Abel Mushipe, 2026, 14:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Evaluating the Effectiveness of Predictive Data Analytics in Detecting and Combating Money Laundering Layering Schemes: A Case Study of a Local Bank, Zimbabwe

Abel Mushipe[1] Faith Nyakudya[2]

[1]Master of Technology (Honours) Student, Department of Forensic Accounting and Auditing, School of Business and Management Sciences, Harare Institute of Technology, Ha-rare, Zimbabwe, h240617n@hit.ac.zw

[2]Supervisor, Department of Forensic Accounting and Audit-ing, School of Business and Management Sciences, Harare Institute of Technology, Harare, Zimbabwe, fnya-kudya@hit.ac.zw

Abstract- Money laundering layering schemes that move funds rapidly across bank accounts, interbank switches and mobile money wallets are difficult to detect with static, rule-based transaction monitoring, particularly in Zimbabwe's volatile multi-currency environment, where fixed thresholds decay quickly and alert queues are dominated by false positives. This study evaluates the effectiveness of Predictive Data Analytics (PDA), implemented through the Vneuron anti-money laundering platform at the local Bank in Zimbabwe, in de-tecting layering schemes, reducing false positives and supporting regulatory reporting to the Financial Intelligence Unit (FIU). An embedded mixed-methods single-case design was adopted. Questionnaires were completed by 44 compliance, risk, IT forensic and digital banking professionals (88.0% response rate) and eight senior specialists were interviewed, complemented by document analysis and researcher observation. Data were analysed using descriptive statistics, Wilcoxon signed-rank tests and thematic analysis. Respondents rated rigid thresholds, unsustainable false-positive volumes and linear, account-by-account analysis as substantial weaknesses of the legacy system (means 4.16–4.20). Agreement that PDA improved layering detection, network visibility, alert prioritisation and regulatory reporting was high (means 4.02–4.32; 81.8%–90.9% agreeing or strongly agreeing), and Wilcoxon tests showed significant post-implementation improvements in perceived layering detection ($Z = -5.42$), hidden-relationship iden-tification ($Z = -5.38$) and false-positive control and investigation efficiency ($Z = -5.41$), all $p < 0.001$. Inter-viewees attributed these gains to unsupervised anomaly detection based on statistical distance, graph-based link analysis and automated narrative generation. Interpreted through agency, game and systems theories, the findings indicate that PDA removes the launderer's advantage of predictability and converts raw alerts into higher-quality evidence for the FIU. Because effectiveness was assessed through practition-er perceptions in a single institution, validation against alert-level performance data is recommended.

Keywords: Predictive Data Analytics, Anti-Money Laundering, Layering, Network Analytics, False Positives, Model Decay

I. INTRODUCTION

Money laundering remains a serious threat to the integrity of the financial system; the United Nations Office on Drugs and Crime estimates that the amount laundered each year is equivalent to 2–5% of global gross domestic product [1]. Laundering proceeds through placement, layering and integration, and it is the layering stage, in which illicit funds are fragmented and moved rapidly through many accounts, institutions and channels to sever the audit trail, that is hardest to detect. In Zimbabwe, banks must comply with the

Money Laundering and Proceeds of Crime Act [Chapter 9:24] [2] and with the Reserve Bank of Zimbabwe (RBZ) AML/CFT/CPF Guideline No. 01/2025/BSSFS [3], which push the sector towards proactive, risk-based

© 2026 Abel Mushipe, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

surveillance and the timely reporting of suspicious transactions to the Financial Intelligence Unit (FIU).

Most banks nevertheless still rely on rule-based systems (RBS) that apply static if-then thresholds to individual accounts. Such systems are reported to generate false-positive alert rates as high as 95% [4, 5], leaving investigators to spend much of their time clearing benign alerts and exposing them to alert fatigue. Because they inspect one account or network at a time, they also struggle to detect the non-linear, cross-channel loops that characterise layering [6]. In Zimbabwe's multi-currency economy, continuous inflation and exchange-rate movements between local transactional tokens and United States dollar (USD) balances make fixed value thresholds obsolete almost immediately, a phenomenon referred to in this paper as model decay. Launderers exploit these weaknesses by splitting funds into small amounts ("smurfing") and routing them through high-velocity interbank platforms such as ZIPIT and mobile money wallets [7].

Predictive Data Analytics (PDA), which combines machine learning, behavioural profiling and graph-based network analytics, offers a way to replace fixed thresholds with dynamic behavioural baselines. The local bank integrated the Vneuron AML platform in November 2025, yet empirical evidence on how effectively PDA performs in Zimbabwean commercial banks remains limited. Existing studies concentrate largely on algorithmic accuracy [8, 9], whereas the operational and regulatory outcomes that matter to compliance teams and the FIU, namely alert quality, investigation efficiency and the quality of reporting, are seldom examined. This paper addresses that gap.

1. Aim, objectives and hypotheses

The aim was to evaluate the effectiveness of PDA in improving AML transaction monitoring, reducing false positives and strengthening regulatory compliance at the local bank. Five objectives guided the study: (1) to assess the limitations of the bank's traditional rule-based monitoring; (2) to examine how PDA improves the detection of suspicious layering patterns; (3) to evaluate the role of anomaly detection and network analytics in identifying hidden transaction relationships; (4) to assess whether PDA reduces false positives and improves investigation efficiency; and (5) to determine how PDA outputs support FIU regulatory reporting.

Three alternative hypotheses were tested. H1: PDA significantly improves the detection of suspicious layering patterns. H2: Anomaly detection and network analytics significantly enhance the identification of hidden transaction relationships and cross-channel routing paths. H3: PDA significantly reduces false-positive alerts and improves investigation efficiency.

II. LITERATURE REVIEW

1. Rule-based monitoring and the layering problem

Rule-based systems encode regulatory requirements and expert knowledge as if-then rules, for example flagging every transaction above a fixed value. Their principal weaknesses are rigidity and high false-positive rates [4, 5]. Rigidity matters most at the layering stage, where criminals fragment funds below reporting thresholds and pass them through many accounts so that each transaction resembles ordinary retail activity [10]. Because legacy platforms inspect accounts one at a time, they cannot reconstruct the network that links those transactions. Jimu and Chimwai [6] argue that manual monitoring and rule-based systems are insufficient against evolving laundering techniques and point to a technological lag in the implementation of financial intelligence systems in Zimbabwe. In high-inflation, multi-currency settings the problem is compounded: thresholds fixed in one currency lose meaning as prices and exchange rates move, so rules either flood analysts with alerts or miss genuine activity.

2. Predictive data analytics in AML

PDA applies statistical techniques, machine learning and data mining to historical and live data in order to identify patterns and predict risk. Unsupervised learning

is central to layering detection because it isolates outliers without prior knowledge of what a particular crime looks like [11], and data-mining approaches have long been used to reveal hidden correlations in financial fraud data [10]. Network (graph) analytics extends this by linking accounts through shared attributes and transaction flows, exposing mule clusters and coordinated rings that account-level analysis misses [12]. Comparative and applied studies generally report improved detection capability over conventional monitoring [8, 13–17]. Mohamed [9], for example, reports that HSBC achieved a 20% reduction in false positives in 2022 through its Dynamic Risk Assessment tool and that JPMorgan Chase recorded a 25% increase in illicit-activity detection in 2023.

Evidence from Africa is growing. Studies of the South African and wider Southern African banking sectors point to the disruptive potential of artificial intelligence for money laundering control [18, 19], and Zimbabwean work has examined big data analytics in curbing financial crime and in commercial banking [20, 21]. The RBZ's own survey found varying degrees of AI adoption among supervised institutions, from advanced integration to early exploration, with use cases that include fraud detection and risk management [22]. A recurring concern is explainability: outputs must be transparent and auditable if they are to stand as evidence before regulators.

3. Theoretical framework

The study is anchored on three interlinked theories. Agency theory [23] examines friction between a principal and an agent. In AML governance the FIU is the principal and commercial banks are the agents; under rule-based monitoring, information asymmetry encourages defensive "box-ticking", in which banks over-report low-value alerts to avoid penalties. Game theory [24] treats laundering as a non-cooperative game in which launderers and auditors continuously adapt: static rules are predictable, so criminals learn to operate just beneath thresholds, whereas unsupervised models change the payoff structure by removing that predictability. Systems theory [25] views an organisation as an open system of interdependent parts; layering exploits siloed channels, and network analytics restores the whole-system view. Table 1 maps each theory to the hypothesis it informs.

Table 1: Theoretical mapping

Theory	Core proposition	Hypothesis
Agency	Information asymmetry between the FIU (principal) and the bank (agent) drives defensive over-reporting of low-value alerts.	H3
Game	Static rules are predictable and exploitable; adaptive, unsupervised models remove that predictability.	H1
Systems	Layering exploits siloed channels; network analytics restores the interdependent whole-system view.	H2

4. Research gap and conceptual framework

Global literature documents the technical superiority of PDA, but localised evidence on its regulatory and operational effectiveness in Zimbabwe's volatile macroeconomic environment is scarce. Figure 1 presents the conceptual framework. PDA (unsupervised machine learning, anomaly detection, network and link analytics, and real-time monitoring) is the independent variable; institutional readiness and context (IT infrastructure, macroeconomic volatility, the regulatory environment and analytical skills) mediate its effect; and effectiveness is the dependent variable, operationalised as detection accuracy for layering and smurfing, false-positive reduction, compliance with FIU benchmarks, forensic soundness of evidence and reduced operational risk.

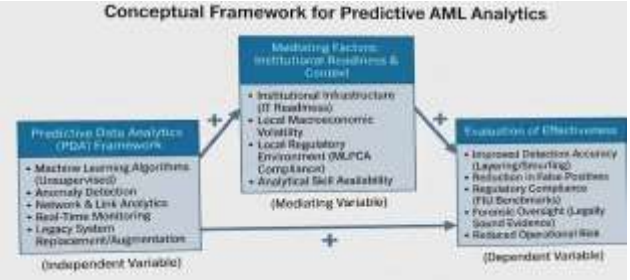


Figure 1: Conceptual framework for predictive AML analytics

III. METHODOLOGY

1. Research design

The study adopted a pragmatic philosophy and an abductive logic that moves between deductive hypothesis testing and inductive discovery. An embedded mixed-methods single-case design was used, with the local bank as the case. Data were collected at the bank's head office in Harare, which houses its centralised compliance and IT forensic infrastructure, and the study is delimited to the application of PDA to the layering phase of money laundering. Vneuron, the enterprise AML platform integrated at the bank in November 2025, served as the host environment for the PDA tools evaluated.

2. Population and sampling

The population comprised an estimated 60 professionals in the Compliance, Risk Management and IT Forensic units responsible for AML protocols and automated detection systems. Purposive sampling selected specialists with hands-on experience of PDA, and snowball sampling extended the pool to less visible pockets of expertise. Fifty questionnaires were distributed and 44 usable questionnaires were returned; ten interviews were scheduled and eight were conducted.

3.Data collection and analysis

Four instruments were used. A structured questionnaire captured demographic data and five-point Likert ratings (1 = strongly disagree, 5 = strongly agree) on the limitations of legacy systems and the effectiveness of PDA. Semi-structured interviews with senior compliance heads and chief forensic analysts explored how analysts use PDA outputs and how laundering tactics adapt. Document analysis covered internal AML policies, historical suspicious transaction reports and regulatory circulars, and direct observation recorded how analysts interact with legacy alert queues and with live demonstrations of the Vneuron link-analysis interface.

Questionnaire data were coded and analysed in IBM SPSS Version 29 using frequencies, percentages, means and standard deviations. Three Wilcoxon signed-rank tests ($\alpha = 0.05$) compared respondents' paired pre- and post-implementation ratings for each hypothesis. Interview transcripts were analysed thematically and triangulated with the survey, documents and observation notes.

4. Validity, reliability and ethics

The questionnaire was piloted on 10% of the sample and reviewed by the research supervisor and experienced banking compliance specialists to establish face and content validity, and Cronbach's alpha of at least 0.70 was set as the benchmark for internal consistency. Trustworthiness of the qualitative data was supported by triangulation and by member checking of preliminary findings with participants. All data were anonymised to protect client confidentiality, and interview participants are reported under codes.

IV.RESULTS AND DISCUSSION

1. Response rate and respondent profile

Of the 50 questionnaires distributed, 44 were returned and usable, a response rate of 88.0%, and 8 of the 10 scheduled interviews were conducted (80.0%). Both exceed the 70% level that Mugenda and Mugenda [26] classify as very good (Table 2).

Table 2: Questionnaire response rate by department

Department	Issued	Returned	Rate (%)
Compliance and AML surveillance	16	15	93.8
IT forensics / data science	8	7	87.5
Risk management	14	12	85.7
Operational / digital banking	10	8	80.0
Other	2	2	100.0
Total	50	44	88.0

Respondents were 54.5% male (n = 24) and 45.5% female (n = 20), and 47.7% were aged 30–39 and 31.8% aged 40–49. Highly qualified staff predominated: 43.2% held a postgraduate degree, 38.6% a bachelor's degree, and 18.2% a professional AML certification such as CAMS or ICA. A total of 70.4% had at least six years of banking, risk or compliance experience, and 54.5% had served the bank for six years or longer, so most respondents could compare the legacy and PDA environments. Compliance and AML surveillance (34.1%), risk management (27.3%), operational and digital banking (18.2%), IT forensics and data science (15.9%) and other control functions (4.5%) were all represented.

4.2 Limitations of the legacy system (Objective 1)

Respondents rated all three tested weaknesses of the rule-based system as substantial or severe (Table 3): rigid hardcoded thresholds (M = 4.20, SD = 0.76; 84.1% agreement), unsustainable false-positive ratios (M = 4.16; 79.5%) and linear analysis that cannot link webs of accounts (M = 4.16; 86.4%). Interviewees identified two structural failure points. The first was chronic alert fatigue: legacy rules reportedly consumed up to 80% of operational hours in clearing normal transactions, causing genuine anomalies to be overlooked. The second was a masking blind spot: because systems viewed transactions account by account and relied on historical typologies, they could not see the circular, multi-account paths used in layering until a human updated the rules. Researcher observation corroborated this; analysts faced a visible backlog in which static rules without multi-currency indexation repeatedly flagged routine retail deposits and salary adjustments. These findings are consistent with reports that rule-based monitoring is rigid and prone to excessive false positives [4, 5] and that isolated data inspection cannot stop coordinated, multi-layered schemes [10].

Table 3: Respondents' ratings of legacy and PDA performance (N = 44)

Item	Mean	SD	Agree / strongly agree, n (%)
Objective 1: limitations of the legacy system			
Rigid, hardcoded linear thresholds	4.20	0.76	37 (84.1)
Unsustainable false-positive alert ratios	4.16	0.75	35 (79.5)
Linear analysis cannot link webs of accounts	4.16	0.78	38 (86.4)
Objective 2: layering detection			
Legacy systems insufficient for non-linear layering	4.16	0.78	38 (86.4)
PDA identifies hidden anomalies in real time	4.05	0.78	37 (84.1)
PDA unmasks smurfing and structuring networks	4.14	0.70	38 (86.4)
Objective 3: network analytics			
Link analysis exposes concealed relationships	4.25	0.69	40 (90.9)
Unsupervised detection unmasks multi-account networks	4.14	0.77	39 (88.6)
Visualisation identifies mule clusters	4.11	0.78	37 (84.1)
Objective 4: false positives and efficiency			

Item	Mean	SD	Agree / strongly agree, n (%)
Less time spent on false-positive alerts	4.30	0.79	39 (88.6)
Risk scores used to prioritise investigations	4.16	0.71	38 (86.4)
Objective 5: regulatory reporting			
Improved timeliness and quality of SAR submissions	4.32	0.71	40 (90.9)
Agile under currency volatility without model decay	4.02	0.76	36 (81.8)

Five-point Likert scale (1 = strongly disagree, 5 = strongly agree). Source: primary data.

3. Layering detection and network analytics (Objectives 2 and 3)

Agreement was strong that PDA improves layering detection (Table 3, Chart 1). Respondents agreed that legacy systems are insufficient for non-linear layering (M = 4.16), that PDA identifies hidden anomalies in real time (M = 4.05) and that it unmasks smurfing and structuring networks (M = 4.14). Network analytics scored highest: link analysis exposing concealed relationships between separate accounts (M = 4.25, SD = 0.69) attracted 90.9% agreement, followed by unsupervised detection of multi-account networks without predefined criteria (M = 4.14) and visualisation of mule clusters and synthetic identities (M = 4.11). All standard deviations were below 0.80, indicating consensus.

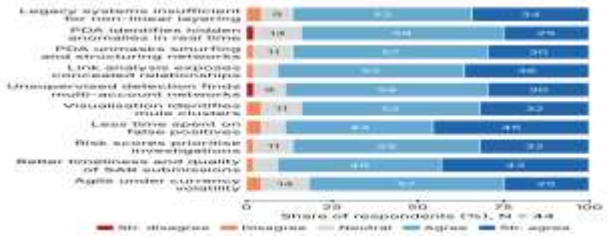


Chart 1: Distribution of responses on PDA effectiveness (Objectives 2–5), %

Interviewees described two behaviours behind these ratings: real-time dynamic tracking in place of historical batch processing, and behavioural clustering of velocity and frequency deviations in place of fixed dollar ceilings. Holistic network views made automated pass-through accounts and loop routing apparent, and visual graphs removed the burden of reading raw ledger lines when tracing funds across branches. In a live demonstration observed by the researcher, a simulated smurfing scenario, in which separate retail accounts at different branches deposited amounts 5% below the reporting limit, went undetected by the legacy rules; the Vneuron link engine clustered the accounts into a single web through shared device identifiers, IMEI signatures and rapid-succession corporate distribution pools. Although a single demonstration is illustrative rather than conclusive, the pattern matches the literature on anomaly detection as deviation from a calculated baseline [11] and on network analytics for exposing concealed relationships [12].

4. False-positive reduction and regulatory reporting (Objectives 4 and 5)

Respondents agreed that the transition to Vneuron significantly reduced the time spent on false-positive alerts (M = 4.30, SD = 0.79; 88.6% agreement) and that automated risk scores are used to prioritise investigations (M = 4.16; 86.4%). Interviewees explained that statistical distance allows low-risk behavioural deviations to be archived automatically, and that risk-ranked queues let analysts isolate high-probability layering paths in minutes rather than hours. These perceptions echo the false-positive reductions reported by major banks [9].

For regulatory reporting, improved timeliness and quality of suspicious activity report (SAR) submissions recorded the highest mean of all items (M = 4.32, SD = 0.71; 90.9%), and 81.8% agreed that the system is agile enough to handle local currency volatility without model decay (M = 4.02). Informants attributed the latter to a shift from nominal currency triggers to statistical distributions (Z-scores) that absorb inflationary spikes

without artificial alerts, and the former to automatically compiled forensic narratives that standardise the time needed to submit complete investigative dossiers to the FIU. Such transparent, human-readable audit trails also respond to the explainability concern noted in Section 2.2.

5. Hypothesis testing

Wilcoxon signed-rank tests on the paired pre- and post-implementation ratings (N = 44) rejected all three null hypotheses (Table 4). Perceived capability to unmask layered transaction loops (H1), to map hidden relationships and cross-channel routing paths (H2) and to control false positives and investigation turnaround (H3) were each significantly higher after the deployment of Vneuron (all $p < 0.001$). For H3, mean perceived performance rose from 1.82 under the legacy system to 4.64 after implementation.

Table 4: Wilcoxon signed-rank tests (N = 44)

Hyp.	Paired ratings compared (pre vs post)	Z	p	Decision
H1	Capability to unmask layered transaction loops	−5.42	< 0.001	H0 rejected
H2	Capability to map hidden relationships and routing paths	−5.38	< 0.001	H0 rejected
H3	False-positive control and investigation efficiency	−5.41	< 0.001	H0 rejected

Source: primary data analysis (SPSS).

The interviews illustrate the mechanisms. A senior AML surveillance officer explained how syndicates exploited the old setup:

> "They mapped out our hardcoded currency ceilings and split large transactions into small, rapid fractions … The old system was blind because it only checked files account-by-account. Vneuron changed the game by tracking statistical distance and frequency deviations rather than rigid dollar amounts." (Participant 01)

A chief compliance executive described the effect on analysts' workload:

> "Analysts were desensitized by a non-stop wave of normal commercial transactions flagged … simply because a client crossed a hardcoded dollar threshold during inflation cycles. Vneuron's automated alert verification cuts through this white noise." (Participant 03)

6. Discussion

The results are consistent with the three theoretical lenses. In line with game theory, replacing fixed ceilings with continuously recalculated behavioural baselines removes the predictability on which sub-threshold structuring depends. In line with systems theory, analysing the transaction web as a whole rather than account by account addresses the siloed blind spots that layering exploits, as reflected in the high ratings for network analytics. In line with agency theory, converting raw alerts into probabilistic narratives of suspicion aligns the bank's output with the FIU's objective of tracking financial crime networks rather than filing defensively, which is consistent with the high ratings for reporting quality. Together with the quantitative evidence, the findings support H1, H2 and H3 within the limits of the design discussed in Section 5.

V. CONCLUSION

This study evaluated the effectiveness of PDA, deployed through the Vneuron platform, in detecting and combating money laundering layering schemes at the local bank. Practitioners judged the legacy rule-based system to be rigid, noisy and blind to cross-channel loops, and judged PDA to be markedly better at

detecting layering, mapping hidden relationships, reducing false-positive workload and supporting FIU reporting under volatile multi-currency conditions. All three hypotheses were supported. The evidence indicates that PDA shifts the bank from volume-centric box-ticking towards intelligence-led surveillance.

Recommendations

For the local bank: establish dedicated high-speed application programming interfaces between core banking systems and mobile payment networks so that unified transaction streams feed the PDA engine; build automated multi-currency calibration for USD and ZWG wallets to prevent model decay; train compliance officers and forensic accountants in graph databases, machine-learning outputs and anomaly verification; and review model performance regularly as laundering tactics evolve. For the RBZ and FIU: move reporting benchmarks from volume to quality indices that assess the actionable value of suspicious transaction reports; establish a regulatory sandbox under Guideline No. 01/2025/BSSFS for testing unsupervised algorithms; and enable secure, anonymised exchange of layering typologies between institutions. For governance: audit scoring engines periodically for demographic, regional or socio-economic bias; adopt explainable ("white-box") AI so that flags can be defended in legal and regulatory reviews; and protect training data through tokenisation and encryption in line with data-protection law.

Limitations and future research

Effectiveness was assessed through practitioner perceptions, retrospective pre/post ratings and qualitative evidence rather than alert-level performance logs such as precision, recall and investigation turnaround times, so the findings may reflect perception bias. The sample was small, non-probability and drawn from a single institution, and Vneuron had operated at the bank for a limited period, which restricts generalisability and prevents conclusions on long-term adaptation by launderers. Future research should validate these results against objective alert-level data, adopt longitudinal designs, extend the scope to other commercial banks and microfinance institutions, and examine cross-border laundering through decentralised finance and peer-to-peer mobile networks.

Acknowledgements

The author thanks God for the strength and opportunity to complete this work and is deeply grateful to the supervisor, Ms Nyakudya, for her time, guidance and constructive criticism. Sincere thanks go to the compliance, risk, IT forensic and digital banking professionals at the local bank who completed the questionnaires and gave interviews despite busy schedules, and to family and friends for their steadfast support.

REFERENCES

1. United Nations Office on Drugs and Crime. (n.d.). Money laundering. https://www.unodc.org/unodc/en/money-laundering/overview.html
2. Government of Zimbabwe. (2013). Money Launder-ing and Proceeds of Crime Act [Chapter 9:24]. https://www.fiu.co.zw/amlcft-framework
3. Reserve Bank of Zimbabwe, Bank Supervision, Surveil-lance and Financial Stability Division. (2025). Guidance to reporting institutions on AML/CFT/CPF obligations: AML/CFT/CPF Guideline No. 01/2025/BSSFS. Harare: Re-serve Bank of Zimbabwe.
4. Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Ak-su, G., Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. Future Generation Computer Systems, 159, 161–171. https://doi.org/10.1016/j.future.2024.05.027
5. Tiwari, S. (2025). Enhancing financial crime detection through data science-driven transaction monitoring: A comprehensive framework for modern financial institutions.

International Journal of Computing and Engineering, 7(13), 53–63. https://doi.org/10.47941/ijce.2423

6. Jimu, T., Chimwai, L. (2025). A model for harnessing financial intelligence systems for money laundering preven-tion: A systematic review of technological and regulatory approaches. Lighthouse: The Zimbabwe Ezekiel Guti Univer-sity Journal of Law, Economics and Public Policy, 4(1&2).
7. Zimbabwe Ministry of Finance, Financial Intelligence Unit. (2024). National Money Laundering Risk Assessment 2024. Harare: Government of Zimbabwe.
8. Ajagbe, SA., Majola, S., Mudali, P. (2025). Compara-tive analysis of machine learning algorithms for money laundering detection. Discover Artificial Intelligence, 5(144), 1–19. https://doi.org/10.1007/s44163-025-00397-4
9. Mohamed, B. (2025). The use of artificial intelligence in combating financial crimes and money laundering in international trade: A data-driven analysis (2010–2024). International Journal of Economic Performance, 8(1), 310–330. https://doi.org/10.54241/2065-008-001-017
10. Ngai, EWT., Hu, Y., Wong, YH., Chen, Y., Sun, X. (2011). The application of data mining techniques in finan-cial fraud detection: A classification framework and an aca-demic review of literature. Decision Support Systems, 50(3), 559–569.
11. Chandola, V., Banerjee, A., Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15.
12. Deprez, B., Vanderschueren, T., Baesens, B., Verdonck, T., Verbeke, W. (2025). Network analytics for anti-money laundering – a systematic literature review and experimental evaluation. arXiv preprint.
13. Hamza, M., Raffat, MW. (2024). AI-driven compliance and detection in anti-money laundering: Addressing global regulatory challenges and emerging threats. Journal of Computer Science and Applications, 1(2), 1–9. https://doi.org/10.51846/jcsa.v1i2.3886
14. Iguodala, OD., Oyiborhoro, A. (2025). AI-powered anti-money laundering (AML) and fraud detection – en-hancing financial security through intelligent fraud detec-tion. World Journal of Advanced Research and Reviews, 26(02), 3702–3714. https://doi.org/10.30574/wjarr.2025.26.2.0637
15. Torres, IL. (2023). Using predictive modeling to com-bat money laundering. Issues in Information Systems, 24(1), 233–244. https://doi.org/10.48009/1_iis_2023_120
16. Ogunleye, OS. (2025). AI in anti-money laundering (AML) and transaction monitoring: Improving detection of suspicious activities. ResearchGate. https://www.researchgate.net/publication/399285534
17. Bolu, T., Heart, S. (2024). Predictive analytics for iden-tifying money laundering patterns in Azerbaijani banking transactions. International Journal of Scientific Research and Management, 12(08), 5865–5872. https://doi.org/10.18535/ijsrm/v12i08.ec02
18. Chitimira, H., Torerai, E., Jana, VLM. (2024). Leverag-ing artificial intelligence to combat money laundering and related crimes in the South African banking sector. Potchefstroom Electronic Law Journal, 27, 1–30. https://doi.org/10.17159/1727-3781/2024/v27i0a18024
19. Masunda, M., Barot, H. (2025). Disruption in South-ern Africa's money laundering activity by artificial intelli-gence technologies. Journal of Risk and Financial Man-agement, 18(1), 1–18.
20. Dandazara, S., Chisunga, D. (2026). The role of big data analytics in curbing financial crime in Zimbabwe's public sector. International Journal for Multidisciplinary Research, 8(2).
21. Mangwiro, B. (2025). A critical analysis into big data analytics as a weapon for competitive advantage for com-mercial banks in Zimbabwe. Dissertation, Midlands State University, Gweru.
22. Reserve Bank of Zimbabwe. (2024). Bank Supervision Annual Report 2024. Harare: Reserve Bank of Zimbabwe.
23. Jensen, MC., Meckling, WH. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

24. Von Neumann, J., Morgenstern, O. (1944). Theory of Games and Economic Behavior. Princeton, NJ: Princeton University Press.
25. Von Bertalanffy, L. (1968). General System Theory: Foundations, Development, Applications. New York: George Braziller.
26. Mugenda, OM., Mugenda, AG. (1999). Research Methods: Quantitative and Qualitative Approaches. Nairo-bi: ACTS Press.