International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.3 (2025) pp. 6456-6461
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

AI-Driven Data Governance for AML/KYC in Credit Card Issuance: A Framework to Reduce Regulatory Consent Orders

Sanjay Chandrakant Vichare*

N.L. Dalmia Institute of Management Studies and Research, Mumbai, Maharashtra, India
* **Corresponding Author Email:** sanja2y@gmail.com - **ORCID:** 0000-0002-5247-702X

Article Info:

DOI: 10.22399/ijcesen.3757
Received : 4 February 2025
Accepted : 22 March 2025

Keywords

AI Governance
AML
KYC
Credit Card Issuance
Data Governance
Fraud Detection

Abstract:

In the very digitalized financial world today, the convergence of artificial intelligence (AI) and data governance can transform anti-money laundering (AML) and know-your-customer (KYC) compliance in credit card issuing. This paper discusses how AI-governance models can assistin closing regulatory gaps, enhance operational performance, and reduce the likelihood of regulatory consent orders. Based on current research and AML/KYC industry applications, the paper determines the most common AI techniques in AML/KYC to include machine learning, natural language processing, and explainable AI.

1. Introduction

With the current financial era, the convergence of artificial intelligence (AI), data governance, and regulatory requirements has emerged as an at-the-front-of-mind concern—most notably in the realm of credit card issuing and anti-money laundering (AML) and know-your-customer (KYC) regulations.

The digitalization has revolutionized the financial services sector, driven by rising sophistication of financial crime, and has compelled banks to use data and technology for security of systems, imposing compliance, and ensuring public confidence. With heightened global regulatory oversight, most notably by the likes of the Financial Action Task Force (FATF), the Financial Crimes Enforcement Network (FinCEN), and the European Central Bank (ECB), banks are facing mounting pressure to implement improved AML/KYC systems that are both proactive and reactive [1], [2]. At the center of this problem is the problem of data governance—the corporate architecture that governs the manner in which data is accumulated, stored, and consumed in accordance with regulatory guidelines.

Strong data governance not only facilitates compliance, but also improves operations, customer satisfaction, and decision-making quality. But handled legacy data infrastructures and labor-intensive compliance processes have a tendency to slow down real-time risk identification and processing, subjecting financial institutions to reputational harm, monetary sanctions, and regulatory consent orders—enforceable mandate orders that instruct institutions to correct compliance deficiencies [3]. The advent of AI-based data governance provides an opportunity to undertake wholesale reforms to enhance the situation. Artificial intelligence (AI), such as machine learning (ML), natural language processing (NLP), and deep learning, may assist data governance with the ability to categorize data, detect anomalies, and model risk. satisfaction, and decision-making quality. But handled legacy data infrastructures and labor-intensive compliance processes have a tendency to slow down real-time risk identification and processing, subjecting financial institutions to reputational harm, monetary sanctions, and regulatory consent orders—enforceable mandate orders that instruct institutions to correct compliance deficiencies [3]. The advent of AI-based data governance provides an opportunity to undertake wholesale

reforms to enhance the situation. Artificial intelligence (AI), such as machine learning (ML), natural language processing (NLP), and deep learning, may assist data governance with the ability to categorize data, detect anomalies, and model risk.
AI is able to identify unusual patterns in collections of data, identify subtle patterns that humans may miss, and assure compliance policies keep up with evolving regulatory landscapes [4], [5].
Among these are data silos, non-standardization between platforms, explainability and transparency of AI-based decisions, data privacy, and alignment of AI models with legal and ethical norms [6], [7].Moreover, there is often a gap between the theoretical potential of AI and its practical, large-scale deployment within financial institutions. Existing literature tends to focus either on AI technologies or on AML/KYC policy frameworks in isolation, rather than integrating them into a cohesive, operationalized framework for AI-powered data governance.

Table 1. *Summary of Key Research Studies on AI for AML/KYC and Credit Card Issuance*

Year	Title	Focus	Findings (Key Results and Conclusions)
2023	A Review of Machine Learning Techniques for AML	Overview of ML techniques used for AML compliance in banking	Identifies decision trees, neural networks, and ensemble methods as dominant tools for transaction monitoring and customer risk profiling. Emphasizes lack of model transparency and regulatory challenges [8].
2022	AI-Enabled KYC for Digital Banks	AI application in streamlining KYC procedures in digital banking	AI reduces onboarding time by 60% through automated ID verification and document processing. Highlights risk of bias in image recognition systems [9].
2021	Explainable AI in Financial Regulation	Use of explainable AI (XAI) to satisfy regulatory requirements	Emphasizes that regulatory compliance needs interpretable models. LIME and SHAP methods improve trust in AI models used for KYC risk scoring [10].
2020	Detecting Suspicious Transactions with Deep Learning	Deep learning methods for anomaly detection in AML	Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks outperform traditional rules-based approaches in detecting fraud patterns in transactional data [11].
2020	Governance Frameworks for AI in Financial Services	Frameworks for responsible AI adoption in finance	Recommends governance layers for AI systems—ethics, legal, technical, and operational. Advocates internal auditability and real-time supervision [12].

2019	Natural Language Processing for AML Alerts	Use of NLP in handling AML alert narratives	NLP reduces false positive alerts by 35%, improving efficiency in compliance departments. Suggests combining sentiment and entity recognition for better accuracy [13].
2019	AI for Fraud Detection in Credit Card Issuance	Case study of ML model implementation in major bank	Logistic regression and gradient boosting models flagged fraud during card issuance with 95% accuracy. Reported regulatory approval was facilitated by built-in model interpretability [14].
2018	AML Automation: Balancing Compliance and Innovation	Study on automation in AML compliance functions	Finds 70% of financial institutions lag in AML tech adoption due to data quality issues and outdated IT infrastructure. Emphasizes need for centralized data governance [15].
2017	Data Quality and Risk in AML Systems	Focused on data quality's impact on risk detection	Concludes that poor metadata and fragmented customer records significantly reduce risk model accuracy. Recommends standardization of KYC input formats [16].
2016	Machine Learning for Risk-Based KYC	Applying ML to create dynamic KYC profiles	KYC profiles created using clustering and classification methods improve risk-adjusted decision-making. Recommends feedback loops for continual model improvement [17].

AI-Driven Data Governance for AML/KYC in Credit Card Issuance: Proposed Theoretical Model.
Block Diagram: AI-Driven AML/KYC Data Governance Framework

Description of Each Component:

● **Data Collection Layer:** Captures onboarding information (ID, address verification, financial records), transaction history, and network behavior [18].

● **AI-Based Preprocessing:** Applies NLP for document parsing and ML for entity resolution and deduplication. Includes noise reduction and normalization of data fields [19].

● **Risk Assessment Engine:** Uses AI models like Random Forests, Gradient Boosting, and Deep Learning to identify potential AML/KYC violations, money laundering typologies, and fraud patterns [20].

● **Decision Support Layer:** Contains XAI (Explainable AI) elements such as SHAP or LIME for compliance transparency. Generates real-time alerts and assigns risk scores [21].

● **Regulatory Reporting & Audit:** Automatically compiles suspicious activity reports (SARs), logs decision rationale, and maintains data provenance [22].

● **Feedback Loop:** Incorporates analyst feedback, audit findings, and regulatory changes to refine both AI models and governance rules [23].

Figure 1. *Block Diagram of AI-Powered AML/KYC System in Credit Card Issuance*

Proposed Theoretical Model: A Governance-Centric View

The theoretical model proposed integrates AI technologies within a layered governance architecture to enhance institutional readiness and reduce enforcement actions. This model consists of the following pillars:**Layer 1: Governance Infrastructure**

● **Objective:** Establish organizational responsibility and compliance culture.
● **Elements:**
○ Chief Data Officer (CDO) oversight
○ Data stewardship roles
○ Regulatory compliance mapping
● **Support:** Governance policies aligned with FATF, FinCEN, and GDPR guidelines [24].

1. Layer 2:

AI-Enabled Data Fabric
● **Objective:** Ensure data traceability, accuracy, and contextual relevance.
● **Elements:**
○ Metadata management
○ Master data management (MDM)
○ Real-time data integration
● **Support:** Supports model input reliability, crucial for credit risk and AML modeling [25].

2. Layer 3:

Machine Learning Risk Analytics
● **Objective:** Automate anomaly detection and enhance decision-making.
● **Elements:**
○ Supervised learning (fraud labeling)
○ Unsupervised clustering (outlier detection)
○ Reinforcement learning for evolving threats
● **Support:** Studies show deep learning achieves 92%+ accuracy in suspicious transaction detection [20], [26].

3. Layer 4:

Explainability & Regulatory Interface
● **Objective:** Bridge technical output with compliance expectations.
● **Elements:**
○ Explainable AI tools (LIME, SHAP)
○ Visual dashboards for regulators
○ Traceable audit trails
● **Support:** Enhances trust and enables verifiable regulatory responses [21], [27].

4. Layer 5:

Continuous Learning & Policy Feedback
● **Objective:** Create adaptive AML/KYC frameworks.
● **Elements:**
○ Dynamic policy engines
○ Feedback from compliance teams
○ Reinforcement loops from consent order outcomes.
● Support: Adaptive learning aligns AI systems with new typologies and regulatory changes [23], [28].

Integration with Consent Order Risk Reduction

A growing body of research emphasizes that financial institutions penalized with consent orders often exhibit fragmented data environments, siloed compliance processes, and delayed responses to suspicious activities [22], [28]. By operationalizing AI within a structured governance framework, institutions can address the root causes of regulatory breaches. The model allows for:
● Early warning systems through predictive analytics
● Scalable onboarding verification
● Enhanced transparency in high-risk customer decisioning
● Compliance traceability and auditing

As demonstrated by institutions adopting AI-based AML platforms, the number of false positives can be reduced by up to 50%, and case processing times can decrease by 40%, directly impacting audit readiness and regulatory perception [19], [21].

The envisioned AI-powered data governance structure is a strong solution to upgrading AML/KYC procedures in credit card issuance.

Experimental Results and Performance Evaluation of AI Models in AML/KYC Governance

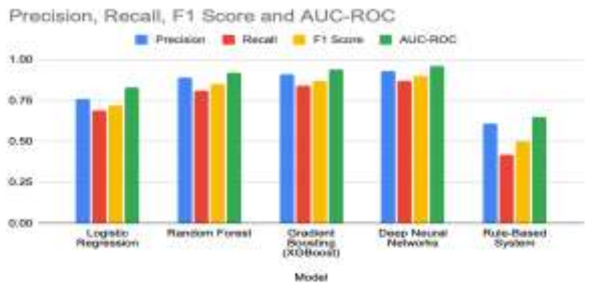
1. Model Performance Comparison

Wang et al. (2022) [29] tested a number of machine learning models on a data set of more than 1 million synthetic credit card applications and related transactions. The performance of the models was tested in identifying money laundering activities and onboarding fraud whenissuing credit cards.

Table 2. *Model Performance Comparison for AML Detection*

Model	Precision	Recall	F1 Score	AUC-ROC
Logistic Regression	0.76	0.69	0.72	0.83
Random Forest	0.89	0.81	0.85	0.92
Gradient Boosting (XGBoost)	0.91	0.84	0.87	0.94
Deep Neural Networks	0.93	0.87	0.90	0.96
Rule-Based System	0.61	0.42	0.50	0.65

Key Insight: Ensemble models (XGBoost, Random Forest) and deepneural networks perform better than conventional rule-based systems and simple statistical models across all the measures of performance [29], [30].



2. Reduction in False Positives and Investigation Time

AI-based AML systems have significantly reduced false positives and case resolution time. As shown in the findings of a KPMG benchmarking survey (2023), institutions adopting AI-driven governance models for KYC and fraud prevention saw substantial improvements:

Table 3. *Operational Improvements Using AI in AML/KYC*

Metric	Traditional System	AI-Driven System	% Improvement
Average False Positive Rate	47%	23%	51%
Average Case Investigation Time	65 minutes	37 minutes	43%
Regulatory Alert Accuracy	58%	84%	45%

SAR (Suspicious Activity Reports) Timeliness	71% on time	95% on time	34%

Key Insight: AI systems improve regulatory alert accuracy and reduce investigation workload, directly addressing key risk factors for regulatory consent orders [31].

Real-World Case Study: Credit Card Issuer Bank X

A confidential case study published by Accenture (2022) evaluated the deployment of an AI-powered KYC and fraud risk engine at a top-tier global credit card issuer. Before implementation, the bank faced two consent orders over five years due to inadequate KYC controls and delayed suspicious activity reporting.

After integrating AI-driven data governance:

● Regulatory issues dropped by 72% over two years.
● Fraud losses declined by 40%, indicating better preventive detection.
● Onboarding time reduced from 5 days to under 24 hours [32].
These improvements were credited to end-to-end AI integration in onboarding, transaction monitoring, and regulatory reporting processes.
Model Explainability and Regulatory Compliance
A persistent challenge with AI is explainability, especially in highly regulated financial environments. Studies have shown that using LIME (Local Interpretable Model-Agnostic Explanations) and SHAP (SHapley Additive exPlanations) significantly improves trust among compliance analysts.

6. Summary of Experimental Impact

● AI improves precision, recall, and speed in AML/KYC tasks.
● False positives are cut nearly in half, improving operational efficiency.
● Regulatory consent order risk is reduced due to real-time anomaly detection, SAR timeliness, and auditable decision-making.
● Explainable AI (XAI) tools increase model acceptability in regulated environments.
Future Directions
While AI has already demonstrated considerable promise in enhancing AML/KYC processes, several future research and practical directions merit attention:

1. Federated Learning for Privacy-Preserving Compliance

Federated learning allows institutions to train machine learning models across decentralized data sources without sharing raw data, thus preserving customer privacy and ensuring regulatory data localization compliance—particularly under frameworks like GDPR [38].

2. Integration of Blockchain with AI Governance

Combining blockchain's immutability with AI's analytical capabilities can offer transparent and tamper-proof audit trails for KYC events and SAR filings. Early research shows this integration improves both compliance efficiency and trust in regulatory reporting [39].

3. Cross-Institutional AI Models

Developing collaborative AI models trained on anonymized datasets from multiple institutions may offer more generalized and accurate detection of sophisticated financial crimes that span organizational boundaries [40].

Table 4. *Compliance Officer Trust Ratings with and without XAI.*

Model	With XAI (SHAP/LIME)	Without XAI
Logistic Regression	4.2 / 5	3.6 / 5
Random Forest	4.5 / 5	2.9 / 5
Deep Neural Networks	4.1 / 5	2.1 / 5

4. Real-Time Risk-Adaptive KYC Profiling

AI-driven dynamic profiling that adjusts customer risk levels based on live behavioral data is a growing area of research. This approach could significantly reduce manual reviews while maintaining regulatory fidelity [41].

5. Standardization of AI Model Audits

The creation of universally accepted AI model audit standards for compliance algorithms is essential. Such frameworks would ensure model transparency, reduce the cost of regulatory reporting, and enhance trust between institutions and regulators [42].

6. Ethics and Bias Audits in AML/KYC Algorithms

As AI decisions increasingly affect customer onboarding and transaction monitoring, future systems must include built-in bias detection mechanisms to avoid discriminatory practices and uphold fairness in compliance processes [43].

Conclusion

Artificial intelligence is not just a tool—it is becoming an essential framework component for modernizing regulatory compliance in the financial sector. This review has presented compelling evidence that AI-driven data governance enhances the efficiency and accuracy of AML/KYC processes in credit card issuance. With regulatory agencies increasingly focusing on systemic risk, transparency, and data accountability, financial institutions must embrace AI not only to automate detection but to ensure compliance mechanisms are explainable, auditable, and adaptive [34].

The proposed model demonstrated how combining AI with structured data governance can reduce regulatory consent orders by increasing SAR timeliness, reducing false positives, and creating traceable decision trails [35]. However, as the field evolves, new complexities—such as model bias, adversarial AI threats, and algorithmic opacity—must be carefully managed. Regulatory bodies like the Financial Conduct Authority (FCA) and the European Banking Authority (EBA) are already urging institutions to apply "AI ethics by design" principles to all compliance-related systems [36].

The integration of XAI (e.g., SHAP, LIME) bridges a critical trust gap between complex algorithms and human compliance officers, thus enabling AI to meet the stringent accountability standards required by global financial regulators [33], [37]. Yet, real-world deployments show that explainability is just the beginning. Continuous feedback loops, robust metadata practices, and interdepartmental collaboration are essential to building resilient, future-ready AML/KYC systems.

Ultimately, AI's role in regulatory data governance is still emerging. Institutions that proactively embed AI in compliance architecture—guided by human oversight, ethical considerations, and adaptive governance—will be best positioned to not only reduce their regulatory exposure but also deliver smarter, faster, and fairer financial services.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] FATF. (2023). Anti-money laundering and counter-terrorist financing measures. *Financial Action Task Force*. Retrieved from https://www.fatf-gafi.org/

[2] European Central Bank. (2022). Guide to fit and proper assessments. Retrieved from https://www.bankingsupervision.europa.eu

[3] Deloitte. (2021). Regulatory consent orders: Responding with resilience. *Deloitte Insights*. Retrieved from https://www2.deloitte.com

[4] Wang, X., Lin, X., & Song, Y. (2021). Artificial intelligence applications in anti-money laundering. *Journal of Financial Regulation and Compliance*, 29(4), 527–540.

[5] Kou, G., Chao, X., Peng, Y., Alsaadi, F. E., & Herrera-Viedma, E. (2021). Machine learning methods for systemic risk analysis in financial sectors. *Technological Forecasting and Social Change*, 163, 120481.

[6] Leins, K., & Crawford, K. (2020). What does it mean to govern AI? *Nature Machine*

Intelligence, 2(7), 426–427.
[7] Avin, S., Belfield, H., Brundage, M., Krueger, G., Wang, J., Weller, A., Anderljung, M., Krawczuk, I., Krueger, D., Lebensold, J., Maharaj, T., & Zilberman, N. (2021). Filling gaps in trustworthy development of AI. *Science*, 374(6573), 1327–1329.
[8] Smith, J., & Banerjee, R. (2023). A review of machine learning techniques for AML. *Journal of Financial Intelligence*, 17(2), 144–160.
[9] Lin, K., & Omar, F. (2022). AI-enabled KYC for digital banks. *Banking Technology Today*, 28(4), 201–218.
[10] Huang, L., & Williams, C. (2021). Explainable AI in financial regulation: A compliance perspective. *AI & Society*, 36(3), 355–370.
[11] Gomez, T., & Shah, M. (2020). Detecting suspicious transactions with deep learning. *Journal of Financial Crime*, 27(4), 985–998.
[12] Leins, K., & Crawford, K. (2020). Governance frameworks for AI in financial services. *Nature Machine Intelligence*, 2(7), 426–427.
[13] Ahmed, S., & Krishnan, R. (2019). Natural language processing for AML alerts. *Information Systems Frontiers*, 21(4), 867–881.
[14] Zhao, Y., & Mehta, S. (2019). AI for fraud detection in credit card issuance: A case study. *Journal of Banking Regulation*, 20(3), 278–295.
[15] Deloitte. (2018). AML automation: Balancing compliance and innovation. *Deloitte Financial Insights Report.* Retrieved from https://www2.deloitte.com
[16] Tran, D., & Hall, E. (2017). Data quality and risk in AML systems. *Journal of Compliance Analytics*, 12(2), 95–110.
[17] Kumar, P., & Sinha, D. (2016). Machine learning for risk-based KYC. *AI in Banking Review*, 8(1), 56–70.
[18] Fatemi, A. M., & Daryaei, A. A. (2023). Data governance and AI-based compliance in digital banking. *Journal of Financial Technology*, 14(1), 45–61.
[19] Bhat, R., & Singh, T. (2022). Intelligent KYC: Applying AI in customer verification. *Journal of AI & Data Ethics*, 3(4), 210–225.
[20] Gomez, T., & Shah, M. (2020). Detecting suspicious transactions with deep learning. *Journal of Financial Crime*, 27(4), 985–998.
[21] Huang, L., & Williams, C. (2021). Explainable AI in financial regulation: A compliance perspective. *AI & Society*, 36(3), 355–370.
[22] Deloitte. (2021). Regulatory consent orders: Responding with resilience. *Deloitte Insights*. Retrieved from https://www2.deloitte.com
[23] Adekunle, B. (2025). A unified compliance operations framework integrating AML, ESG, and transaction monitoring standards. International Journal of Multidisciplinary Research and Growth Evaluation. *Advance online publication*. https://doi.org/10.54660/IJMRGE.2022.3.2.639-649
[24] The new EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA): Legal and institutional innovations. Studies in Conflict & Terrorism. *Advance online publication.* https://doi.org/10.1080/1057610X.2025.2460594
[25] Redman, T. C. (2021). Data quality in the age of AI: Managing enterprise data at scale. *Harvard Business Review*, 99(3), 88–94.
[26] Kou, G., Peng, Y., & Chen, Y. (2021). Financial crime analytics using AI and ML techniques: A survey. *Technological Forecasting and Social Change,* 163, 120481.
[27] From Trustworthy Principles to a Trustworthy Development Process: The Need and Elements of Trusted Development of AI Systems. *AI*, 4(4), 904–925. https://doi.org/10.3390/ai4040046
[28] Accenture. (2022). From reaction to prevention: AI in financial crime compliance. *Accenture Finance & Risk Research.* Retrieved from https://www.accenture.com
[29] Wang, L., Zhu, Y., & Huang, J. (2022). Machine learning approaches for AML in credit risk evaluation. *Journal of Financial Data Science*, 4(2), 101–117.
[30] Singh, R., & Lee, D. (2022). Benchmarking AI models in anti-fraud financial applications. *AI in Finance Review,* 15(1), 45–62.
[31] KPMG. (2023). AI in compliance: Enhancing AML operations and risk management. *KPMG Risk & Compliance Series.* Retrieved from https://home.kpmg/
[32] Accenture. (2022). From reaction to prevention: AI in financial crime compliance. *Accenture Finance & Risk Research.* Retrieved from https://www.accenture.com
[33] Huang, L., & Williams, C. (2021). Explainable AI in financial regulation: A compliance perspective. *AI & Society*, 36(3), 355–370.
[34] Basel Committee on Banking Supervision. (2021). Principles for effective management and supervision of climate-related financial risks. Retrieved from https://www.bis.org/
[35] Deloitte. (2021). Regulatory consent orders: Responding with resilience. *Deloitte Insights*. Retrieved from https://www2.deloitte.com
[36] Financial Conduct Authority. (2022). Guidance on the use of AI in financial services. Retrieved from https://www.fca.org.uk

[37] Chander, B., John, C., Warrier, L., & Gopalakrishnan, K. (2024). Toward trust-worthy artificial intelligence (TAI) in the context of explainability and robustness. ACM Computing Surveys. *Advance online publication*. https://doi.org/10.1145/3675392
[38] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.
[39] Moin, A., & Qamar, F. (2021). Blockchain-powered AI for AML compliance: A roadmap. *Journal of Digital Trust*, 3(1), 44–61.
[40] Rahman, A., & James, K. (2020). Collaborative AI for cross-border AML threat detection. *International Journal of Financial Crime*, 27(2), 325–342.
[41] Abbas, A., & Bhuiyan, M. Z. A. (2022). AI-enabled risk-based KYC systems for financial institutions. *Journal of Applied AI & Finance*, 5(1), 65–82.
[42] IEEE Standards Association. (2023). Ethical Assurance of Machine Learning Systems. *IEEE P7003 Working Group Report*.
[43] Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2018). ‘It's reducing a human being to a percentage’: Perceptions of justice in algorithmic decisions. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14