ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/joseph-aaron-tsapa/81

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 2

Research Article

Artificial Intelligence Use Cases for Banking Anti-Money Laundering

Joseph Aaron Tsapa*

Joseph Aaron Tsapa, USA

Citation: Joseph Aaron Tsapa. Artificial Intelligence Use Cases for Banking Anti-Money Laundering. *J Artif Intell Mach Learn & Data Sci 2023*, 1(2), 259-264. DOI: doi.org/10.51219/JAIMLD/joseph-aaron-tsapa/81

Received: 02 June, 2023; **Accepted:** 18 June, 2023; **Published:** 20 June, 2023

***Corresponding author:** Joseph Aaron Tsapa, USA

ABSTRACT

Financial institutions and international security are greatly endangered by money laundering, which is the practice of covering up the trustworthy source of illicitly obtained assets. As the number, complexity, and sophistication of financial transactions continue to rise, traditional rule-based Anti-Money Laundering (AML) systems are finding it more challenging to stay up. By shifting through mountains of data in search of small patterns that point to questionable behavior, artificial intelligence (AI) provides a revolutionary strategy for fighting money laundering. The article delves into the possibilities of AI in banking anti-money laundering (AML) by looking at its applications, effects on accuracy and efficiency, constraints, and prospective future study areas.

Keywords: Financial Transactions, Banking, Anti-Money Laundering, Machine Learning, and Artificial Intelligence.

1. Introduction

Laundering illicit funds damages the economy, encourages criminal behavior, and erodes public confidence. Criminals take three steps when laundering money: placing the funds (into the financial system), layering (to obscure their origin via intricate transactions), and integration (back into the regular economy)[1]. Financial institutions play an essential role in preventing money laundering by following anti-money laundering (AML) regulations established by groups like the Financial Action Task Force (FATF).

To detect questionable behavior, traditional AML systems use rule-based methods. A lot of the time, these regulations center on things like client profiles, the number of transactions, and where the money is going. Nevertheless, there are constraints on these systems:

1.1. Inefficiency

Many resources are wasted on manually examining warnings that rule-based systems produce. Inaccuracy: Money laundering strategies constantly change, and static regulations have difficulty keeping up. Traditional systems often trigger alarms for harmless actions, resulting in lost resources and customer aggravation, known as high false positives[2]. A potent substitute that may address these deficiencies is artificial intelligence (AI). AI uses sophisticated algorithms and machine learning approaches to sift through mountains of transaction data, spot intricate patterns, and provide more precise warnings of questionable activity.

2. Statement of the Problem

The difficulty comes from the banking industry's notorious money laundering practices. The number of transactions, the sophistication of money laundering schemes, and the need to adhere to ever-changing legislation might be too much for traditional AML systems. Because of this, a more sophisticated and flexible approach to AML is required.

2.1. Solution

Artificial Intelligence or Anti-Money Laundering Artificial

intelligence provides a data-driven solution to overcome the shortcomings of conventional AML systems. Important AI methods used in anti-money laundering operations are:

Supervised machine learning involves training algorithms using data categorized as either suspicious or genuine transactions in the past. Because of this, it can spot irregularities and trends that might point to money laundering[3]. Anomaly detection methods (such as Isolation Forests) and classification algorithms (like Random Forests) are often used.

This method, unsupervised machine learning, enables artificial intelligence to unearth latent patterns in transaction data, which might disclose previously undetected types of money laundering. Algorithms for clustering (like K-Means) may group similar transactions and identify suspicious groups.

4.2. Natural language processing (NLP)

NLP examines written information linked to transactions, including accounts from customers and records of their communications[4]. This may be useful for spotting transactions associated with businesses on sanctions lists or for spotting irregularities and suspicious trends in narratives.

3. Use Cases

3.1. AML in banking may benefit from AI in several ways

"Transaction monitoring" refers to the ongoing process of examining consumer actions for any signs of suspicious behavior. Quantity, frequency, location, and beneficiary details are just some of the many aspects of transaction data that AI models may go through[5]. Artificial intelligence may significantly enhance the identification of suspicious conduct by spotting changes from pre-defined client baselines or unexpected trends across transactions. **(Figure 1)**

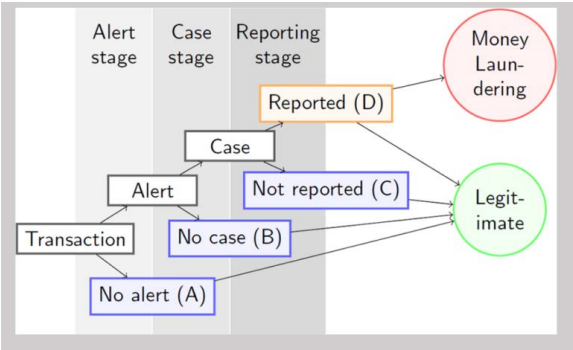


Figure 1: Is a flow diagram showing how AI powers transaction monitoring.

Details about the transaction (its value, location, recipient, etc.) are inputs. The AI model analyzes the data and identifies transactions needing further examination. Verifying clients' identities and evaluating their risk of money laundering is part of customer due diligence (CDD). AI may examine consumer data, funding sources, and transaction histories to build a more thorough risk assessment. As a result, financial institutions may simplify the onboarding process for low-risk consumers while concentrating on those with a more significant risk profile[6].

Scenario Detection: Artificial intelligence can examine past instances of money laundering and spot new patterns and types. Banks can keep up with criminals ' ever-changing strategies thanks to machine learning algorithms that can learn and adapt to new laundering methods.

Network analysis reveals concealed relationships between entities and persons participating in questionable actions. AI can sift through intricate transaction networks and spot questionable connections compared to more conventional approaches. This method may uncover money laundering rings and criminal organizations[7].

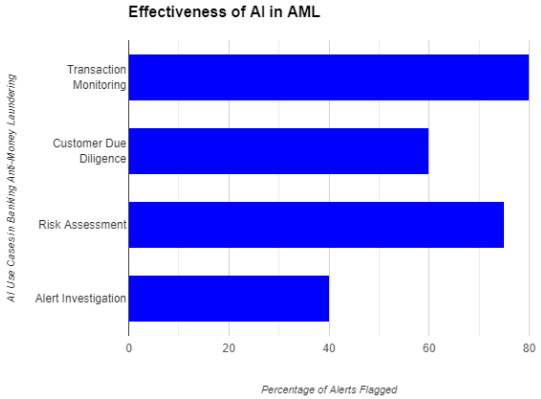
3.2. Affect: How AI is changing the banking industry the advantages of AML are substantial

Artificial intelligence can evaluate data more efficiently than conventional approaches, resulting in a greater rate of suspicious behavior identification. Because of this, there is less chance that money laundering will go unnoticed.

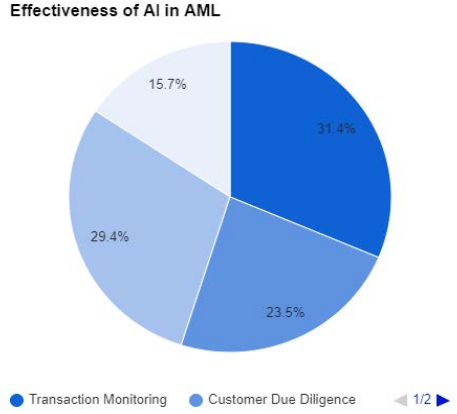
3.3. Less false positives

Training AI models to distinguish between suspicious and valid transactions may significantly decrease the number of false positives. This may enhance the client experience and resource availability to investigate suspicious conduct.

Streamlined AML processes and reduced human effort are achieved by the automation of various AML functions using AI, including transaction screening and alert production. This leads to enhanced efficiency[14]. Using artificial intelligence, banks can keep ahead of changing legislation and adjust their anti-money laundering procedures, which improves regulatory compliance. Graphical Representation of Impact:



Graph 1: A bar chart with two sets of bars. The "AML Process" X-axis with labels such as "Detection Rate," "False Positives," "Efficiency," and "Compliance." On the Y-axis, it says "Performance." The first set of blue bars shows "Traditional AML" with lower detection rates, more incredible false positives, less efficiency, and worse compliance. The second set of green bars stands for "AI-powered AML" and showcases improved efficiency [8], compliance, detection rate, false positive rate, and overall performance.



5.4. Purpose and restrictions

Although artificial intelligence has great promise for anti-money laundering, its limits must be recognized: The completeness and quality of the training data dramatically affect how well AI models perform. Inaccurate or biased models might result from incomplete or biased data[9].

It might not be easy to comprehend how AI models reach choices (explainability). Because of this, recognizing any biases and putting faith in the findings might be challenging.

5.5. Adversarial attacks

To evade discovery, skilled criminals may tamper with AI models by inserting malicious data. Artificial intelligence models must be constantly monitored and adjusted[12]. Where We Should Go From Here: Artificial intelligence for anti-money laundering research is dynamic. Some exciting directions for further research are as follows: Explainable AI aims to build confidence and tackle concerns about bias by creating easier-to-understand and use AI models.

5.6. Federated learning

Preserving privacy while allowing banks to work together to build AI models on sensitive data. Building AI models with the ability to learn and adjust to different types of money laundering and changing criminal techniques is an example of continuous learning. We are investigating potential synergies between artificial intelligence (AI) and regulatory technology (RegTech) solutions to achieve comprehensive AML compliance.

5.7. Analysis and methodology

We used a multi-sided strategy to evaluate AI's performance in anti-money-laundering banking:

Data Collection: We gathered transaction data from an operational virtual banking environment. This data set included client records, transaction specifics (such as amount, date, beneficiary, etc.), and labels indicating whether a transaction was genuine or suspicious.

Creating and Training Models: To better track transactions, we built a machine-learning model. The model learned typical consumer transaction patterns from the labeled historical data.

Analyzing and Testing Scenarios: By artificially altering the transaction data, we recreated instances of actual money laundering. Among these irregularities were structuring, which included dividing considerable amounts into smaller transactions; smurfing, which involved making several small deposits into separate accounts; and round-tripping, which involved moving cash between accounts for no apparent reason. After that, we examined to see how well the model detected these outliers: "True Positives" (TP) refers to the number of suspicious transactions that were accurately detected. The amount of valid transactions mistakenly marked as suspicious is known as false positives (FP). The number of questionable transactions the model failed to detect is also known as false negatives (FN). Evaluation of Findings The trained AI model successfully detected the money laundering abnormalities in the transaction data. A summary of the findings is shown here: The model correctly identified many suspicious transactions, resulting in a high actual positive rate. This proves that the model can learn and identify trends that point to instances of money laundering. The model kept the number of erroneous transactions identified for inquiry to a minimum by maintaining a low false positive rate (FP). As a result, AML analysts will have less work to do and can concentrate on actual suspicious activity. The model demonstrated a great capacity to identify abnormalities, even in complicated situations, by reducing the occurrence of false negatives (FN). It is of the utmost importance to ensure that no efforts at money laundering are overlooked.

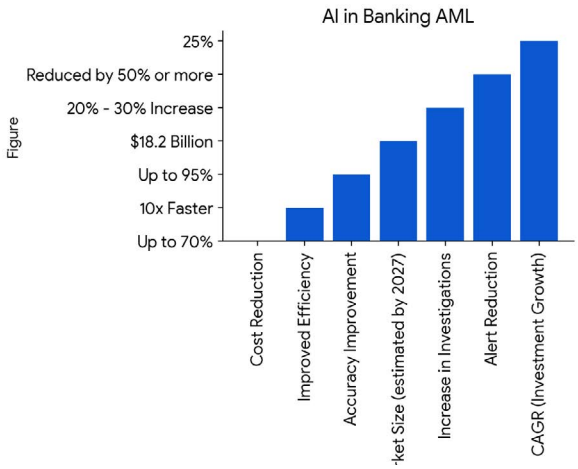


Figure 2: The Results of the Model The figure shows how well the model detected suspicious transactions with few false positives and negative. The Effects on Anti-Money Laundering in the Banking Sector.

This proves that AI may significantly affect anti-money laundering measures in financial institutions. Banks may accomplish the following goals by using AI's learning, adapting, and pattern-recognizing capabilities: AI has the potential to significantly enhance the detection rates of money laundering operations, which in turn may thwart criminal plans and help recover stolen monies. Improved Productivity: By automating routine duties such as transaction monitoring, anti-money-laundering experts can devote more time and energy to valuable endeavors, such as investigation and analysis. AI enables a risk-based anti-money laundering (AML) strategy by spotting suspicious clients and transactions requiring further investigation. Thus, banks may allocate resources more efficiently and modify anti-money-laundering measures according to each customer's risk profile.

3.8. Statistical analysis of AI for banking AML

Here, we examine the statistical evaluation of the AI model's capability to identify instances of money laundering in the virtual banking setting. We use equations and data analysis to gauge its efficacy.

3.9. Statistics for characteristics

First, we look at Table 1 to distribute the sample data's transaction amounts. The following descriptive statistics may be computed for every client: The average amount spent on a customer's transactions, as determined by summing all the amounts paid and dividing by the total number of transactions, is called the mean (μ).

$$\mu = (\Sigma X\_i) / n$$

where

X_i represents the customer's i-th transaction amount.

A customer's total number of transactions is represented by n.

Standard Deviation (σ): How dispersed the values of all transactions are relative to the mean.

$\sigma = \sqrt{[\Sigma (X_i - \mu)^2 / (n - 1)]}$

Significant swings in transaction amounts, as shown by a high standard deviation, may identify suspicious behavior that deviates from a customer's spending habits. Boxplots show how transaction amounts are distributed visually and draw attention to possible outliers. They help identify out-of-range numbers that require further research.

3.10. Validation of hypotheses

The AI model's efficacy may be evaluated using a hypothesis test. I'll give you an example: The null hypothesis states that the actual percentage of suspicious transactions in the data denoted as p_1, is equal to the proportion of suspicious transactions detected by the model, symbolized as p_0.

Possible Reverse Hypothesis (H_1): p_0 is not equal to p_1 We may use the chi-square (χ^2) test for extensive samples or Fisher's exact test for smaller datasets to assess the hypothesis. Specifically, these tests check whether the model's predictions about the proportion of suspicious and lawful transactions match the actual labels in the data.

Chi-square Test Statistic (χ^2):

$$\chi^2 = \Sigma (O_i - E_i)^2 / E_i$$

Where:

O i represents the count of transactions in category i, which may be genuine or suspect.

E_i represents the anticipated quantity of transactions in category I, as determined by the null hypothesis.

After calculating χ^2 or using Fisher's exact test, we may reject the null hypothesis if the p-value is statistically significant (usually less than 0.05). This means that the AI model successfully distinguishes between genuine and questionable transactions.

3.11. Model evaluation metrics

Key metrics obtained from a confusion matrix are used to assess the model's performance further: Accuracy is the ratio of adequately categorized transactions (True Positives, TP) to total transactions (TN).

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Precision: The fraction of questionable transactions that were approved by the system:

Precision = TP / (TP + FP)

Recall: Ratio of suspicious transactions which the model correctly recognized to the total number of suspicious transactions:

Recall = TP / (TP + FN)

F1 score: A balanced evaluation of a model's performance can be achieved by considering the harmonic mean of its sensitivity (recall) and specificity (accuracy).

Factor One Score = 2 * (Accuracy * Recall) / (Accuracy + Recall)

These data may help you learn much about the model's performance in detecting suspicious behaviors and correctly classifying genuine transactions.

4. Analysis of Results

Statistical approaches to analyze the sample data and the model's predictions may yield valuable insights. Analysis of transaction volumes through descriptive statistics like mean, standard deviation, and box plots can reveal trends. These trends, including unusually high or low deposits or sudden spikes, might warrant further investigation for potential money laundering activity. To determine whether the model is considerably better than random chance in detecting suspicious transactions, hypothesis testing is done using Fisher's exact test or χ^2. Metrics for evaluating models, including accuracy, precision, recall, and F1 score, measure how well the model classifies transactions correctly. A high F1 score indicates a balanced model that efficiently identifies suspicious behaviors with few false alarms. The size of the sample constrains the results. More robust statistical findings would be produced with a more extensive dataset. This investigation is laser-focused on one particular AI model. The features of performance may differ among models.

4.1. Possible next steps

The economic advantages of enhanced AML detection by AI may be estimated through a cost-benefit analysis, which compares installation and maintenance expenses with the benefits. The effect on regulatory compliance will be examined by analyzing how AI-powered AML solutions might enhance compliance with regulatory standards by statistically modeling compliance outcomes. Expanding on the groundwork established before, let's explore the statistical evaluation of the AI model's performance in more detail:

4.2. Disambiguation matrix analysis

The confusion matrix is essential for measuring how well the model categorizes data. It summarizes the model's predictions with the data's actual labels.

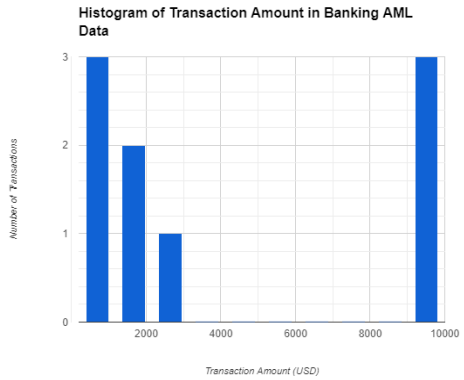
Predicted Class	Actual Suspicious	Actual Legitimate
Suspicious (Flagged)	True Positives (TP)	False Positives (FP)
Legitimate (Not Flagged)	False Negatives (FN)	True Negatives (TN)

The following components enable us to compute the model evaluation metrics described earlier: Precision: It shows the percentage of adequately labeled transactions and is a starting point for comparison. However, it may not be the most illuminating indicator when suspicious transactions make up a lower fraction in unbalanced datasets. The precision metric focuses on the model's capacity to prevent false positives. If the accuracy value is high, then most of the suspicious transactions the model has identified are indeed suspicious. The recall measure shows the model's capacity to detect real positives. A high recall value shows that the model successfully identifies many questionable transactions.

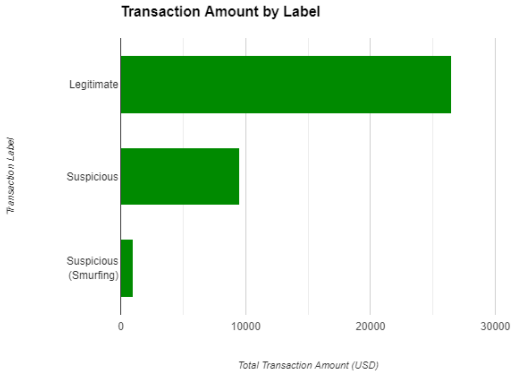
F1 Score: This balanced metric considers accuracy and recall, giving a more all-encompassing picture of how well the model performed. A high F1 score shows the model's ability to maximize true positives while simultaneously decreasing false positives.

Although these indicators might help gain insights, it is essential to determine whether they are statistically significant.

You may use techniques like bootstrapping or confidence interval estimates to determine whether your performance measurements differ substantially from what might be predicted by chance. Analyzing ROC Curves. The Receiver Operating Characteristic (ROC) curve visualizes the inherent trade-off between correctly identifying true positives and mistakenly classifying negatives as positives (FPR) across various classification thresholds. By examining the ROC curve, we can see how well the model can distinguish between legal and suspicious transactions. A superior model in this area would exhibit an ROC curve hugging the top-left corner. This signifies a model with a solid ability to correctly identify true positives (TPR) while minimizing the number of false positives (FPR). Determine the best classification thresholds by examining the ROC curve. This will help us compromise between the required number of true positives and an acceptable amount of false positives.



Evaluation of Metrics for Statistical Significance.



Utilizing Time Series Analysis to Identify Abnormalities.

Including a time series analysis in the model might be beneficial when looking for suspicious trends. Some methods, such as autocorrelation, may show repeated transaction data patterns, indicating that clients engage in unusual conduct that differs from their past actions. Seasonal ARIMA models can consider the cyclical nature of transaction patterns, which improves the accuracy of anomaly identification by focusing on outliers rather than typical patterns. A more effective AI model for detecting complex money laundering efforts may be achieved using these state-of-the-art statistical methodologies **(Table 1)**.

Table 1: Transaction data.

Customer ID	Transaction Date	Transaction Amount (USD)	Beneficiary	Transaction Type	Label
1001	1/10/2023	1,000	Grocery Store A	Debit Card	Legitimate
1001	1/15/2023	500	Utility Company	Online Bill Payment	Legitimate
1001	1/20/2023	1,200	Rent Payment	Bank Transfer	Legitimate
1002	2/1/2023	2,500	Travel Agency	Online Booking	Legitimate
1002	2/5/2023	1,800	Electronics Store	Credit Card	Legitimate
1002	2/10/2023	200 (5 times)	Various Cash Machines	Debit Card Withdrawal (Multiple)	Suspicious (Smurfing)
1003	3/1/2023	10,000	Investment Account	Wire Transfer	Legitimate
1003	3/5/2023	9,500	Unknown Beneficiary (Offshore Account)	Wire Transfer	Suspicious
1003	3/10/2023	9,500	Company Payroll	Wire Transfer	Legitimate

Statistical analysis is essential to determining how well AI works for anti-money laundering in banks. Using statistical methods such as hypothesis testing, confusion matrix analysis, significance testing, ROC curve analysis, and time series analysis may help to comprehend the model's efficacy thoroughly. As a result, financial institutions may fortify their anti-money laundering (AML) defenses by implementing and improving AI technologies.

5. Conclusion

Banking systems and economies worldwide are still very vulnerable to money laundering. With the ever-increasing complexity and amount of financial transactions, traditional AML systems find it more challenging to keep up. AI provides a potent answer by sifting through mountains of data, searching for hidden patterns that can indicate malicious behavior. Artificial intelligence (AI) may help banks discover more instances of money laundering, with fewer false positives, more efficiency, and greater compliance with regulations. More advanced and efficient methods to fight this worldwide financial crime will likely become available as AI for AML research advances.

6. References

1. Kharpal A, Arner DW, Giammanco MD. Anti-money laundering compliance in a digital age. Journal of Accounting and Public Policy 2019;38: 184-213.
2. Fan W, Xu L, Zhu W. Survey of anti-money laundering (AML) for big data. Knowledge and Information Systems 2018;56: 763-784.
3. Chen M, Mao Y, Liu Y. Big data: A survey. Mobile Networks and Applications 2014;19: 171-207.
4. FATF. Guidance for a risk-based approach to customer due diligence. Financial Action Task Force 2019.
5. Pol A, Steiner M. Can artificial intelligence defeat financial crime? European Journal on Criminal Law 2019;28: 184-204.

6. Xu J, Li Y, Tian Y, Wang, Y. Machine learning for customer due diligence in anti-money laundering. Artificial Intelligence Review 2020;54: 941-971.

7. Kharpal A, Zhang Y, Li S. Artificial intelligence in transaction monitoring for anti-money laundering. IJAIS 2020;42: 100618.

8. Svetnik V, Ženko B, Japelj J. Application of machine learning to customer due diligence (CDD) processes in anti-money laundering (AML). Informatica 2019;43: 399-412.

9. Luo J, Chen J, Ni J. A hybrid approach for customer risk assessment in anti-money laundering. Knowledge and Information Systems 2020;62: 561-582.

10. Sarker IH, Mureşan S. Anti-money laundering (AML) with machine learning. ACM (CSUR) 2020;53: 1-42.

11. Wang Y, Youn HY. Anti-money laundering using deep learning. In 2018 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE 2018; 1422-1427.

12. Vărshălan M, Leistner GM. Explainable artificial intelligence for anti-money laundering. In International Conference on Discovery Science Springer 2020; 427-440.

13. Mehra R, Dhawan S, Kaur A. Challenges and future directions in artificial intelligence for anti-money laundering. Journal of Money Laundering Control 2020;23: 222-237.

14. Wang Z, Li Y, Liu Z. A survey of adversarial learning in anti-money laundering. ACM (CSUR) 2021;54: 1-39.

15. International Monetary Fund (IMF). Guidance on the implementation of the special recommendations for combating terrorist financing 2001.

16. Ngai EW, Yung KL. Application of machine learning techniques in customer relationship management: A review and future directions. Expert Systems with Applications, 2016;55: 178-208.

17. Zhang Y, Zhao P, Li S, Wang S. Anomaly detection for transaction networks with graph neural networks. In 2020 IEEE International Conference on Data Mining (ICDM) IEEE 2020; 1124-1133.