Internasional Journal of Integrative Sciences (IJIS)
Vol.5, No.10, 2026: 1273-1280

Early Detection of Fraud Indications in Ultra-Micro Financial Institutions Using Machine-Learning-based Financial Journal Data Analysis

Epa Yulaikha[1*], Stepani Sisca Wulandari[2]
Perbanas Institute
Corresponding Author: Epa Yulaikhan ; epa.yulaikha@gmail.com

A R T I C L E I N F O

Keywords: Fraud Detection, Fraud Triangle, Transaction-Level Data, Accounting Journal, Machine Learning, Early Warning System, Ultra Micro Financial Institutions.

Received : 2 August 2026
Revised : 16 September 2026
Accepted: 17 October 2026

©2026 Yulaikha, Wulandari : This is an open-access article distributed under the termsof the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

Ultra Micro Financial Institutions (UMFI) play an important role in expanding financial inclusion, but their high transaction volume, relatively small transaction values, direct cash handling, and limited internal control capacity may create fraud risks that are difficult to detect from aggregated financial statements. This study develops an early fraud-indication detection framework using transaction-level accounting journal data from PT Permodalan Nasional Madani (PNM), Magelang Branch. The study adopts a quantitative predictive case-study and proof-of-concept design. The available dataset covers 1 January to 31 March 2026 and contains 305,343 transactions from five units, 104 unique general-ledger codes, and balanced debit and credit totals of IDR 160,274,807,743. The novelty lies in translating the Fraud Triangle—pressure, opportunity, and rationalization—into operational transaction features, including end-period activity, transaction spikes, outliers, duplication, unusual account combinations, reversals, and correction-related descriptions. Rule-based screening is used only to identify risky candidates, while final fraud and non-fraud labels must be validated by internal audit. The analytical pipeline includes anonymization, leakage-aware preprocessing, feature engineering, train-validation-test splitting, SMOTE only within training data, Stratified 5-Fold Cross-Validation, hyperparameter tuning, Logistic Regression, Decision Tree, Random Forest, threshold selection, confusion-matrix evaluation, ROC-AUC, PR-AUC, and SHAP interpretation. At the time of article preparation, validated labels and final experiments were not yet available; therefore, model performance and the best-performing model are not reported. The article focuses on the methodological framework, theory-based feature design, and a risk-scoring early warning system for internal audit support

DOI: https://doi.org/10.55927/ijis.v5i10.78
E-ISSN: 2985-9050
https://journalijis.my.id/index.php/ijis/index

INTRODUCTION

Ultra Micro Financial Institutions (UMFI) have a strategic role in expanding access to financing for communities and very small businesses. Their operations are characterized by relatively small but frequent transactions, direct interaction with clients, and the need for fast and accurate recording. These characteristics make effective internal control important because control weaknesses may create opportunities for irregularities that are not necessarily visible in aggregated financial statements.

Fraud may involve misuse of cash, journal manipulation, misappropriation of installment payments, duplicate recording, or unsupported transaction corrections. In journal data, indications of irregularity may appear through unusual values, increased transaction frequency, unusual transaction times, specific account usage, duplication, reversals, or uncommon combinations of transaction attributes. However, an anomaly is not equivalent to fraud. An anomaly should be treated as a red flag or audit lead that requires further examination.

The development of data analytics and machine learning enables examination of a broader population of transactions. Debreceny and Gray (2010) demonstrated the potential of journal-entry data mining for fraud detection, while Abdallah et al. (2022) reviewed the broad application of machine learning in financial fraud detection. Nevertheless, machine-learning research in fraud detection needs to consider interpretability and its relationship with fraud theory so that model outputs can be meaningfully used by auditors and management.

This study uses the Fraud Triangle as its conceptual foundation, consisting of pressure, opportunity, and rationalization. The central challenge is translating these conceptual constructs into features that can be processed computationally. Accordingly, the study develops transaction-level feature engineering based on journal characteristics and connects these features with Logistic Regression, Decision Tree, and Random Forest. Model outputs are subsequently designed to support risk scoring and an early warning system for audit prioritization.

The research object is PT Permodalan Nasional Madani (PNM), Magelang Branch. The study is positioned as a case study, proof of concept, and model-development exercise; therefore, findings from one branch are not intended to be statistically generalized to all PNM branches or all UMFI. The main contribution is not a new algorithm, but a traceable bridge from the Fraud Triangle, transaction-level journal data, and feature engineering to predictive modelling, model interpretation, and audit-priority decisions.

LITERATURE REVIEW

Fraud in Ultra Micro Financial Institutions

Fraud refers to intentional actions undertaken to obtain benefits through irregularities, manipulation, asset misuse, or misleading information. In UMFI, high transaction frequency and close operational interaction with clients increase the need for risk-based monitoring. Internal control and internal audit are therefore important mechanisms for identifying irregularities at an early stage.

Fraud Triangle and Translation into Transaction Features

The Fraud Triangle explains fraud through pressure, opportunity, and rationalization. In this study, these elements are not assumed to be directly measurable as psychological conditions from journal data. Instead, each element is translated into operational proxies based on available transaction information.

Table 1. Fraud Triangle and Translation into Transaction Features

Fraud Triangle Element	Examples of Operational Features	Logic
Pressure	end_period_flag; transaction_spike; round_amount_flag	End-of-period activity, frequency spikes, or patterned amounts.
Opportunity	after_hours_flag; duplicate_flag; dormant_account_flag; unusual_account_pair	Transactions outside operating hours, duplication, dormant accounts, or unusual account combinations.
Rationalization	reversal_flag; correction_flag; description_keyword_flag	Reversals, corrections, cancellations, and characteristics of transaction narratives.

Financial Journals as Transaction-Level Data

Financial journals provide high granularity because each observation represents a transaction and retains attributes such as date, account, amount, unit, user-related information, and description. Numerical, categorical, textual, temporal, and account-relationship dimensions allow richer feature construction than analysis based solely on aggregated financial statements. Journal-entry analysis can therefore help auditors identify unusual transactions as audit leads.

Machine Learning and Explainable Artificial Intelligence

Supervised machine learning is planned after fraud and non-fraud labels have been validated. Logistic Regression serves as a relatively simple and interpretable baseline. Decision Tree provides traceable decision rules, while Random Forest is an ensemble of trees designed to capture nonlinear relationships and reduce dependence on a single tree. Feature importance and SHAP are planned to explain the contribution of features to risk scores.

Research Gap and Novelty

The research gap concerns the need for a more explicit integration between fraud theory and machine-learning analytics using transaction-level journal data in the UMFI context. The novelty of this study lies in translating the Fraud Triangle into transaction-level feature engineering, establishing an internal-audit-based ground-truth labeling procedure, preventing data leakage during preprocessing and validation, incorporating model interpretation, and translating model outputs into risk scoring and an early warning system.

METHODS

Research Design and Object

The study uses a quantitative predictive approach with a case-study and model-development design. The unit of analysis is a financial journal transaction at PT PNM Magelang Branch. Five units are included: KLDG, TMGG, BJEN, KDTM, and NGJO. The study is a proof of concept; empirical generalization requires replication across other branches or periods.

Database

Table 2. Database

Component	Actual Data
Period	1 January 2026–31 March 2026
Number of transactions	305,343 transactions
Units	5 units: KLDG, TMGG, BJEN, KDTM, NGJO
Unique account codes	104 GL codes
Initial columns	14 columns
Total debit and credit	IDR 160,274,807,743; balanced

The balance between total debit and credit indicates basic consistency of double-entry recording, but it does not prove that all transactions are free from fraud because manipulation may still occur within balanced journal entries.

Labeling and Preprocessing

Rule-based anomaly detection is used to screen transactions for risk candidates, not to establish fraud ground truth. Candidate transactions are subsequently intended to be validated by internal auditors or authorized company personnel. Sensitive identities are anonymized through masking or hashing. Preprocessing includes handling missing values, duplicates, outliers, categorical encoding, construction of time- and amount-based features, and data reconciliation.

To prevent data leakage, the train-validation-test split is performed before processes that learn from the data. SMOTE is applied only to training data and within training folds during cross-validation. Evaluation is designed using Stratified 5-Fold Cross-Validation, hyperparameter tuning, threshold selection, and testing on data not used for model learning.

Modelling and Evaluation

Three models are planned for comparison: Logistic Regression, Decision Tree, and Random Forest. Evaluation metrics include precision, recall, F1-score, ROC-AUC, PR-AUC, and confusion matrix. Because fraud is generally a minority class, PR-AUC and recall are important alongside other performance measures. The threshold is to be selected using validation data and audit examination capacity rather than relying solely on the default classification threshold.

Interpretation and Early Warning System

Feature importance and SHAP are planned to explain feature contributions. Predictions are then intended to be translated into risk scores and risk categories. The proposed operational scenario is for auditors to review transactions with the highest scores, for example the top 5% or top 10%, depending on examination capacity. Business usefulness can be evaluated through top-k precision, audit-finding recall, reduction in the number of transactions requiring manual review, and screening time saved.

Ethics and Confidentiality

Company data are treated as sensitive information. Client and staff identities are not presented in the article. Publication is directed toward aggregate information, model metrics, and non-identifying examples of transaction patterns. Research implementation should comply with access restrictions, secure storage, company approval, and applicable confidentiality requirements.

RESULTS

Findings Supported by the Available Dataset

The available dataset contains 305,343 transactions over three months across five units and 104 unique account codes. The data volume indicates a need for data-based screening mechanisms because manual examination of the entire transaction population requires substantial resources. The dataset also contains temporal, account, amount, unit, batch, and description dimensions that can be used for feature engineering.

At the analytical-design stage, candidate anomaly patterns include value, frequency, time, account, user-behavior, duplication, reversal/correction, and transaction-splitting anomalies. These patterns are treated as red flags. The study explicitly does not conclude that a transaction is fraudulent merely because it satisfies a rule or receives an anomaly score.

Translation of the Fraud Triangle

Pressure is represented primarily through end-period indicators and activity spikes; opportunity through transactions outside operating hours, duplicates, dormant accounts, and unusual account pairs; and rationalization through reversals, corrections, cancellations, and narrative keywords. These features are operational proxies rather than direct evidence of an individual's psychological condition.

Status of Machine-Learning Experiments

At the time of article preparation, the dataset did not yet contain final validated fraud and non-fraud labels. Consequently, Logistic Regression, Decision Tree, and Random Forest cannot yet be legitimately trained and compared as final fraud-classification models. Confusion matrices, ROC-AUC, PR-AUC, SHAP outputs, optimal thresholds, and the best-performing model are

therefore not reported. Reporting numerical performance at this stage would produce claims unsupported by the available research evidence.

Table 3. Status of Machine-Learning Experiments

Component	Status	Next Action
Dataset profile	Available	Verify after preprocessing
Rule screening	Designed	Run and retain screening logs
Audit labeling	Not yet available	Validate with internal audit
Logistic Regression, Decision Tree, Random Forest	Cannot yet be legitimately trained	Train after final labels
Testing evaluation	Not yet available	Complete after experiments
SHAP	Not yet available	Run for selected model
Top-k/business evaluation	Not yet available	Calibrate to audit capacity

Managerial Implications

The framework supports a shift from predominantly manual or sampling-based examination toward risk-based prioritization. Auditors are not replaced by the model; rather, the model functions as a decision-support tool to narrow the transaction population into a prioritized review list. For management, information about risk-driving features can support evaluation of control weaknesses. For data managers, the availability of transaction IDs, complete timestamps, anonymized user IDs, change histories, and structured audit outcomes is important for sustainable system development.

Limitations

The main limitation is the absence of validated fraud/non-fraud labels, which means that predictive-model results cannot yet be reported. In addition, several features require confirmation of standard operating procedure parameters, such as operating hours and transaction-splitting thresholds. The relationship between anomalies and fraud may also be affected by operational context that is not fully recorded in journal data. Therefore, document examination and professional judgment remain necessary.

CONCLUSIONS AND RECOMMENDATIONS

This study develops an early fraud-indication detection framework for UMFI based on transaction-level journal data by integrating the Fraud Triangle, feature engineering, machine learning, explainable artificial intelligence, and an early warning system. The available dataset consists of 305,343 transactions, five units, 104 unique account codes, and the period from 1 January to 31 March 2026, with balanced debit and credit totals of IDR 160,274,807,743.

The Fraud Triangle can be operationalized through transaction-level feature proxies: pressure through end-period indicators and activity spikes; opportunity through outliers, duplicates, dormant accounts, and unusual account pairs; and rationalization through reversals, corrections, cancellations,

and narrative characteristics. Rule-based screening serves only to generate candidates and cannot be treated as the sole ground truth.

The main contribution of the article is a methodological framework connecting fraud theory with predictive modelling and management monitoring needs. However, conclusions regarding model performance, the most influential features, threshold selection, and the best model must await completion of label validation and final experiments. After that stage, model outputs can be calibrated into risk scoring and an early warning mechanism aligned with audit capacity.

Recommendations

Future research should complete internal-audit label validation, execute the documented preprocessing and experimental pipeline, compare the three models on held-out testing data, select thresholds according to audit requirements, conduct SHAP analysis, and evaluate top-k performance. After the proof of concept is completed, external validation across other branches or periods and model-drift monitoring should be conducted to assess empirical generalizability.

FURTHER STUDY

This study still has limitations, so further research on Early Detection of Fraud Indications in Ultra-Micro Financial Institutions Using Machine-Learning-based Financial Journal Data Analysis is needed to refine this study and enhance the insights of readers and the authors

REFERENCES

Abdallah, A., Maarof, M. A., & Zainal, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637

Bao, Y., Ke, B., Li, B., Yu, Y. J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. Journal of Accounting Research, 58(1), 199–235. https://doi.org/10.1111/1475-679X.12292

Bakumenko, A., & Elragal, A. (2022). Detecting anomalies in financial data using machine learning algorithms. Systems, 10(5).

Beneish, M. D. (1999). The detection of earnings manipulation. Financial Analysts Journal, 55(5), 24–36. https://doi.org/10.2469/faj.v55.n5.2296

Debreceny, R. S., & Gray, G. L. (2010). Data mining journal entries for fraud detection: An exploratory study. International Journal of Accounting Information Systems, 11(3), 157–181. https://doi.org/10.1016/j.accinf.2010.08.001

Fay, R., & Negangard, E. M. (2017). Manual journal entry testing: Data analytics and the risk of fraud. Journal of Accounting Education.

Gassama, S., & Sudaryati, E. (2022). The role of internal audit quality to the sustainability and success of microfinance program. Manajemen Bisnis, 12(1), 45–51. https://doi.org/10.22219/mb.v12i01.15642

Gepp, A., & Kumar, K. (2024). Taking the hunch out of the crunch: A framework to improve variable selection in models to detect financial statement fraud. Accounting & Finance, 64(2), 1569–1588. https://doi.org/10.1111/acfi.13192

Hamdani, R., & Albar, A. R. (2016). Internal controls in fraud prevention effort: A case study. Jurnal Akuntansi dan Auditing Indonesia, 20(2), 127–135. https://doi.org/10.20885/jaai.vol20.iss2.art5

Lin, K., & Gao, Y. (2022). Model interpretability of financial fraud detection by group SHAP. Expert Systems with Applications, 210, 118354. https://doi.org/10.1016/j.eswa.2022.118354