AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Business Management, Economics and Banking
ISSN (E): 2832-8078 Volume 47, April - 2026

INTERNATIONAL EXPERIENCE IN ARTIFICIAL INTELLIGENCE IMPLEMENTATION IN AML SYSTEMS: ANALYSIS OF LEADING BANKS AND CIS COUNTRIES PRACTICES

Rashidov Avazbek Raximovich,
The Independent Applicant of Tashkent
State University of Economics, Tashkent, Uzbekistan.
Email: arfinancier@gmail.com
ORCID: 0009-0001-7054-9758
Tel.: +998 90 989 0008

ABSTRACT

The global banking system is actively implementing artificial intelligence technologies to combat money laundering and terrorist financing. This article presents a systematic analysis of international experience in applying AI technologies in AML systems of leading global banks and financial institutions of CIS countries. Cases of HSBC, JPMorgan Chase, Standard Chartered, Deutsche Bank, and Citibank demonstrating specific measurable implementation outcomes are analysed. Special attention is devoted to the state of AI adoption in the banking sectors of Russia, Kazakhstan, and other CIS countries, including a detailed analysis of Sberbank's experience. Critical limitations of traditional financial monitoring systems and the advantages of AI-based solutions are identified. Federated learning technology is examined as an innovative approach to interbank cooperation that does not require the disclosure of confidential client data.

KEYWORDS

Artificial intelligence, AML, international experience, machine learning, federated learning, financial monitoring, compliance, CIS countries, digital transformation.

Introduction

The global banking system is undergoing a fundamental transformation driven by the digitalisation of financial services, the deepening of international cooperation, and the growing complexity of capital flows. The exponential growth in transaction volumes and the widespread adoption of remote banking services is creating new challenges for anti-money laundering (AML) systems.

Traditional methods of detecting suspicious transactions, based on static rule sets and manual data processing, are demonstrating critical limitations under contemporary conditions. International

research indicates that the false positive rate in rule-based systems can reach 95-99%, placing an enormous burden on banks' internal compliance functions and increasing the risk of overlooking genuinely suspicious activity.

Against this backdrop, leading global banks are actively deploying artificial intelligence technologies to modernise their financial monitoring infrastructure. Global financial sector investment in AI is growing exponentially: from USD 35 billion in 2023 to a projected USD 97 billion by 2027, representing a compound annual growth rate of 29%.

The objective of this study is to conduct a systematic analysis of international experience in implementing AI technologies in AML systems, to examine the practices of leading global banks, and to assess the current state of AI adoption in the banking sectors of CIS countries, including the identification of key success factors and barriers to technological transformation.

Materials and Methods

The methodological foundation of this study comprises a comprehensive approach encompassing the analysis of international regulatory standards, public reporting of leading global banks, research outputs of international consultancy firms, and academic literature on the application of artificial intelligence in financial monitoring.

The study employs comparative analysis to evaluate the practices of various financial institutions; a case study method for detailed examination of AI implementation experience in specific banks; and statistical analysis to identify trends in AI adoption at both global and regional levels.

The information base of the study includes reports of the Financial Action Task Force (FATF), public disclosures of HSBC, JPMorgan Chase, Standard Chartered, Deutsche Bank, and Citibank; research publications by Boston Consulting Group and McKinsey; data from Statista and Gartner research agencies; and publications on AI implementation outcomes in the CIS banking sector, including Sberbank reporting, FinTech Association data, and materials from Kazakhstani financial regulators.

Results and Discussion

Critical Limitations of Traditional AML Systems and the Advantages of AI-Based Solutions

Traditional anti-money laundering systems, based on static rule sets and threshold values, exhibit multiple limitations whose severity is compounded in the context of banking digitalisation.

The most critical issue is the excessively high false positive rate. Transaction monitoring systems based on predefined rules establish fixed thresholds for suspicious activity. However, legitimate clients may conduct such transactions for entirely valid reasons. International research demonstrates that false positive rates in rule-based systems can reach 95-99%, meaning that only 1-5% of generated alerts relate to genuinely suspicious activity. This creates an immense burden on compliance teams, who must manually review thousands of false alerts, not only increasing operational costs but also elevating the risk of missing actual suspicious transactions due to "alert fatigue". Frequent unjustified blocking of legitimate clients' transactions negatively affects service quality and the institution's reputation.

Rule-based systems are characterised by excessive rigidity and an inability to adapt to evolving financial crime typologies. Traditional systems employ static rules developed from historical fraud cases, yet lack the flexibility to adapt to emerging patterns. Complex, multi-layered money laundering schemes involving chains of transactions through multiple accounts, financial institutions, and

jurisdictions remain invisible to rule-based systems, as each individual transaction may appear legitimate. Whenever a new fraud scheme emerges, manual rule updates are required – a process that takes time during which criminal activity may continue undetected.

The absence of real-time monitoring capability is a particularly critical limitation in the era of instant payments. Traditional systems are frequently based on batch processing conducted at intervals of several hours to a full day. Such detection latency impedes real-time fraud prevention. By the time a suspicious transaction is identified, funds may already have been transferred through numerous intermediary accounts or converted into cryptocurrency. This represents a reactive rather than a proactive approach to money laundering risk management.

Traditional suspicious activity detection systems rely exclusively on structured transaction data, disregarding critically important contextual factors. A client's behavioural profile, interaction history with the bank, and patterns of use of various financial instruments substantially affect the assessment of a transaction's legitimacy. Moreover, traditional systems are ill-equipped to process unstructured data–transaction narrative fields, email correspondence, information from open sources, and adverse media coverage.

Artificial intelligence systems fundamentally address these limitations through machine learning algorithms and contextual analysis. Rather than applying rigid thresholds, AI systems evaluate multiple factors holistically: a client's transaction history, behavioural patterns, geographic characteristics of transactions, and relationships with other participants in the financial system. A critically important advantage is the capacity for continuous learning from new data. Machine learning algorithms are capable of independently identifying previously unknown patterns of suspicious activity without the need to pre-programme specific rules.

Graph analytics and network analysis, implemented through AI, enable the visualisation and examination of complex relationships among financial transaction participants, revealing concealed networks used for money laundering. Graph analysis algorithms can identify structural patterns characteristic of criminal activity, such as circular fund transfers, the concentration of flows around specific nodes, or the use of multiple intermediary accounts to obscure the true origin of funds.

AI-driven transaction monitoring systems conduct real-time analysis, evaluating each transaction at the moment of initiation. Machine learning algorithms are capable of processing data streams at speeds unattainable by traditional systems, instantly identifying anomalies and generating alerts. This enables banks not merely to detect, but to prevent financial crimes by blocking suspicious transactions before they are completed.

Natural language processing technologies enable AI systems to analyse unstructured textual data: transaction descriptions, email messages, client documentation, and news articles. Named entity recognition algorithms automatically identify references to persons, organisations, and locations relevant to risk assessment. Sentiment analysis facilitates the evaluation of adverse media coverage of clients as an important indicator of reputational risk. Semantic analysis of transaction narratives identifies discrepancies between the stated purpose of a payment and the nature of the participants' business activities.

International Experience in AI Implementation in AML Systems of Leading Global Banks

An analysis of international experience in implementing artificial intelligence in AML systems at leading global banks demonstrates not only the technical feasibility and economic efficiency of AI-based solutions, but also provides valuable lessons for the banking systems of developing countries.

HSBC, one of the world's largest banks with a presence in more than 60 countries, faced serious compliance failings in the past that resulted in USD 1.9 billion in regulatory fines from US authorities in 2012 for inadequate transaction monitoring. In response to this regulatory pressure, HSBC invested substantial resources in modernising its anti-money laundering systems, including the deployment of an advanced machine learning-based transaction monitoring platform.

The implementation results were remarkable: the bank doubled the number of genuinely suspicious transactions identified compared to its previous rule-based system, while simultaneously reducing false positives by 20%, thereby freeing up significant compliance team capacity. This demonstrates that AI systems are not only more effective at detecting actual suspicious activity, but also reduce the operational burden on bank personnel.

JPMorgan Chase, the largest US bank by assets, deployed a comprehensive AI-based solution for Know Your Customer (KYC) processes, focusing on automating and accelerating client onboarding while simultaneously enhancing security. The implementation of AI solutions enabled a dramatic reduction in client verification time–from 3-5 business days to under 5 minutes for the majority of cases.

This constitutes a fundamental improvement in the client experience, as new customers can begin using banking services almost immediately upon application submission. The system detected and blocked 25% more fraudulent account opening applications involving forged or stolen identity documents compared to the previous approach, demonstrating that AI-powered automation can simultaneously improve both the client experience and security.

Standard Chartered, a global bank with a primary focus on Asia, Africa, and the Middle East, faced significant challenges in sanctions compliance screening and politically exposed person (PEP) monitoring. The bank implemented an AI-based sanctions compliance screening and PEP monitoring system. Implementation results include a 50% reduction in false positives, substantially alleviating the burden on compliance specialists and enabling them to concentrate on genuinely critical cases. This is particularly significant given the continuously expanding sanctions lists and the need to screen vast volumes of transactions in real time.

Deutsche Bank, Germany's largest bank, faced the challenge of detecting money laundering conducted through complex schemes involving shell companies. The bank deployed an AI-based AML/CFT analytical system specifically designed to identify complex network-based schemes. The system identified 35% more illicit transactions involving shell companies compared to the previous approach. The AI system identifies high-risk transactions five times faster than traditional methods through automated analysis of complex networks and patterns. The application of graph analytics enabled the visualisation of concealed relationships among various participants in money laundering schemes–connections that were undetectable by traditional methods.

Citibank, one of the world's largest international banks, required a system capable of real-time fraud detection and prevention. Citibank implemented an AI-based fraud detection system. Results include a 50% reduction in fraud losses, attributable to the AI system's ability to block fraudulent transactions

in real time before fund transfers are completed. The system identifies and blocks unauthorised transactions within seconds of initiation, demonstrating the critical importance of real-time analytical capability for effective financial crime prevention.

Table 1. AI Implementation Outcomes in AML Systems of Leading Global Banks

Bank	Solution Deployed	Key Outcomes	Implementation Period
HSBC	ML-based transaction monitoring system	Doubling of detected suspicious transactions; 20% reduction in false positives	2015-2018
JPMorgan Chase	AI-based KYC solution	Verification time reduced from 3-5 days to 5 minutes; 25% increase in fraudulent application detection	2017-2019
Standard Chartered	AI-based sanctions and PEP screening system	50% reduction in false positives	2018-2020
Deutsche Bank	AML/CFT analytical system with graph analytics	35% increase in illicit transaction detection; 5× faster identification	2019-2021
Citibank	Real-time fraud detection system	50% reduction in fraud losses; blocking within seconds	2020-2022

Analysis of these cases yields several key lessons. All banks under review commenced implementation with pilot projects in limited domains, gradually expanding the application of technologies as experience was accumulated and value was demonstrated. Successful AI implementation projects are characterised by strong executive sponsorship. All banks invested substantial resources in personnel training and organisational culture change. Integration with existing systems proved to be one of the principal challenges. Measuring and demonstrating results is critical for maintaining project momentum and justifying continued investment.

State of AI Implementation in the Banking Sectors of CIS Countries

A comparative analysis of AI implementation in the banking systems of CIS countries reveals a substantial regional lag behind global trends–a situation that paradoxically creates favourable conditions for banks that are prepared to adopt innovative solutions promptly. According to international consultancy research, as of 2024, only a small minority of banks in CIS countries have deployed fully functional AI solutions for financial monitoring and anti-money laundering, whereas in developed countries such technologies have become mainstream.

In Russia, the region's largest banking system, only Sberbank, VTB, and Gazprombank have implemented large-scale AI-enabled financial monitoring automation projects. According to the FinTech Association, Russia's largest banks invest approximately USD 1 billion per year in AI development, while mid-sized and smaller banks invest only RUB 100-300 million annually–a gap of approximately 500-fold. The majority of banks continue to rely on traditional rule-based systems, citing high implementation costs and a shortage of qualified specialists.

Sberbank exemplifies best practice in AI adoption within the banking sector, having integrated these technologies into 85% of its business processes with a cumulative financial effect of RUB 450 billion in 2024. The bank's anti-fraud system, based on machine learning and big data analytics, achieves 99.8% effectiveness while processing 150,000 transactions per second, enabling the real-time detection of suspicious transactions. The greatest economic impact has been realised in risk management and automated credit decisioning, where AI deployment has reduced application processing time from weeks to minutes.

Sberbank's experience highlights several defining characteristics of successful AI implementation. First, a strategic approach to digital transformation with full executive sponsorship. Second, substantial investments in developing internal competencies and building data science and machine learning specialist teams. Third, phased implementation beginning with pilot projects and progressively scaling across all processes. Fourth, the development of a proprietary technology ecosystem with the cultivation of partnerships with leading global technology companies.

Sberbank's approach to training machine learning models merits particular attention. The bank has assembled extensive labelled datasets comprising millions of historical transactions annotated with confirmed fraud case information. This has enabled the training of highly accurate models capable of detecting even complex multi-stage money laundering schemes. A continuous model quality monitoring system ensures regular retraining on new data, enabling adaptation to evolving financial crime patterns.

Table 2. **State of AI Implementation in the Banking Sectors of CIS Countries (2024)**

Country	AI Implementation Level	Leading Banks	Key Indicators	Global AI Index Ranking
Russia	Initial, fragmented	Sberbank, VTB, Gazprombank	85% of Sberbank processes; investment ~USD 1 bn/year by largest banks	31 of 83
Kazakhstan	Very low	Halyk Bank, Kaspi Bank	32% of market participants use AI; 45% plan adoption	76 of 193
Uzbekistan	Pilot projects	Uzpromstroybank, Asakabank	Isolated pilot projects	70 of 193 (1st in Central Asia)
Belarus	Early stage	–	Experimental projects	N/A
Azerbaijan	Early stage	–	Feasibility exploration	N/A
Kyrgyzstan	Minimal	–	Early-stage exploration	134 of 193
Tajikistan	Minimal	–	Early-stage exploration	131 of 193
Turkmenistan	Minimal	–	Early-stage exploration	153 of 193

In Kazakhstan, only 3-4 banks out of more than 20 in operation have deployed AI-based AML systems. Overall, research indicates that only 32% of Kazakhstan's financial market participants are utilising AI technologies, while 45% plan to adopt them. Halyk Bank and Kaspi Bank are regional pioneers, yet

their experience has not yet been widely replicated. In other countries of the region–Belarus, Armenia, Azerbaijan, Kyrgyzstan, Tajikistan, and Turkmenistan–the application of AI in financial monitoring remains at the stage of feasibility exploration and experimental pilot projects.

This regional lag creates a unique window of opportunity for banks prepared to adopt AI technologies promptly. In the context of low demand for AI-based financial monitoring solutions across the CIS, international technology providers–both large corporations (IBM, Microsoft, Oracle, SAS) and specialised vendors (FICO, Nice Actimize, Feedzai, ComplyAdvantage)–are offering significantly more favourable implementation terms than they will be able to offer in 3-5 years, once these technologies become a mainstream standard and demand rises sharply.

According to market expert estimates, the cost of implementing a comprehensive AI-based financial monitoring system in 2024 is 30-40% lower than the projected cost in 2027-2028. This is attributable to intensifying competition among vendors for market share in emerging markets, excess capacity among AI solution developers, and the willingness of technology companies to offer substantial discounts for reference projects in new regions. Within a few years, as demand increases, such conditions will no longer be available, and banks will be compelled to pay full market prices for standardised solutions.

The low competition for qualified data science and machine learning specialists in the CIS region makes the present moment optimal for team formation and the development of internal competencies. Banks that begin investing in building data science teams now can attract talented specialists with relatively modest salary expectations, offering them the opportunity to work on innovative projects. In 3-5 years, when AI deployment becomes a mass trend in the region, competition for such specialists will intensify sharply, and salary expectations will increase substantially.

Early adoption of AI technologies confers a material competitive advantage: higher operational efficiency and reduced compliance costs; superior quality of financial monitoring; an enhanced client experience through a reduction in erroneous transaction blocks; and a positive reputation as a technologically advanced financial institution. By the time competitors begin mass AI deployment in a few years, early movers will already possess years of practical experience, optimised processes, trained personnel, and accumulated data for continuous model refinement.

Federated Learning: Interbank Cooperation
Without Disclosing Client Data

One of the most promising directions in the application of artificial intelligence to financial monitoring is federated learning technology, which enables banks to jointly improve machine learning models without the need to share confidential client and transaction data. This technology represents a revolutionary approach to collective financial crime prevention while strictly adhering to requirements of confidentiality, banking secrecy, and personal data protection legislation.

The traditional approach to machine learning requires data centralisation: all training examples must be aggregated in a single location to train a model. In the banking context, this would entail transmitting detailed client transaction data, identification information, and behavioural profiles to a centralised repository–creating critical issues related to banking secrecy legislation, personal data protection laws, cybersecurity risks, and the competitive sensitivity of the information.

Federated learning addresses this problem through a decentralised approach. A central coordinator–which could be a central bank or an industry association–creates an initial version of the machine

learning model and distributes it to each participating bank. Each bank receives a copy of the model and trains it on its own local data, which never leaves its information system perimeter. Upon completion of local training, the bank transmits to the central coordinator not the source data, but only the model parameter updates. These updates are abstract mathematical values from which it is impossible to reconstruct specific transactions or client information.

The central coordinator receives parameter updates from all participating banks and aggregates them to produce an improved global model. The aggregation process typically involves a weighted averaging of updates. This improved global model is then redistributed to all participating banks for the next round of local training. The process repeats iteratively until the desired performance level is achieved.

It is critically important to understand that throughout the federated learning process, no participant in the system has access to another bank's data, nor can such data be reconstructed from the transmitted model parameters. For additional protection, differential privacy techniques may be applied– introducing carefully calibrated mathematical noise into the transmitted updates to provide mathematically provable privacy guarantees.

In exchange, each bank derives enormous benefit from the collective experience of the entire system. A model trained on aggregated patterns from multiple financial institutions is substantially more effective at detecting financial crimes than a model trained solely on a single bank's data. This arises from data diversity, the ability to capture schemes distributed across multiple banks, and the opportunity for smaller banks to achieve detection quality comparable to that of large institutions.

Experience from other jurisdictions demonstrates the viability of this approach. In Singapore, the Monetary Authority initiated a pilot project employing federated learning for money laundering detection, involving six of the country's largest banks. In the European Union, several bank consortia are experimenting with federated learning to improve financial monitoring systems in compliance with stringent GDPR requirements. Federated learning represents an opportunity to implement an innovative approach that is currently applied in only a limited number of jurisdictions, positioning early-adopter countries as leaders in the application of advanced technologies for financial crime prevention.

Conclusion

This study of international experience in implementing artificial intelligence technologies in anti-money laundering systems demonstrates that AI solutions are not merely an innovative option, but a critically necessary instrument for effective financial monitoring under contemporary conditions.

Analysis of the practices of leading global banks–HSBC, JPMorgan Chase, Standard Chartered, Deutsche Bank, and Citibank–has revealed specific measurable outcomes of AI technology implementation: a doubling in the number of detected suspicious transactions with a 20-50% reduction in false positives; a reduction in client verification time from days to minutes; a 25-35% increase in the detection of fraudulent applications; and a 50% reduction in fraud losses. These results are not theoretical projections–they represent the verified achievements of financial institutions that faced analogous challenges and successfully addressed them through the application of AI technologies.

A comparative analysis of AI adoption in the CIS banking sector has identified a substantial regional lag that paradoxically creates a unique window of opportunity. The advanced experience of Sberbank, which has integrated AI into 85% of its business processes with a financial impact of RUB 450 billion in 2024, demonstrates the potential for rapid scaling when a strategic approach is adopted. At the

current low level of regional adoption, solution costs are 30-40% below the projected cost in 3-5 years, combined with low competition for qualified specialists.

Federated learning technology opens revolutionary possibilities for collective financial crime prevention while strictly adhering to confidentiality requirements. Successful pilot projects in Singapore and the European Union demonstrate the viability of this approach and its potential for banking systems aspiring to technological leadership.

Key lessons from international experience encompass the necessity of a strategic approach with executive sponsorship; phased implementation beginning with pilot projects; substantial investment in developing internal competencies; meticulous integration with existing systems; and systematic results measurement to justify continued investment.

The window of opportunity created by the current low level of AI adoption in the CIS region is limited to 3-5 years. Banks that act promptly and decisively will secure lasting competitive advantages: higher operational efficiency, superior financial monitoring quality, an enhanced client experience, and a positive reputation as a technologically advanced financial institution. Those who delay risk finding themselves in a follower position with substantially higher costs and foregone opportunities.

Global AI investment in the financial sector is growing explosively, from USD 35 billion in 2023 to a projected USD 97 billion by 2027. Leading AI companies anticipate 60% higher revenue growth and 50% greater cost reductions by 2027 compared to lagging competitors. The moment for action is now.

References

1. Financial Action Task Force (FATF). https://www.fatf-gafi.org/en/home.html
2. Boston Consulting Group. AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value. October 2024.
3. Statista Research Department. (2024, August). Financial sector AI spending worldwide 2023-2024, with forecasts to 2028. Statista. https://www.statista. com/statistics/1446037/financial-sector-estimated-ai-spending-forecast/
4. The Astana Times. Nearly One-Third of Financial Market Participants Use AI in Kazakhstan. April 2024.
5. Klover.ai. Sberbank's AI Strategy: Analysis of Dominance in Banking AI. July 2025.
6. Sberbank Plans AI Technology Revenue of No Less Than RUB 450 Billion in 2025 [Electronic resource] // Interfax. 11.12.2024. https://www.interfax.ru /business/ 997224
7. Sberbank Has Implemented Artificial Intelligence in 85% of Processes [Electronic resource] // Banki.ru. 10.04.2024. https://www.banki.ru/news/lenta/?id=11001653
8. How Russian Software Enables Real-Time Fraud Monitoring [Electronic resource] // SberTech. 09.08.2024.
9. Sberbank Links 2025 Staff Reductions to AI Implementation [Electronic resource] // The Moscow Times. 28.10.2025.
10. Big Data and Machine Learning in Anti-Fraud Systems [Electronic resource] // BigDataSchool. 03.10.2021. https://www.bigdataschool.ru/blog/antifraud-cases.html
11. Artificial Intelligence in Banking: Enhancing Efficiency and Security [Electronic resource] // MWS. 10.07.2025. https://mws.ru/blog/iskusstvennyj-intellekt-dlya-bankov/
12. TAdviser. Artificial Intelligence in Banks. https://www.tadviser.ru/index.php/
13. Yang Q., Liu Y., Chen T., Tong Y. Federated Machine Learning: Concept and Applications // ACM

Transactions on Intelligent Systems and Technology. 2019. Vol. 10, No. 2. Article 12. 19 p.
14.AI for Fraud Detection and Suspicious Transaction Monitoring. https://www.udemy.com/course/ai-for-fraud-detection-and-suspicious-transaction-monitoring/