emerald PUBLISHING

Journal of Money Laundering C

Improving client risk classification with machine learning to increase anti-money laundering detection efficiency

Journal:	*Journal of Money Laundering Control*
Manuscript ID	JMLC-03-2024-0040.R1
Manuscript Type:	Scholarly Article
Keywords:	Money Laundering, Client Risk Classification, Machine learning, Supervised Learning, XGBoost

Improving client risk classification with machine learning to increase anti-money laundering detection efficiency

Abstract

Purpose: This study describes and empirically explores a new method for bank anti-money laundering (AML) systems using machine learning models. Current automated money laundering detection systems are notorious for flagging many false positives, causing bank employees to spend unnecessary time manually checking transactions that do not constitute money laundering. Decreasing the number of false positives can free up resources for investigating money laundering.

Design/methodology: This study employs unique bank data on small- and medium-sized enterprises (SMEs) to examine how various client risk classification models can predict future suspicious transactions. We explore various sources of client risk data and machine learning approaches.

Findings: Client risk classification models can accurately predict suspicious future transactions. Adding accounting data and credit score information to client risk classification dramatically improves accuracy. This makes it easier to balance the risk of missing suspicious transactions with the need to reduce the number of false positives.

Originality/value: This study is the first to empirically explore machine learning in client risk classification, document how machine learning in client risk classification can significantly reduce false positives by incorporating novel, but readily available sources, such as credit risk and accounting data.

Practical implications: Our suggested approach with readily available data sources and a focus on classifying client risk in a dynamic model can help banks significantly improve their efficiency by targeting their AML efforts toward the riskiest clients.

Introduction

Machine learning is increasingly used to detect money laundering activities to potentially identify unusual financial behaviors and patterns (Alotibi *et al.*, 2022). However, the literature has limited research on this technique, indicating the need for further exploration in this area (Zhang and Trubey, 2019). With the increasing complexity and speed of banking transactions, classifying client risk has become increasingly important in anti-money laundering (AML) efforts. The lack of access to high-quality training datasets (Canhoto, 2021) and data quality issues are significant concerns leading to suboptimal machine learning models for money laundering detection (Gupta *et al.*, 2022). Additionally, machine learning models return false positives, emphasizing the importance of minimizing such errors to ensure accurate predictions (Ketenci *et al.*, 2021). Moreover, the use of machine learning algorithms to identify money laundering patterns and groups necessitates a critical review of techniques to enhance detection effectiveness (Kute *et al.*, 2021).

False positives in AML detection are a significant challenge. Ketenci *et al.* (2021) emphasize that most current financial institution systems are rule-based and ineffective, resulting in over 90% false positives. This high rate of false positives can lead to an overwhelming number of alerts that require manual review, consume valuable resources, and potentially cause genuine suspicious activities to be overlooked. This highlights the complexity of addressing false positives in AML detection, especially when considering the diverse nature of financial transactions, and underscores the potential for false positives in AML detection, where benign or legitimate financial activities may trigger alerts owing to similarities with illicit transactions. To address the problem of false positives, Alotibi *et al.* (2022) highlight the promising results of deep learning techniques for money laundering detection, which can decrease false positives compared with other classifiers. This suggests that advanced technological approaches may offer potential solutions for mitigating false positives in AML detection by improving the accuracy and efficiency of identifying suspicious activities.

The XGBoost and gradient boosting algorithms (Chen and Guestrin,2016), are scalable tree-boosting systems with demonstrated effectiveness in various machine learning tasks. In the AML domain, the application of XGBoost can provide robust and efficient methods for detecting and preventing money laundering activities, such as in detecting money laundering in cryptocurrencies (Vassallo *et al.*, 2021). Research is limited because of the lack of available data. However, these advanced machine learning techniques offer potential solutions for detecting and preventing money laundering activities.

In this study, we employ unique microdata from one bank in Norway to explore the possibilities and limitations of combining internal bank data with external sources. The dataset includes false positives and reported money laundering. Building on studies exploring machine learning in transaction monitoring (Jullum *et al.*, 2020) and the significance of different sources of information on money laundering (Ketenci *et al.*, 2021; Reite *et al.*, 2023), this study explores how access to information on credit risk, the use of banking products, and accounting information on small- and medium-sized enterprises (SMEs) increases the ability to predict whether a client will later be involved in a suspicious transaction.

Lokanan and Maddhesia (2023) identify regulatory filings received by the bank, products, and customers' relationships with the institutions as the most important features predicting suspicious activity report (SAR). We explore the importance of additional features available to banks. We explore machine learning models relying on only external information, models with banking information previously used in machine learning in AML (Jullum *et al*., 2020; Pettersson Ruiz and Angelis, 2021; Lablanca *et al*., 2022; Lokanan and Maddhesia, 2023), and on data for SMEs – a client group previously not explored.

Furthermore, we investigate how the efficiency of machine learning can be improved by classifying clients based on risk, thereby reducing false positives without losing true positives when such external sources are employed. This study is unique in that it is the first to incorporate the trade-off between not detecting all suspicious clients and minimizing false positives to reduce unnecessary costs or breaches of privacy when investigating a high number of clients not actually involved in money laundering. To the best of our knowledge, this is the first empirical study to employ machine learning for money laundering in SMEs.

This paper proceeds with an overview of AML regulations, and then describes data processing, methodology and framework before presenting and discussing our results. We conclude with the practical implications of our findings.

Anti-money laundering regulations

The Financial Action Task Force (FATF) is a crucial international organization combating money laundering and terrorist financing. The FATF provides recommendations and guidelines for countries and institutions to address the evolving trends in money laundering, expanding its coverage beyond drug trafficking and money laundering (Chitimira and

Munedzi, 2022). The FATF also emphasizes the importance of additional due diligence processes in banks to mitigate corruption risks and those of politically exposed persons (Naheem, 2018). The FATF's risk-based approach allows countries and institutions to promote financial inclusion while simultaneously addressing money laundering and terrorist financing (Koker, 2011). The FATF's AML recommendations are specific and comprehensive, encompassing a wide range of non-financial businesses and emphasizing high-risk areas such as customer due diligence and the establishment of cross-border correspondent banking relationships (FATF, 2018). Pol (2018) raises the question of whether the focus on compliance overshadows the primary policy objective of the FATF, to prevent financial crime.

This debate raises questions about the efficacy of the FATF's policy framework for combating money laundering and terrorist financing activities in member states, revealing both its achievements and obstacles (Nanyun and Nasiri, 2020). Machine learning is an important tool to increase the efficiency of AML efforts and the proportion of recovered criminal funds relative to the compliance costs (Pol, 2020).

AML regulations in Norway are in accordance with the FATF framework. According to the Anti-Money Laundering Act (2018), all banks must report suspicious transactions to The National Authority of Investigation and Prosecution of Economic and Environmental Crime (police). We divide banks' AML monitoring into three stages: alert, case, and reporting (Jullum *et al*., 2020). During the alert stage, all transactions pass through an automated AML system based on a set of rules. *Alerted* transactions then proceed to the case stage where they are manually checked to identify false positives. If suspicion cannot be ruled out after an investigation, suspicious transactions are reported to the police.

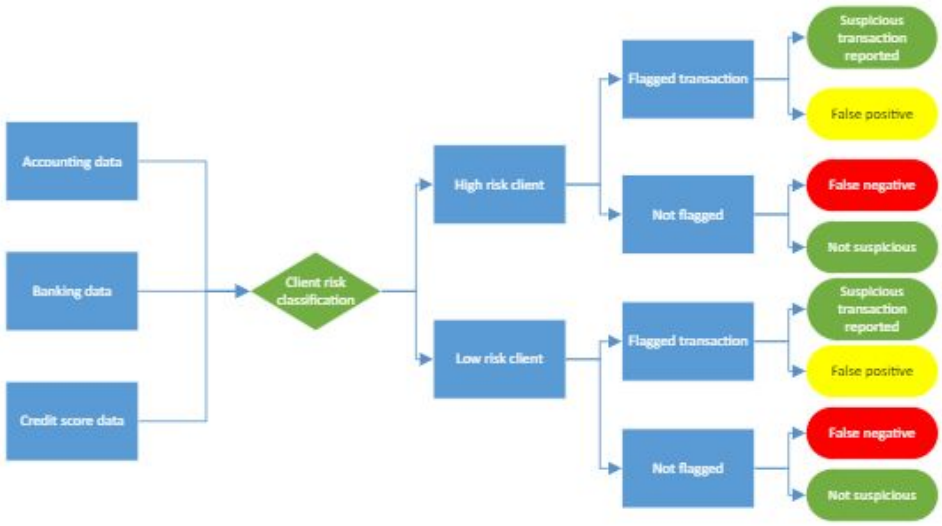

Figure 1: Client risk modeling and flagging.

However, the problem with current rule-based models is the number of false positives. According to Jullum *et al.* (2020), approximately 95–98% of alerted cases are expected to be non-suspicious after controls. Crucial to the effectiveness of an AML system and one methodological expansion of our approach is the integration of the transaction monitoring system with a dynamic client risk assessment model.

We hypothesize that classifying clients based on their characteristics makes it possible to predict whether a subsequent flagged transaction is a suspicious false positive. While a reported suspicious transaction may or may not represent money laundering, a bank will only rule out a flagged transaction as non-suspicious if it is certain after investigation. One novelty of our approach is that instead of optimizing machine learning for reported cases that may or may not actually represent money laundering, we focus on minimizing the number of transactions flagged and defined as non-suspicious after investigation, while not losing flagged transactions that were reported. Furthermore, we focus on client risk and whether client characteristics can predict subsequent suspicious transactions based on the client characteristics identified by Reite *et al.* (2023). While transaction monitoring-based approaches to AML can identify money laundering when it is performed and sometimes stop and prevent further money laundering, we propose that a client risk-based approach has advantages when it comes to stopping money laundering before it happens, because it enables stricter monitoring and countermeasures for certain clients.

Data processing, features, and cross-validation of the AML system

Rather than studying a transaction's amount, type, or recipient (transaction characteristics), our study focuses on the client characteristics such as credit score, bank use, products, and accounting information available before a suspicious transaction (Reite *et al.*, 2023). We then compare these characteristics with the alerted cases from the bank's AML system, transactions found not to be suspicious after manual investigation, and transactions not confirmed as false positives and thus reported to the police after this manual investigation. A *reported* transaction is defined as one that has been referred to or is under investigation by the police. We note here that the police do not report to the bank whether a suspicious transaction is linked to money laundering after their investigation. Thus, our approach defines reported cases as suspicious, and differs from a methodology focusing on predicting reported cases, which assumes that all reported cases represent money laundering.

Dataset

We collected a large data panel from BN Bank's small- and medium-sized business customers (SME) characteristics and transaction histories. The data cover February 28, 2021 to September 30, 2023. The set contains 500,767 observations; 9,831 were flagged as suspicious, underwent manual investigation, and were defined as false positives or reported if suspicion remained after the investigation. During the study, our focus turned to AML rule-based alerts because the primary aim was to develop a model dedicated to reducing the occurrence of false positives within specified risk parameters, particularly in the context of prevailing AML systems.

Independent variables

The dataset provides 48 usable features that can be categorized as bank internal, credit, and accounting data. In customer-bank relationships, the bank's internal data can be construed as numerical representations including facets such as total deposits, debt, accounts, and similar parameters. Such data can indicate the relationship between the customer and the bank. We saw this as convenient for two reasons. First, banks possess this type of information naturally. Second, it helps clarify how customers use banks.

Credit data are related to a customer's credit history, such as credit scores, default probabilities, and payment remarks. We expect changes in credit scores to be significantly and positively correlated with the likelihood of flagging and reporting (Reite *et al.*, 2023). Our accounting data describe key business figures such as equity percentage, operating revenue, and costs. These numbers are less sensitive because all joint-stock companies must publicly release accounting figures. Table I shows the independent variables along with their descriptions and measurements. We divide the three types of features into internal bank data describing bank and customer relations and customer size. Credit score indicates the customer's risk of default and accounting figures.

Table I: Overview of independent variables, N= 500,767

Variable	Median	Description	Type
Online Banking	41 %	Binary	Banking data
Bank Card	13 %	Binary	
No payment transactions in the Last 12 Months	37 %	Binary	
Total Deposits	81 %	Customer total deposit, measured in NOK	
Number of Deposit Accounts	1.44	Number of deposit accounts that the customer has in the bank	
Average Deposits in the Last 6 Months	805,000	Average total deposit the last 6 months (of clients with deposits)	
Total loans	10 %	Total NOK the customer has in debt	
Average loans to the bank in the Last 6 Months	52,000,000	Average debt last 6 months (of loan clients)	
Number of Immediate Payments in the Last Year	8.42	Average of clients using, 23% of observations	
Number of Foreign Payments in the Last 2 Years	16.33	Average of clients using, 8% of observations	
Total Foreign Payments in the Last 2 years	1,830,200	Average value in NOK of clients using	
Number of Foreign Payments in the Last Month	3.26	Number of foreign payments in the last month of clients using	
Total Foreign Payments in the Last Month	43,240	Average value in NOK of clients using	
Number of Foreign Payments to Risky Countries in the Last 2 Years	17.83	Payments to high-risk countries the last 2 years, 2.3% of observations	
Total Foreign Payments to Risky Countries in the Last 2 Years	8,630.00	Average value in NOK of clients using	
Number of Foreign Payments to Risky Countries in the Last Month	4.12	Payments to high-risk countries the last 2 years, 1.3% of observations	
Total Foreign Payments to Risky Countries in the Last Month	292,000	Total value in NOK	
Number of New Disbursements in the Last Month	1.61	Number of new disbursements last month, 3% of observations	
Probability of Default next 12 months	2.50 %	Credit score - available for 67% of observations - not on new entities	Credit score
Bad Creditscore Management or Board member	5.10 %	Of total observations	
Auditor Remarks	3.70 %	Of total observations	
Equity Percentage	7.6	Equity in percentage of its assets, 67% of observations	Accounting data
Total Operating Income per month	2,901,000	Monthly operating income, NOK, 67% of observations	
Total Inflows in the Last Month	677,317	Inflows to accounts, NOK, of clients with inflow	
Total Operating Costs Per Month	1,864,730	Total operating costs, NOK	
Total Payouts in the Last Month	465,959	Total outflows from accounts, NOK	
Rights Holder Foreign Citizen	4 %	Binary - beneficiary foreign citizen	
Rights Holder Foreign Residence	2 %	Binary, beneficiary foreign resident	
Rights Holder Taxable Abroad	6 %	Binary, beneficiary is taxable abroad	

We explore how additional data sources, such as accounting information and credit scores, can improve the machine learning models' predictions for SME clients. We compare the ability to predict the probability of a subsequent SAR with machine learning models based on novel data sources to a model using accounting, credit score, and banking data in one combined model. Furthermore, we examine the tradeoff between the loss of true positives and the reduction in false positives. We adopt this approach to determine whether client risk classification is a practical approach to a two-step approach to transaction monitoring and enable fine-tuning transaction monitoring rules to the inherent client risk level.

Methodology

To reduce the proportion of false positives and enhance the efficiency of the AML detection system, we focus on classifying clients based on the probability of a flagged transaction being defined as a false positive or reported after further investigation. For this purpose, we use the area under curve metric for the ROC curves to evaluate our models. This gives us a meaningful way of ranking the true positive to false positive ratio that our models will obtain at different thresholds, and has been used to evaluate AML models in the past (Jullum *et al.*, 2020).

The area under the ROC curve takes a value between 0 and 1, where 0.5 is equivalent to random guessing and 1 is equal to perfect prediction. It also does not require that our model be calibrated to a certain threshold for false or true positives.

Machine learning algorithms that can handle missing values

A challenge with our dataset is the missing values, some of which were caused by the absence of a product or transaction, and could be replaced by zero. This covers most internal bank data. Accounting figures with missing values are more difficult to interpret or correct. The law requires all JSCs to disclose their accounting figures. The exemption from this obligation for sole proprietorships may explain some of these observations. The lack of accounting feature values and data may also occur because the customer is only recently established.

The first model considers a gradient booster. These machine learning algorithms can handle missing values directly and often with performance equivalent to that of a human (Aydin and

Ozturk, 2021). Therefore, our primary model was XGBoost. The major benefit of the XGBoost model is that it can handle missing values without requiring imputation. When constructing decision trees, XGBoost treats missing values as distinct entities. It assigns a value of 0 where applicable, or classifies them according to the default direction at each node. The default direction is determined by selecting the direction with the maximum gain in the training set (Aydin and Ozturk, 2021). Previous studies demonstrate that impute-free XGB provides comparable accuracy to an imputed model (Aydin and Ozturk, 2021). Therefore, we believe that XGB is a robust choice for our dataset. To check the robustness of XGBoost, we also tested a model that replaces the NaN values with KNN imputation. The rankings of the models did not change when using the LGBM or gradient boosting.

Optimal thresholds

Our goal is to improve the banks' current AML systems. To stop money laundering, flagged transactions previously not confirmed as non-suspicious should not be present in clients defined as low risk in our client risk model. When the tolerance for false negatives is set to 0, creating a function in Python that takes a list of all thresholds output by the ROC curve and identifies the first index of a True Positive Rate (TPR) equal to 1, most of our models would not classify any observation as a false positive, and thus be completely passive. The trade-off between reducing false positives and losing suspicious transactions according to the existing AML rules is illustrated by the gradual reduction in true positives (false positive rate) in the reduced AUC curve. In this trade-off, a bank must consider that the suspicious transactions it reports are not necessarily money laundering. Furthermore, the bank can identify new money laundering by enhancing its monitoring of high risk clients and investigating client groups that the current AML system seemingly fails to address (Reite et al., 2023).
Multiple statistical tools can measure the optimal thresholds for binary classifiers which have room to tolerate false negatives, such as Youden's (1950) J-statistic and minimal distance (Perkins and Schisterman, 2006). The following formula calculates the Youden J-statistic:

$$J = Sensitivity + Specificity - 1$$

The following formula calculates the minimal distance:

$$\sqrt{(1 - Sensitivity)^2 + (Specificity - 1)^2}$$

Robustness tests

Cross-validation is a popular evaluation technique for machine learning models because of its robustness and because it uses an entire dataset (James *et al.*, 2023). It works by splitting the dataset into folds, each with its own training and test sets, and then performing training and prediction with a model for each fold. The predictions of each fold are then evaluated on a metric, and the mean of these predictions is the score on which we evaluate our model (James *et al.*, 2023).

Because positive money laundering cases are rare, and the data are split into very small folds, slight variations can make the variation in the target class across our folds prominent. Therefore, we use stratified cross-validation to ensure that each fold has an even number for each class. The Python library scikit-learn implements this method and has the option of not shuffling the data, which was used here to respect the time dimension. Our results proved to be robust through a stratified cross-validation. Through extensive tuning using the Python library Optuna, we found no significant improvement relative to the base settings of all gradient boosters.

Results and discussion

Reducing false positives employing only bank data

The classification methodology previously employed at BN Bank uses only banking data and data on client deposits and transactions in the bank. We see in Figure 2 that limiting the data available to a client within a bank can predict subsequent suspicious transactions. With a low tolerance for not detecting money laundering, the performance is suboptimal, and detecting more suspicious transactions comes at the price of many new false positives. It is also challenging to reduce false positives without losing suspicious cases, as the confusion matrices in Figure 3 illustrate. These predict that the majority of suspicious cases are not suspicious (122 of 155).

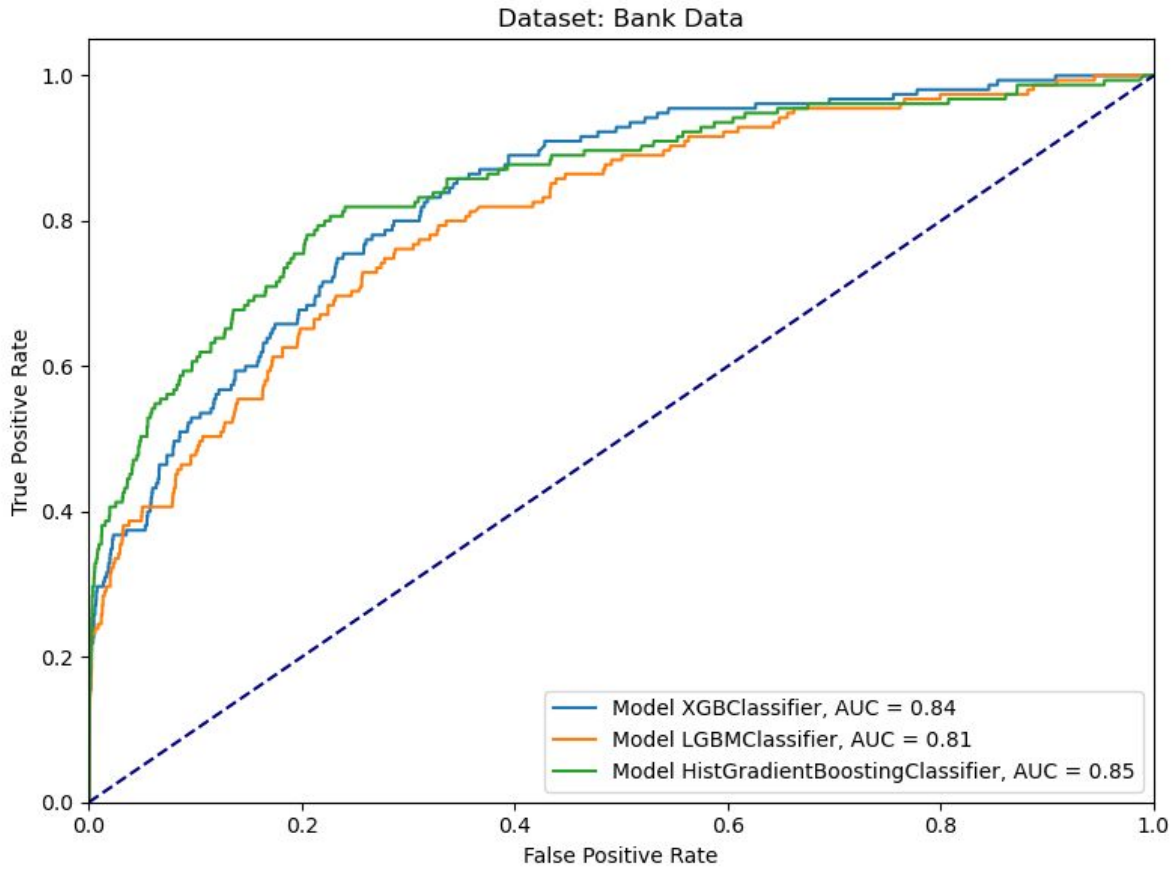

Figure 2: ROC curves from ML with only banking data.

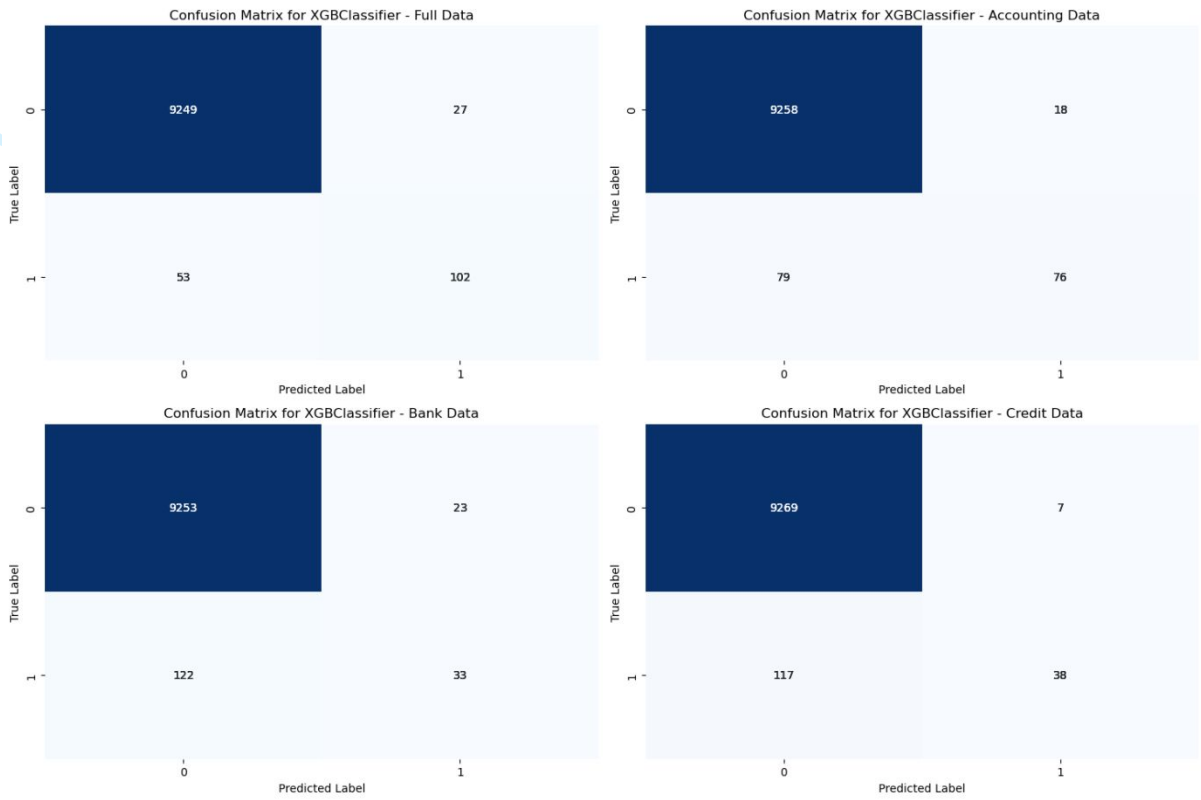

Figure 3: Confusion matrices.

Reducing false positives employing only credit score data

As illustrated in Figure 4 and Table II, we confirm the findings of earlier research that changes in credit score and credit score are significant in classifying SMEs into high-risk and low-risk money laundering (Reite *et al.*, 2023) and the importance of monitoring credit risk not only for corporate clients with credit exposure. An machine learning model based only on credit scoring can significantly reduce the proportion of false positives without losing true positives. We find from Table II that it outperformed a model based only on bank use data. Because credit score data are categorized into a limited number of categories, credit scores can change rapidly between categories when new information is available. Thus, the ROC curve displayed significant drops at the break points between the categories. Although there is a strong link between credit score changes and the risk of a subsequent suspicious transaction, one of the shortcomings of this model is the difficulty of linking this observed risk directly to client-specific changes relevant to client volume and bank use. Thus, the model provides little guidance on what to investigate and monitor besides a heightened overall suspicion level. One reason for the stepwise changes is the absence of scoring information for new companies. These companies are overrepresented in the flagged cases.

Interestingly, as shown in Figure 6, this model slightly outperformed the model based on banking data by wrongly predicting 117 of 155 suspicious cases.

Table II: Summary of all anti-money laundering models.

Model	Dataset	Mean AUC	AUC Std	Youden's J	Min Euclidean Distance	Youden's TPR/FPR	Min Distance TPR/FPR
XGB	Full Data	0.94	0.038	0.83	0.14	0.87/0.04	0.9/0.08
LGBM	Full Data	0.94	0.028	0.80	0.16	0.86/0.06	0.89/0.1
HistGradientBoosting	Full Data	0.94	0.038	0.84	0.13	0.88/0.04	0.89/0.06
XGB	Accounting Data	0.89	0.042	0.68	0.24	0.82/0.14	0.82/0.14
LGBM	Accounting Data	0.87	0.048	0.67	0.26	0.77/0.11	0.79/0.13
HistGradientBoosting	Accounting Data	0.91	0.049	0.74	0.20	0.88/0.13	0.85/0.12
XGB	Bank Data	0.84	0.040	0.58	0.31	0.81/0.23	0.8/0.22
LGBM	Bank Data	0.81	0.043	0.56	0.35	0.76/0.21	0.76/0.22
HistGradientBoosting	Bank Data	0.85	0.045	0.63	0.28	0.78/0.15	0.83/0.21
XGB	Credit Data	0.88	0.043	0.66	0.27	0.91/0.25	0.87/0.22
LGBM	Credit Data	0.86	0.042	0.65	0.27	0.91/0.26	0.87/0.22
HistGradientBoosting	Credit Data	0.87	0.043	0.65	0.28	0.91/0.26	0.87/0.23

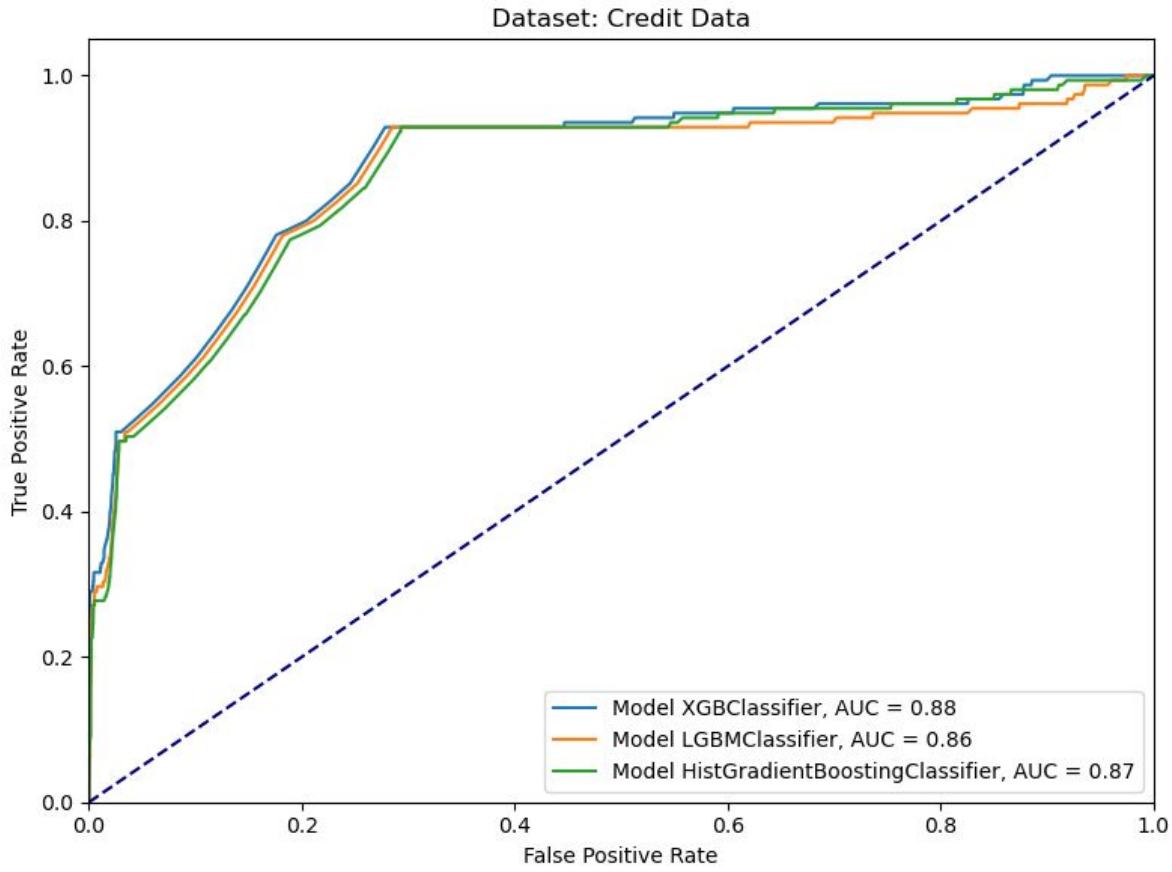

Figure 4: ROC curves from ML with only credit score data.

Reducing false positives employing only accounting data

In BN Bank's previous methodology, a client's risk classification was based on the volume of business and transactions. This is despite the fact that many risky corporate clients interact with several banks. If all banks in a market adopt this narrow perspective on client risk, a money launderer can bank with multiple banks and maintain a business volume below the thresholds for each bank's enhanced controls and volume-based transaction monitoring rules. Changing the client risk classification to employ accounting data instead of bank-specific data proved far superior to employing banking data alone, as illustrated in Figure 5 and Table II. This approach can be expanded based on transaction rules and risk classification by dividing observed data within a bank by the share of business volume of the corporate client within the bank. Banks should adopt stricter transaction monitoring rules for customers who bank with several banks, thus increasing the ability to identify clients who use several banks in an effort to launder money undetected. According to Figure 6, this model significantly outperforms the banking and credit score data models by correctly predicting 76 of the 155 suspicious transactions.

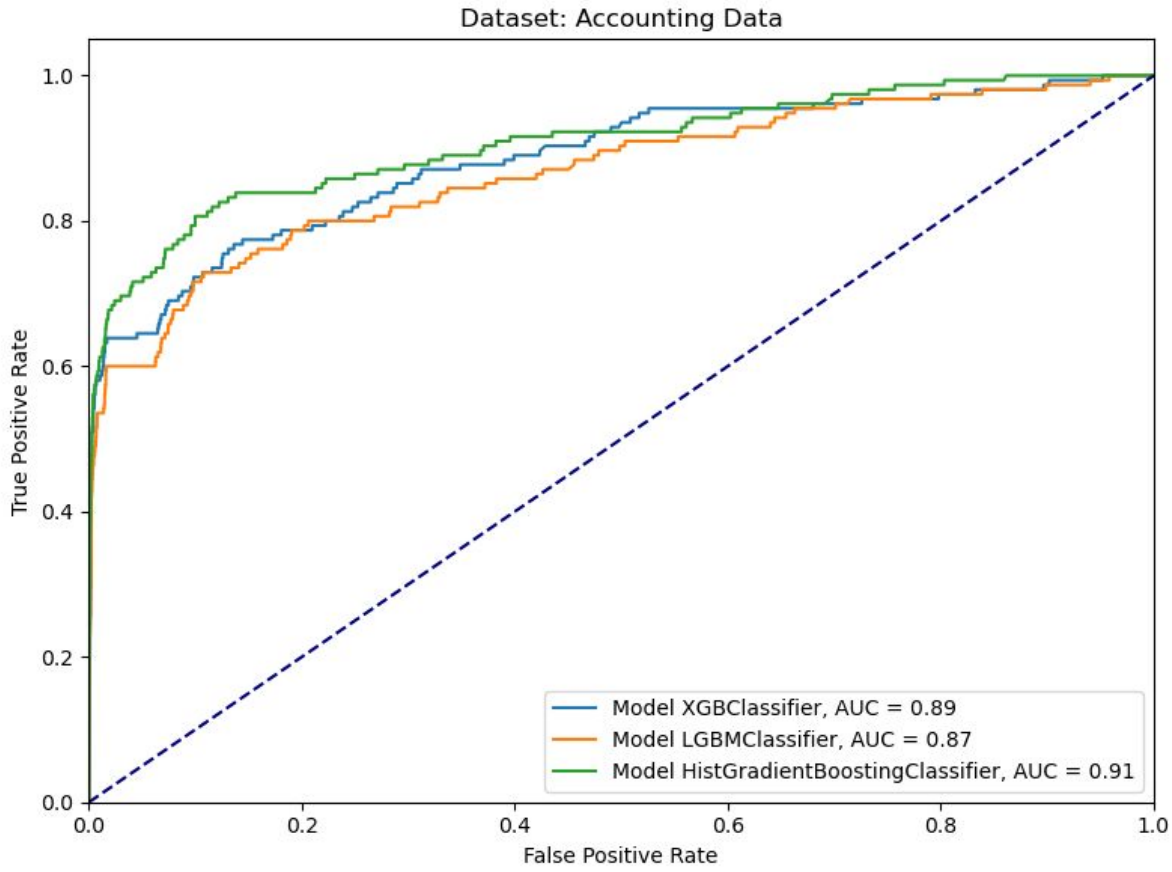

Figure 5: ROC curves from ML with only accounting data.

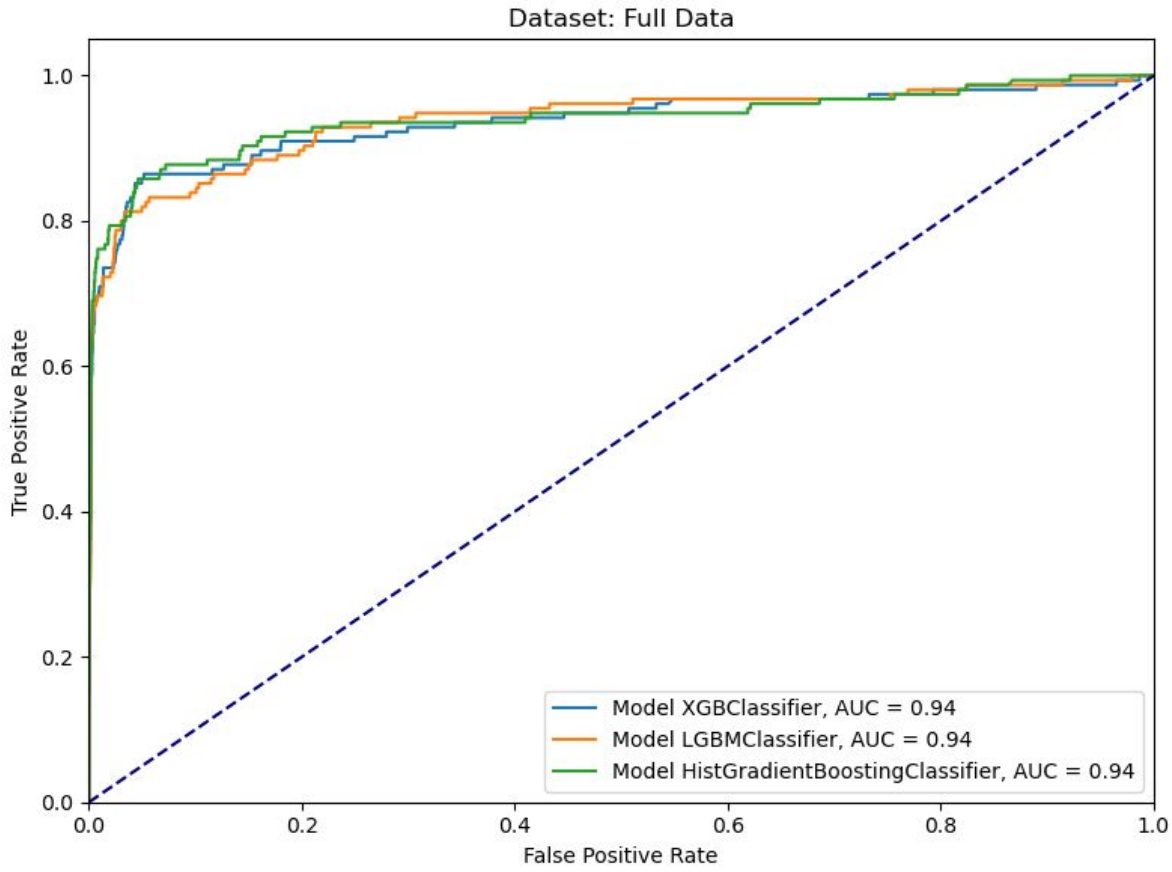

Figure 6: ROC curves from ML with only accounting data.

Combining different data sources to reduce false positives

The last model, where we enrich the banking data with both credit score data and accounting data, outperforms all the other models in Figure 6. In Table II, the combined model lifts the AUC to an excellent level. The model has an advantage over a pure credit score-based model in the link between products and the use of a bank, and in high- and low-risk clients. Furthermore, it considers the proportion of bank transactions by comparing transaction volumes with the firm's reported revenue. In terms of efficiency, our model enables differentiation between clients for whom subsequent flagged transactions are false positives and actual suspicious transactions at the same level of certainty as the transaction-based models in an earlier empirical study of banking transactions by Jullum *et al.* (2020). Figure 6 demonstrates that combining data sources also led to the correct prediction of 102 of 155 suspicious cases.

Conclusion

This study illustrates how client risk modeling with machine learning can predict which corporate clients subsequently have false-positive flagged transactions, thus enabling us to sort clients into high- and low-risk groups with different transaction monitoring rule thresholds and significantly reducing false positives. We find that a client risk classification-based approach can significantly reduce false positives, but with the risk of not detecting suspicious transactions.

Furthermore, our study illustrates how credit risk scores and changes in financial performance based on a firm's financial reports can help predict subsequent suspicious transactions. We find that combining these data sources with the product and banking information traditionally used (Jullum *et al*., 2020; Pettersson Ruiz and Angelis, 2021; Lablanca *et al*., 2022; Lokanan and Maddhesia, 2023) can improve a machine learning model.

A client risk classification model must include several data sources, including external data sources such as credit scoring and accounting data, as this approach outperforms banking data alone. Our models identify new and widely available data sources like financial accounts and credit scoring, but could also be improved by increasing the dataset, integrating new sources of data, and, more importantly, combining a dynamic and machine learning-based client risk classification model with different transaction monitoring rules. This approach would enable stricter thresholds for high-risk clients than for low-risk clients. Banks can also set thresholds and tolerance levels in a client risk classification model to benefit from the reduction in false positives at a minimal risk of losing suspicious transactions. Client risk classification-based approaches with the use of novel data sources can supplement transaction-based monitoring models and significantly improve the efficiency of AML efforts.

Research implications

We suggest a two-stage approach and focus on false positives as the dependent variable for further research, as it has support in related fields such as credit scoring (Kyeong and Shin, 2022). Employing a two-stage approach where clients are first subject to a client risk classification model before machine learning is employed to identify suspicious transactions provides privacy. Using personal data in AML efforts should be proportionate to the

probability of money laundering (Laurinaitis *et al*., 2021). With an improved and more granular client risk classification, a bank can document why certain client groups are subject to stricter scrutinization and lower thresholds for flagging. A transparent client risk classification and two-stage model can also reduce the risk of not detecting new patterns and the inherent risk of a machine-learning model detecting only previously detected patterns (Zhu *et al.*, 2021), as banks can direct their efforts to originally low-risk client groups that should have a higher risk assignment based on recent trends. Reite *et al.* (2023) highlight the potential bias in current AML efforts toward detecting suspicious transactions in mid-size clients. Another practical application of our findings is the false positive-false negative trade-off. Lokanan (2023) finds that money launderers try to use perceived weaknesses in controls by performing transactions early in the morning or late in the afternoon. A dynamic client risk classification model can impose additional controls on high-risk clients prior to a transaction, thus reducing the probability of not detecting money laundering when the capacity to control is lower.

While full reliance on our model comes at the cost of not detecting one-third of the suspicious transactions reported to date, the actual financial crimes not detected are uncertain, and the loss of potentially suspicious transactions must be weighed against the potential to reduce the number of false flagging by up to 95 percent. Reducing the number of false positives will free up more resources to conduct other AML activities and uncover additional financial crimes. Assigning a flagged transaction with the client risk classification of a client can provide a probability range of being a false positive. This can provide decision support and help prioritize the efforts in handling such flags. A similar approach can also be employed to adjust thresholds for flagging in the different client risk groups.

References

Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H. and Baz, A. (2022), "Money laundering detection using machine learning and deep learning", *International Journal of Advanced Computer Science and Applications*, Vol. 13 No. 10. https://doi.org/10.14569/IJACSA.2022.0131087.

Aydin, Z.E. and Ozturk, Z.K. (2021), "Performance analysis of XGBoost classifier with missing data", *Manchester Journal of Artificial Intelligence and Applied Sciences (MJAIAS)*, Vol. 2 No. 02.

Canhoto, A.I. (2021), "Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective", *Journal of Business Research*, Vol. 131, pp. 441-452. https://doi.org/10.1016/j.jbusres.2020.10.012.

Chen, T. and Guestrin, C. (2016), "Xgboost." Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining. https://doi.org/10.1145/2939672.2939785, 785-794.

Chitimira, H. and Munedzi, S. (2023), "Overview international best practices on customer due diligence and related anti-money laundering measures", *Journal of Money Laundering Control*, Vol. 26 No. 7, pp. 53-62. https://doi.org/10.1108/JMLC-07-2022-0102.

Financial Action Task Force (FATF) (2019), Guidance for a risk-based approach: The banking sector. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-banking-sector.html (accessed 01.01.2024)

Gupta, A., Dwivedi, D.N., Shah, J. and Jain, A. (2022), "Data quality issues leading to sub optimal machine learning for money laundering models", *Journal of Money Laundering Control*, Vol. 25 No. 3, pp. 551-555. https://doi.org/10.1108/JMLC-05-2021-0049.

James, G., Witten, D., Hastie, T., Tibshirani, R. and Taylor, J. (2023), *An introduction to statistical learning: With applications in python*, Springer Nature.

Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G. and Lorentzen, J. (2020), "Detecting money laundering transactions with machine learning", *Journal of Money Laundering Control*, Vol. 23 No. 1, pp. 173-186. https://doi.org/10.1108/JMLC-07-2019-0055.

Ketenci, U.G., Kurt, T., Önal, S., Erbil, C., Akturkoglu, S. and Ilhan, H.S. (2021), "A time-frequency based suspicious activity detection for anti-money laundering", *IEEE Access*, Vol. 9, pp. 59957-59967. https://doi.org/10.1109/ACCESS.2021.3072114.

Koker de, L. (2011), "Aligning anti-money laundering, combating of financing of terror and financial inclusion", *Journal of Financial Crime*, Vol. 18 No. 4, pp. 361-386. https://doi.org/10.1108/13590791111173704.

Kute, D.V., Pradhan, B., Shukla, N. and Alamri, A. (2021), "Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–A critical review", *IEEE Access*, Vol. 9, pp. 82300-82317. https://doi.org/10.1109/ACCESS.2021.3086230.

Kyeong, S. and Shin, J. (2022), "Two-stage credit scoring using Bayesian approach," *Journal of Big Data*, Vol. 9 No. 1. https://doi.org/10.1186/s40537-022-00665-5.

Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M. and Zanero, S. (2022), "Amaretto: An active learning framework for money laundering detection," *IEEE Access*, Vol. 10, pp. 41720-41739. https://doi.org/10.1109/ACCESS.2022.3167699.

Laurinaitis, M., Štitilis, D. and Verenius, E. (2021), "Implementation of the personal data minimization principle in financial institutions: Lithuania's case," *Journal of Money Laundering Control*, Vol. 24 No. 4, pp. 664-680. https://doi.org/10.1108/JMLC-11-2020-0128.

Lokanan, M. and Maddhesia, V. (2023). "Predicting suspicious money laundering transactions using machine learning algorithms." https://doi.org/10.21203/rs.3.rs-2530874/v1.

Lokanan, M.E. (2024), "Predicting money laundering using machine learning and artificial neural networks algorithms in banks," *Journal of Applied Security Research*, Vol. 19 No. 1, pp. 20-44. https://doi.org/10.1080/19361610.2022.2114744.

Naheem, M.A. (2018), "Illicit financial flows: HSBC case study", *Journal of Money Laundering Control*, Vol. 21 No. 2, pp. 231-246. https://doi.org/10.1108/JMLC-08-2015-0036.

Nanyun, N.M. and Nasiri, A. (2021), "Role of FATF on financial systems of countries: Successes and challenges", *Journal of Money Laundering Control*, Vol. 24 No. 2 No, pp. 234-245. https://doi.org/10.1108/JMLC-06-2020-0070.

Perkins, N.J. and Schisterman, E.F. (2005), "The Youden index and the optimal cut-point corrected for measurement error", *Biometrical Journal. Biometrische Zeitschrift*, Vol. 47 No. 4 No, pp. 428-441. https://doi.org/10.1002/bimj.200410133.

Pettersson Ruiz, E.P. and Angelis, J. (2021), "Combating money laundering with machine learning – Applicability of supervised-learning algorithms at cryptocurrency exchanges," *Journal of Money Laundering Control*, Vol. 25 No. 4, pp. 766-778.

Pol, R.F. (2018), "Anti-money laundering effectiveness: Assessing outcomes or ticking boxes?", *Journal of Money Laundering Control*, Vol. 21 No. 2 No, pp. 215-230. https://doi.org/10.1108/JMLC-07-2017-0029.

Pol, R.F. (2020), "Anti-money laundering: The world's least effective policy experiment? together, we can fix it," *Policy Design and Practice*, Vol. 3 No. 1, pp. 73-94. https://doi.org/10.1080/25741292.2020.1725366.

Reite, E.J., Oust, A., Bang, R.M. and Maurstad, S. (2023), "Changes in credit score, transaction volume, customer characteristics, and the probability of detecting suspicious transactions", *Journal of Money Laundering Control*, Vol. 26 No. 6, pp. 1165-1178. https://doi.org/10.1108/JMLC-06-2022-0087.

Vassallo, D., Vella, V. and Ellul, J. (2021), "Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies", *SN Computer Science*, Vol. 2 No. 3, p. 143. https://doi.org/10.1007/s42979-021-00558-z.

Youden, W.J. (1950), "Index for rating diagnostic tests", *Cancer*, Vol. 3 No. 1, pp. 32-35.

Zhang, Y. and Trubey, P. (2019), "Machine learning and sampling scheme: An empirical study of money laundering detection", *Computational Economics*, Vol. 54 No. 3, pp. 1043-1063. https://doi.org/10.1007/s10614-018-9864-z.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q. and Li, J.P. (2021), "Intelligent financial fraud detection practices in post-pandemic era," *Innovation*, Vol. 2 No. 4, p. 100176. https://doi.org/10.1016/j.xinn.2021.100176.