crime," *McKinsey & Company*, August 7, 2025, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-agentic-ai-can-change-the-way-banks-fight-financial-crime

10 "Key Considerations for Validation of AI/Machine Learning Models In the AML Space," *Guidehouse*, March 13, 2023, https://guidehouse.com/insights/financial-crimes/2023/considerations-for-validation-of-ai-models-in-aml

11 Zhiyuan Chen, Le Dinh Van Khoa, Ee Na Teoh, et al., "Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review," *Springer Nature Link*, https://link.springer.com/article/10.1007/s10115-017-1144-z

12 Emre Ires, "How AI Is Enhancing Anti-Money Laundering (AML) Compliance in Financial Institutions," *Strategy Software*, https://www.strategysoftware.com/blog/how-ai-is-enhancing-anti-money-laundering-aml-compliance-in-financial-institutions

13 "AI and Machine Learning in AML: Hype vs. Reality in Combating Financial Crime," *Business & Financial Times Online*, July 23, 2025, https://thebftonline.com/2025/07/23/ai-and-machine-learning-in-aml-hype-vs-reality-in-combating-financial-crime/

14 "Can LLMs Improve Sanctions Screening in the Financial System? Evidence from a Fuzzy Matching Assessment," *Federal Reserve Board*, 2025, https://www.federalreserve.gov/econres/feds/files/2025092pap.pdf

15 Lael Brainard, "What Are We Learning about Artificial Intelligence in Financial Services?", *Board of Governors of the Federal Reserve System*, November 13, 2018, https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm

16 "Guidance on Model Risk Management (SR 11-7)," *Board of Governors of the Federal Reserve System*, April 4, 2011, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

17 "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management," *Office of the Comptroller of the Currency*, April 4, 2011, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html

18 "How Model Risk Management (MRM) Teams Can Comply with SR 11-7," *ValidMind*, https://validmind.com/blog/sr-11-7-model-risk-management-compliance/

19 "Opportunities and Challenges of New Technologies for AML/CFT," *Financial Action Task Force*, July 2021, https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html