Online-Journals.org

iTDAF IETI Transactions on Data Analysis and Forecasting

iTDAF | eISSN: 2959-0442 | Vol. 4 No. 1 (2026) | OPEN ACCESS

https://doi.org/10.3991/itdaf.v4i1.59227

SHORT PAPER

Research on the Risk Early Warning Model for Money Laundering Transactions in Bank Accounts

Yunfei Li[1] (✉), Davron Aslonqulovich Juraev[1], Moawia Alghalith[2], Anastasia Kiritsi[3]

[1]Turon University, Karshi, Uzbekistan

[2]UWI, St Augustine, Trinidad and Tobago

[3]International School of Management, Berlin, Germany

11580718@qq.com

ABSTRACT

This paper focuses on the research of the risk early warning model for money laundering transactions in bank accounts, aiming to assist banking and financial institutions in combating money laundering crimes and meeting regulatory requirements. Bank accounts are a key penetration vector for criminals to conduct money laundering activities. The risk early warning model discussed in this paper can be constructed from transaction dimension, customer dimension, and multi-dimensional integration through the data layer, technology layer, and application layer so as to achieve the goal of anti-money laundering and maintain the security of the financial system.

KEYWORDS

bank accounts, money laundering transactions, risk early warning, model research

1 INTRODUCTION

Bank accounts are the core carriers for the capital flow of enterprises and individuals, and also the key targets exploited by criminals to conduct money laundering activities. Most small and medium-sized banks rely mostly on manual work for their anti-money laundering efforts, which is time-consuming and labor-intensive. Therefore, the development of a risk early warning model for money laundering transactions is a critical requirement for banks to combat money laundering crimes [1]. Banks' risk early warning models are generally constructed based on the process of "capital flow – transaction behavior – risk characteristics." By integrating multi-dimensional information such as account transaction data, customer identity information (Know Your Customer, KYC), and external risk lists, these models identify abnormal transactions that "seem normal but are actually money laundering." Such transactions are usually disguised through methods like fund splitting, fake transactions, and cross-border transfers. Therefore, blocking the money laundering fund chain in advance, which complies with the anti-money laundering requirements of regulatory authorities, is a top priority for banks [2].

Li, Y., Juraev, D. A., Alghalith, M., Kiritsi, A. (2026). Research on the Risk Early Warning Model for Money Laundering Transactions in Bank Accounts. *IETI Transactions on Data Analysis and Forecasting (iTDAF)*, 4(1), pp. 66–73. https://doi.org/10.3991/itdaf.v4i1.59227

Article submitted 2025-10-15. Revision uploaded 2025-12-03. Final acceptance 2025-12-03.

2 CORE CHARACTERISTICS OF MONEY LAUNDERING TRANSACTIONS IN BANK ACCOUNTS

The essence of money laundering activities is to disguise illegal funds as legal funds. The account transactions involved typically exhibit three core characteristics: deviation from normal business logic, evasion of regulatory monitoring, and serving specific criminal scenarios. These characteristics also serve as the core design basis for the early warning model [3].

Typical money laundering transactions generally show three types of abnormalities:

1. Abnormal transaction patterns: Manifested as small-amount and high-frequency transactions with fund splitting; rapid inflow and outflow of funds with little or no remaining balance; and scattered and unconnected transaction counterparties.
2. Abnormal fund flow directions: Manifested as funds flowing into high-risk areas (e.g., gambling- or fraud-related platforms, cross-border underground banks, and accounts of shell companies); concentrated inflow and scattered outflow of funds (or vice versa); and cross-border transactions without real trade backgrounds.
3. Mismatch between customers and transactions: Manifested as inconsistency between the scale of account transactions and customer identity; inconsistency between transaction types and the customer's main business; and false customer identity information [4].

3 DESIGN OF THE RISK EARLY WARNING MODEL

3.1 Design logics followed by the early warning model

The design of the model adheres to logic such as industry stratification, transaction lifecycle, and risk scenario mapping.

Customer stratification logic: Based on KYC information, customers are divided into different risk levels ("high," "medium," and "low"). For example, individual customers are classified by factors such as occupation and income, while corporate customers are categorized by factors such as enterprise scale and industry attributes. Differentiated monitoring thresholds are applied according to the corresponding risk levels.

Transaction lifecycle logic: The entire lifecycle of an account covers the full process of "account opening—transaction—account cancellation." Banks need to monitor abnormal account opening behaviors during the account opening phase; abnormal fund flows of the account during the transaction phase; and abnormal transactions (e.g., large-value transfers) before account cancellation during the account cancellation phase.

Risk scenario mapping logic: Banks need to convert common money laundering scenarios into quantifiable transaction characteristics. For instance, money laundering related to drugs is often accompanied by intensive cash transactions and fund flows to drug-related areas; cross-border money laundering is usually associated with fake trade documents and fund transfers through offshore accounts [5–8].

3.2 Construction of the risk early warning model

The system can address different types of money laundering risks by monitoring the transaction dimension, customer dimension, and multi-dimensional integration [7], as shown in Tables 1 to 3.

Table 1. Example of the transaction-dimension early warning model

Data Dimension	Key Information	Correlation Logic
Amount-related	Frequent or large-value transactions occurring in a personal account after small-value exploratory transactions	Number of transactions ≥30 Number of Small-value transactions ≤10 Cumulative transaction amount ≥50,000
	Scattered inflows and scattered outflows of funds	Cumulative amount ≥10,000,000 Number of counterparty accounts ≥200 Number of provinces where counterparties are located ≥5 Outflow ratio: 0.9~1.1 Number of outflow transactions ≥100 Number of inflow transactions ≥100
Frequency-related	Fund flows of the account involving multiple regions	Number of transactions ≥30 Number of regions involved ≥5 Cumulative transaction amount ≥500,000
	A large number of downstream counterparties, covering various parts of the country	Number of regions where outflow counterparties are located ≥4 Number of outflow counterparty accounts ≥10 Cumulative inflow amount to corporate accounts ≥500,000 Cumulative inflow amount to personal accounts ≥100,000
Time-related	Frequent transactions conducted by the customer late at night or in the early morning	Total number of transactions ≥50 Proportion of early-morning transactions ≥25% Early morning: ≤5:00 (24-hour format) Late night: ≥23:00 (24-hour format)
	Rapid inflow and outflow of funds in a personal account, frequent large-value transactions, and little or no balance remaining on the day	Daily cumulative inflow amount ≥500,000 Number of transaction days ≥5 Account balance/Cumulative inflow amount ≤0.1

Table 2. Example of the customer-dimension early warning model

Data Dimension	Key Information	Correlation Logic
Identity-Transaction Matching Degree	Multiple personal accounts share the same IP address, MAC address, mobile phone number, and device information for online transactions	Number of accounts ≥5
	Personal customer identity information does not match their actual transaction scale	Cumulative transaction amount ≥1,000,000 Age ≥65 Age ≤18 Annual income ≤50,000 Occupation = Freelancer
Customer Risk Level Correlation	Excessively high frequency and amount of salary payments made by human resource companies	Number of counterparties' occupations ≥10 Number of transactions with the same counterparty ≥2 Total number of counterparties ≥10 Counterparties' age ≥50
	Personal customers frequently open and close accounts	Number of account opening and closing ≥5 Review period <90 days

Table 3. Example of the multi-dimensional integration early warning model

Data Dimension	Key Information	Correlation Logic
Transaction Data	Counterparty account's industry, region, and transaction frequency	Most counterparties are "shell companies" or "accounts in gambling-related regions," which may be money laundering fund pools
Customer Data	Enterprise's main business, registered capital, and shareholder background	Enterprises with low registered capital and no actual business premises that conduct frequent large-value transfers may be "money laundering shell companies"
External Data	Industrial and commercial deregistration information, fraud-related lists, and credit overdue records	Accounts of deregistered enterprises that are still in use, or accounts associated with fraud-related lists, pose extremely high risks
Business Data	Trade contracts, customs declarations, and invoices	Inconsistency between the contract amount and the transfer amount, or large-value cross-border "payment for goods" without a customs declaration, may indicate fake trade

4 KEY STAGES OF MODEL APPLICATION AND PRACTICAL CHALLENGES

4.1 Core process of model application

The deployment of the risk early warning system can separate the application server from the database server, thereby improving processing efficiency. Small and medium-sized financial institutions can adopt the Spring Boot + VUE architecture for deployment, which is simple and efficient. For data storage and backup, NAS (Network-Attached Storage) can be used, and redundancy can be provided through RAID (Redundant Array of Independent Disks) to ensure data security. The architecture is shown in Figure 1.

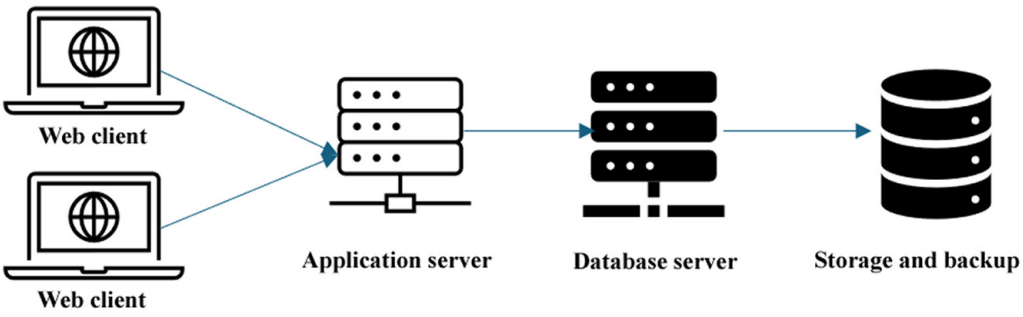

Fig. 1. Deployment architecture of the risk early warning system

The early warning model for money laundering transaction risks adopts a three-layer architecture: Data Layer, Technology Layer, and Application Layer, as shown in Figure 2.

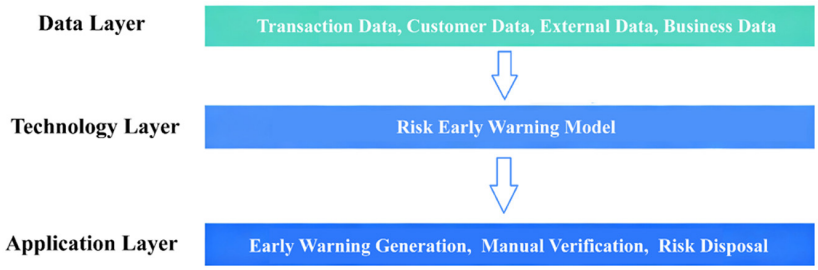

Fig. 2. Risk early warning model for money laundering transactions in bank accounts

In the data preparation phase, banks first integrate internal and external data. Internal data includes core system transaction data, customer KYC data, and account data. External data includes central bank credit reference data, public security fraud/terrorism-related list data, industrial and commercial information, and customs declaration data. This data must first undergo cleansing to eliminate missing, invalid, or other flawed data; then, features such as counterparty information and fund retention time are extracted from the cleansed data [9] [10].

In the early warning generation phase, the risk control model analyzes account transaction information in real time, generates risk early warning information based on the analysis results, and classifies the risk level into "High," "Medium," and "Low." For high-risk warnings, verification must be completed within 24 hours; for medium-risk warnings, verification must be conducted within three working days; for low-risk warnings, dynamic tracking can be carried out in subsequent work.

In the manual verification phase, the anti-money laundering (AML) department or compliance personnel conduct manual verification of the early warning information and confirm whether the transaction is an actual money laundering activity by reviewing transaction documents, communicating with customers, and querying external information.

In the disposal and reporting phase, if money laundering suspicion is confirmed, account control measures must be taken—such as suspending non-counter services, freezing the account, and reporting to the public security anti-fraud department—to block fund flows.

In the model iteration phase, the bank's AML department or compliance personnel regularly review indicators of the early warning system (e.g., accuracy rate and false positive rate). Combined with new money laundering cases and regulatory policies, they update model rules and optimize risk control algorithms [11–14].

The risk management system is shown in Figure 3.

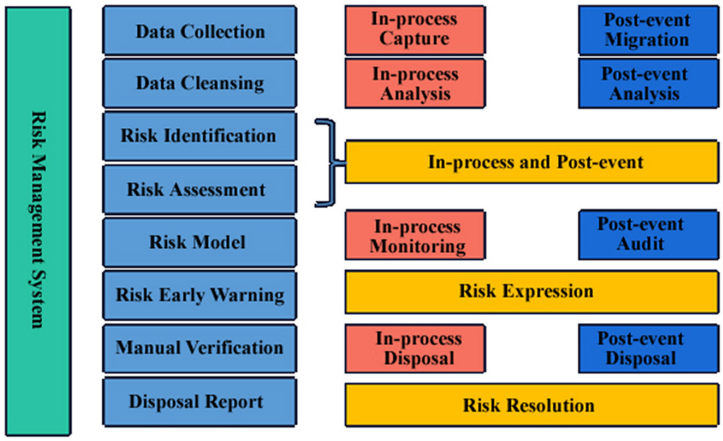

Fig. 3. Risk early warning management system

4.2 Core challenges in model practice

However, in the practical application of risk early warning, there are still issues such as data quality, early warning accuracy, and cross-departmental collaboration.

When banks obtain external data, some key data—such as customs declaration data and information on the actual controllers of enterprises—are difficult for banks to access due to inter-departmental barriers or commercial reasons, resulting in incomplete model information. Additionally, since customer data (including KYC data and transaction data) involves personal information, data collection must comply with the Personal Information Protection Law, and excessive collection or illegal use of data is prohibited.

The traditional early warning rule engines of some banks generate a large number of false warnings due to "outdated rules," leaving AML personnel of banks overwhelmed with verifying false alerts. Meanwhile, new types of money laundering methods are constantly evolving; if the features of old models are not updated in a timely manner, potential risks may be missed.

Furthermore, the verification of model warnings in banks requires collaboration among the AML department, business departments, risk control departments, and other relevant units. However, some banks have inter-departmental barriers, leading to delayed verification and missed opportunities to address risks. Moreover, the development of intelligent models (such as machine learning models) requires significant costs, which are unaffordable for small and medium-sized banks. As a result, these banks mostly rely on third-party models or simplified rule engines.

4.3 Future directions for model optimization

Considering regulatory requirements, technological development, and the evolution of money laundering risks, the optimization of risk early warning models for money laundering transactions in bank accounts can focus on the following directions:

Expansion of data dimensions: Introduce new types of data to enhance comprehensiveness. In the future, exploration can be made to incorporate "unstructured data" and "behavioral data"—using natural language processing (NLP) to identify false information and conducting behavioral analysis to determine whether an account is controlled by others.

Technology integration: Adopt a hybrid model of "rule engine + machine learning" for the collaboration between rule-based and intelligent models. This not only meets the regulatory requirements for interpretability but also improves the ability to identify risks.

Empowerment of small and medium-sized banks: It is recommended that regulatory authorities or industry associations take the lead in building an "AML Model Sharing Platform." Leading banks can provide mature models, and small and medium-sized banks can access these models on demand to reduce R&D costs. At the same time, "Model as a Service (MaaS)" can be offered to help small and medium-sized banks achieve rapid deployment, cost savings, and fast iteration.

5 CONCLUSION

The risk early warning model for money laundering transactions in bank accounts is the core technical support for banks' AML work. It has evolved from a single rule-based model to a multi-dimensional intelligent model and shifted from general monitoring to

scenario-specific early warning. In the future, the optimization of risk control models will not only require technological innovation but also call for efforts to address issues such as data compliance, cross-departmental collaboration, and regulatory adaptation. Ultimately, this will help achieve the AML goals of "accurate identification, efficient disposal, and compliant control," assist banking and financial institutions in building AML systems, and safeguard the security of the national financial system [15].

6 REFERENCES

[1] Financial Action Task Force (FATF), "Guidance on digital identity and anti-money laundering/countering the financing of terrorism," 2022.

[2] Basel Committee on Banking Supervision (BCBS), "Sound management of risks related to money laundering and financing of terrorism," 2019.

[3] C. Liu and P. Wang, "Integrating multi-dimensional data for money laundering risk assessment in cross-border bank transactions," *Computational Economics*, vol. 61, no. 2, pp. 653–678, 2023.

[4] Financial Conduct Authority (FCA), "Anti-money laundering: Guidance for firms on risk assessment and customer due diligence," 2020.

[5] H. Chen, S. Yang, and J. Li, "Rule-based vs. machine learning models for money laundering detection: A comparative analysis of accuracy and efficiency," *International Journal of Financial Engineering*, vol. 9, no. 4, p. 2250045, 2022.

[6] International Monetary Fund (IMF), "Money laundering and the role of financial institutions: Risk mitigation through technology," IMF Working Paper, no. 21/189, 2021.

[7] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," *ACM Computing Surveys*, vol. 42, no. 1, pp. 1–38, 2010.

[8] L. Zhang and W. Chen, "Customer segmentation and risk stratification for anti-money laundering: A KYC data-driven approach," *Journal of Banking and Finance*, vol. 119, p. 105932, 2020.

[9] European Central Bank (ECB), "Anti-money laundering supervision: Expectations for banks' risk models and data governance," 2022.

[10] M. Xu and J. Tang, "Cross-border money laundering detection: Leveraging external data (customs, tax, and police records) in risk models," *Journal of International Money and Finance*, vol. 116, p. 102465, 2021.

[11] Anti-Money Laundering Bureau of the People's Bank of China. *China Anti-Money Laundering Report 2019*. China Financial Publishing House, 2020.

[12] J. Li and Y. Zhang, "Construction and application of a risk early warning model for money laundering in bank accounts based on multi-dimensional integration," *Journal of Financial Research*, vol. 5, pp. 142–158, 2022.

[13] Financial Services Authority (FSA), "Money laundering risk assessment: Guidance for banks on transaction monitoring systems," 2018.

[14] J. Wang and M. Liu, "Architectural design and practice of anti-money laundering risk early warning systems for small and medium-sized banks," *Finance Forum*, vol. 26, no. 8, pp. 56–65, 2021.

[15] Office of the Comptroller of the Currency (OCC), *Bank Supervision Manual: Anti-Money Laundering Risk Management*, 2020.

7 AUTHORS

Dr. Yunfei Li is a postdoctoral researcher at the Postdoctoral Department of Turon University, Karshi 180100, Uzbekistan (E-mail: 11580718@qq.com).

Prof. Dr. Davron Aslonqulovich Juraev is at the Postdoctoral Department of Turon University, Karshi 180100, Uzbekistan (E-mail: juraevdavron12@gmail.com).

Prof. Dr. Moawia Alghalith is at UWI, St Augustine, Trinidad and Tobago (E-mail: malghalith@gmail.com).

Dr. Anastasia Kiritsi is a Professor and researcher at International School of Management Berlin, in the field of Economics and Finance, Governance and Ethics (E-mail: Anastasia.kiritsi@dozent.ism.de).