Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

Machine Learning for Fraud Detection in Nigerian Card and Mobile-Money Payments: Evidence, Data Gaps and Explainability Requirements

[1]*Kufre Ambrose Edet, [2]Patience U. Usip, [3]Kubiat Akpan Ekpo

[1,3]Department of Information Systems and Technology, Faculty of Computing, National Open University of Nigeria (NOUN), Abuja, Nigeria
[2]Department of Computer Science, University of Uyo, Uyo, Akwa Ibom State, Nigeria
*Corresponding Author's E-mail: nou255316957@noun.edu.ng

Abstract: Between 2020 and 2024, reported fraud cases in Nigeria fell by 31% while the value lost rose by 350%, before losses fell by 51% in 2025. Research on machine-learning detection has grown, but much of it rests on data that do not describe Nigerian payments. This targeted review combines recent international reviews of card-fraud detection, six Nigerian-context detection studies, two studies of AI adoption in Nigerian banks, and official and legal sources on fraud reporting and automated decision-making. Four findings emerge. First, international evidence leans on one benchmark: 72.7% of 44 studies reviewed in 2025 used the same European card dataset, and only 11.4% reported the area under the precision-recall curve. Second, the Nigerian-context studies rely on synthetic data, a Nigerian dataset of undocumented provenance, or non-Nigerian public or simulated data, and their results cannot be compared with one another. Third, explanations are rarely tested: about 80% of studies in one review used predictive performance as a proxy for explanation quality, and only two of the six Nigerian-context studies state an explanation method. Fourth, the Nigeria Data Protection Act, 2023, its 2025 implementation directive and recent Central Bank guidance raise the cost of unexplained automated decisions. Eight gaps, a reporting checklist and a research agenda are derived. The paper reports no new experimental results.

Keywords: Fraud detection, Nigeria, Machine learning, Explainable AI, Data scarcity, Data protection, Digital payments, Mobile money.

I. INTRODUCTION

Nigeria's electronic payment system is large and growing, and its fraud statistics are easy to misread. Between 2020 and 2024 the annual number of reported fraud cases fell by 31%, from 101,624 to 70,111, while the value lost rose by 350%, from N11.61 billion to N52.26 billion [1]. More than half of the 2024 total, N31.1 billion, is attributed to a single incident involving one entity [2]. In 2025 reported losses fell by 51% to N25.85 billion across about 67,500 cases [3], [4]. These series depend on institutions reporting what they find, and the number of institutions actively reporting fraud fell from a peak of 45 in the second quarter of 2024 to 34 by the fourth quarter of 2025 [4].

Machine learning is widely proposed as a response, but evidence that transfers to Nigerian banks and payment providers is harder to find than the volume of published work suggests. Three questions decide whether a published model is usable: whether it was tested on data that resemble Nigerian payments, whether it was scored with measures that reflect an investigator's workload, and whether its decisions can be explained to a customer, a regulator or a court. This review examines each in turn.

The paper makes four contributions. It summarises what recent international reviews report about datasets, metrics and explainability in card-fraud research. It examines six Nigerian-context detection studies and two studies of AI adoption in Nigerian banks, and the data on which they depend. It connects explanation requirements to the Nigeria Data Protection Act, 2023 and recent Central Bank guidance. It derives eight research gaps, a reporting checklist and a practical agenda. The paper reports no new experiments; every figure is taken from a cited source.

© 2026 JAIET All Rights Reserved CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

II. REVIEW METHOD

2.1 Questions

The review addresses four questions. RQ1: which datasets, metrics and explainability practices dominate recent reviews of card-fraud detection? RQ2: what machine-learning evidence exists for Nigerian payments, and on what data does it rest? RQ3: what do Nigerian fraud statistics imply for labels and evaluation? RQ4: what do Nigerian law and regulation require of automated fraud decisions?

2.2 Sources and selection

Sources were found by web searches run on 10 and 11 November 2026, rechecked against their sources on 18 November 2026, and were kept only when their bibliographic details and the figures used here could be confirmed on the publisher's or issuer's own page. Four groups were admitted: (i) peer-reviewed reviews of machine learning or explainable AI in payment or financial fraud detection published from 2023 to 2026; (ii) published machine-learning studies on card or payment fraud that use Nigerian data, data calibrated to Nigerian fraud statistics, or that appear in Nigerian journals; (iii) studies of AI adoption for fraud detection in Nigerian financial institutions; and (iv) official, institutional or professional sources on Nigerian fraud statistics, data protection and payment regulation. Student theses, social-media posts and vendor material were excluded. One preprint, the only study found that uses a Nigerian card dataset, is included and identified as a preprint. Where only a news report or a law-firm summary was available for a statistic or a regulation, it is cited as such and identified in the text.

2.3 Limitations

This is a targeted review, not a PRISMA-style systematic review, and it makes no claim to count every Nigerian study. The Nigerian evidence examined here consists of six detection studies and two adoption studies; that number reflects the date and source filters above and should not be read as the size of the national literature. The full texts of the four Nigerian-context detection studies that do not use explanation methods were read to confirm that; Alaba et al. and Ayodeji are described from their published abstracts. Review statistics are reported as their authors state them. The Central Bank guidance is described from a law-firm summary, and readers should consult the primary circular before relying on it.

III. THE NIGERIAN FRAUD LANDSCAPE

Social engineering was the largest category in 2025, accounting for 47% of fraud volume and N17.84 billion of losses, followed by card theft at 17% and robbery at 11% [4]. The same source credits the migration to EMV chip-and-PIN cards with virtually eliminating ATM card cloning. This suggests that the remaining exposure lies more in methods that manipulate customers than in card data.

Three implications follow for model builders. First, labels are not neutral. Fraud labels come from institutional reports, so a training set built from them reflects what institutions detected and chose to report, and the decline in reporting [4], [3] raises the risk that labelled cases are incomplete. Second, much social-engineering fraud involves a transaction that the customer authorises, which can look normal in transaction attributes alone. Whether transaction-level models can detect it is an open question that the evidence reviewed here does not settle. Third, annual loss totals are lumpy, as the single 2024 incident shows, so loss value is a poor yardstick for comparing models across years; case-level measures are more stable.

These conditions bear on the choice of method. Where labelled fraud is scarce or incomplete, supervised models are difficult to train and to validate, and methods that learn normal behaviour and flag departures from it become attractive. The reviews examined here report the label problem [5], but they do not show that any single approach resolves it. Methods of this kind can raise many alerts for each genuine case, so the number of alerts an investigation unit can handle becomes the binding constraint, as the worked example in Section VIII shows.

IV. INTERNATIONAL EVIDENCE

4.1 Recurring obstacles

Recent reviews agree on the main obstacles. A review of artificial intelligence for financial fraud detection covering 2015 to 2025 identifies severe class imbalance, concept drift, limited labelled data and trade-offs between detection performance and interpretability as recurring problems [5]. An earlier systematic review of 181 articles from 2019 to 2021 reaches a similar conclusion, noting that no system had yet delivered both high efficiency and high accuracy [6]. These problems are not specific to Nigeria, but each is sharper where labelled data are scarce and reporting is incomplete.

© 2026 JAIET All Rights Reserved

CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

4.2 Concentration on one benchmark

A systematic review of card-fraud studies that kept the original class imbalance selected 44 studies from 1,425 records identified for 2019 to mid-2025. It found that the European card dataset was used in 32 of the 44 studies, or 72.7% [7]. That dataset contains 284,807 transactions of which about 0.17% are fraudulent [8], and it is conventionally cited to Dal Pozzolo et al. [9]. PaySim appeared in two of the 44 studies (4.5%) [7]. A field whose conclusions rest mainly on one European card dataset cannot assume that its results hold for Nigerian debit cards or mobile wallets.

4.3 Metrics and operational cost

The same review shows how often the measures reported do not match operational needs. Accuracy was reported in 88.6% of studies and AUC-ROC in 47.7%, but the area under the precision–recall curve (AUC-PR) in only five studies (11.4%) [7]. At a fraud prevalence of 0.17%, a classifier that labels every transaction legitimate is about 99.8% accurate and detects nothing, so accuracy says little. Precision-oriented measures matter more to an investigation team, because every false alert consumes analyst time.

4.4 Explainability

Explanation is even less developed. Of the 44 studies, only two implemented operational interpretability, both with SHAP, and none used LIME [7]. SHAP assigns each feature an additive contribution to an individual prediction [10]. A review of 49 studies from 2021 to 2025 on explainable AI in fraud detection reports that SHAP and LIME are the dominant methods, but that around 80% of the studies used predictive performance as a proxy for explanation quality instead of evaluating explanations directly [11]. The same review describes an explainability–imbalance paradox: resampling used to manage class imbalance can distort the background distributions or local neighbourhoods that post-hoc explanations rely on, which compromises their faithfulness [11].

V. NIGERIAN MACHINE-LEARNING EVIDENCE

5.1 Two studies built on synthetic data

Two 2026 studies were identified that apply machine learning with explanation to Nigerian payment fraud. Idowu and Owolabi build a synthetic benchmark of 1,000,000 transactions calibrated to fraud patterns reported by NIBSS [12]. The authors report a 69.1% decrease in simulated fraud-related costs, from N81.8 million to N25.2 million, and an XGBoost model reached a recall of 74.6% and an F1-score of 0.854. SHAP ranked transaction amount first for XGBoost, and the authors single out the web (0.34%) and mobile (0.33%) channels, with their simulated fraud rates, as needing enhanced monitoring [12]. Two details qualify these results. The cost reduction was reached at a decision threshold that produced 2,405 false positives, a trade-off the abstract does not mention, and the simulated fraud rate of 0.30% was chosen deliberately far above the 0.0008% reported by NIBSS, because the real rate would yield only about eight fraud cases per million transactions [12]. Soyemi and Olasina evaluate a stacked ensemble of random forest, gradient boosting and extra trees, with an XGBoost meta-classifier and SHAP, on two datasets: the Kaggle card dataset (the European dataset of Section 4.2) and a new synthetic Nigerian dataset of 150,000 transactions with 1.12% fraud that includes POS, USSD, mobile-money and rural–urban patterns [8].

5.2 The comparability problem

Their results illustrate the comparability problem. On the European card dataset the stacked ensemble reached a recall of 79.70% and an F1-score of 0.880. On the Nigerian synthetic dataset, the abstract puts the recall of the individual classifiers below 3.1%, although the paper's own tables give 31.0% for XGBoost, and the ensemble reached 64.10% recall and an F1-score of 0.460 [8]. Differences of this size suggest that how a synthetic dataset is built can matter as much as the model, so results from one synthetic dataset should not be read as the performance to expect in a Nigerian bank. The two studies also differ in data size, fraud prevalence and the measures they emphasise, and neither can be compared directly with the other.

5.3 Mobile money and simulators

Mobile-money research has the same dependence. PaySim was created because of the lack of legitimate public datasets on mobile-money transactions; it simulates transactions based on an original dataset [13]. It is useful for method development, but a simulator can only reproduce fraud behaviour that its designers encoded, which limits what a model trained or tested on it can show about real fraud. Table 1 summarises the principal sources.

© 2026 JAIET All Rights Reserved

CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

Table 1: Principal sources reviewed

Source	Type and scale	Relevance to Nigerian payments
Yang *et al.* [5]	Review of AI for financial fraud detection, 2015–2025	Imbalance, drift, scarce labels and the interpretability trade-off recur
Marazqah Btoush *et al.* [6]	Systematic review; 181 articles, 2019–2021	No system yet combined high efficiency with high accuracy
Baisholan *et al.* [7]	Systematic review; 44 studies kept from 1,425 records, 2019–2025	European dataset in 72.7%; AUC-PR in 11.4%; two studies with operational SHAP
Zafar and Wu [11]	Systematic review; 49 studies, 2021–2025	About 80% use predictive performance as a proxy for explanation quality
Idowu and Owolabi [12]	Synthetic NIBSS-calibrated benchmark; 1,000,000 transactions	Cost cut of 69.1% at a threshold giving 2,405 false positives; web and mobile channels flagged
Soyemi and Olasina [8]	Stacked ensemble; European dataset and 150,000-transaction Nigerian synthetic set	Recall 79.70% on European data against 64.10% on Nigerian synthetic data
Ejalonibu *et al.* [3]	Working paper on 2025 payment-fraud data	Losses fell 51% to N25.85 billion; warns of declining reporting

Results are quoted as reported by each source; the studies use different data and metrics and are not directly comparable.

5.4 Other Nigerian-context studies

Four further detection studies were identified. Onyeama compares an autoencoder with principal component analysis on Nigerian credit-card fraud data that the paper says were retrieved from a code repository, where a research team had stored them; the paper does not name the team or institution, and does not document how the data were collected or labelled [14]. It treats fraud as an anomaly-detection problem and reports the autoencoder as the more reliable method, but it reports counts of correct predictions and not precision, recall or F1 [14]. This preprint also states that access to reliable data is a major obstacle to card-fraud research in Nigeria [14]. Oguntunde and Abioye address fake transaction alerts, a problem reported to affect Nigerian point-of-sale businesses, using a synthetic PaySim-generated dataset of about one million transaction alerts from Kaggle and an ensemble of support vector machine and random forest models; both reach an F-measure of about 97.5%, and the authors judge random forest the more suitable [15]. Enehikhare and Odumuyiwa, from the University of Lagos, compare logistic regression, decision trees, random forest and XGBoost on a European card dataset of over 550,000 transactions and a simulated set of 1,000 transactions, and list explanation of model decisions as a future challenge [16]. Adejoh et al. propose an unsupervised ensemble of autoencoders, self-organising maps and restricted Boltzmann machines with an adaptive reconstruction threshold, tested on the European and IEEE-CIS datasets, and report higher accuracy and fewer false positives than one-class SVM and Isolation Forest [17]. Their motivation, that static thresholds limit unsupervised detectors, bears directly on alert volume; the paper names explainable AI as future work [17].

Table 2 sets the six Nigerian-context studies side by side. Two use synthetic data calibrated to Nigeria, one uses a Nigerian dataset of undocumented provenance, and three use public or simulated data that are not Nigerian. Two use an explanation method, SHAP, and the other four use none. None of the six describes a test of explanation quality, an evaluation with investigators, or a deployed decision-support system.

Table 2: Nigerian-context detection studies

Study	Data	Method	Explanation stated
Idowu and Owolabi [12]	1,000,000 synthetic transactions calibrated to NIBSS fraud statistics	Logistic regression, random forest, XGBoost	SHAP
Soyemi and Olasina [8]	European dataset and 150,000 synthetic Nigerian transactions	Stacked ensemble	SHAP

© 2026 JAIET All Rights Reserved

CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

Study	Data	Method	Explanation stated
Onyeama [14]	Nigerian card data from a code repository; collection and labelling undocumented	Autoencoder and PCA	None
Oguntunde and Abioye [15]	Synthetic PaySim-generated alert dataset from Kaggle; not Nigerian	SVM and random forest	None
Enehikhare and Odumuyiwa [16]	European card dataset (over 550,000) and 1,000 simulated transactions; not Nigerian	Logistic regression, decision tree, random forest, XGBoost	None
Adejoh et al. [17]	European and IEEE-CIS datasets; not Nigerian	Unsupervised autoencoder, SOM and RBM with adaptive threshold	None

"None" means the full text uses no explanation method.

5.5 Organisational readiness

Two studies look at the institutions that must use these models. Alaba et al. surveyed Nigerian banks using a Likert-scale questionnaire and ordered logistic regression, and report that top-management support, IT infrastructure, regulatory compliance, staff competency and perceived effectiveness raise the adoption of AI-driven fraud detection, while high implementation cost discourages it [18]. Ayodeji studied, through a qualitative design grounded in the UTAUT2 model, how IT leaders in the Nigerian financial sector use big data analytics to develop fraud detection strategies, and notes that growth in digital banking has raised both transaction volume and fraud cases [19]. Neither study tests a model. Their relevance is that a detector with high precision on paper still needs staff who can run it and trust it, which places weight on the explanation requirements discussed next.

VI. EXPLAINABILITY AND REGULATION

6.1 Automated decisions under the Data Protection Act

Section 37 of the Nigeria Data Protection Act, 2023 gives a data subject the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject [20]. The right does not apply where the decision is necessary for entering into or performing a contract, is authorised by a written law that sets suitable safeguards, or is authorised by the data subject's consent. Even then, the controller must implement suitable safeguards, including the rights to obtain human intervention, to express a point of view and to contest the decision [20]. The Nigeria Data Protection Commission lists, among a data subject's rights, the right not to be subjected to automated decision-making [21]; the Act sets out these rights in sections 34 to 38 [20]. The Commission's 2025 implementation directive (GAID) goes further in two places. Article 18(1)(f) requires consent before a controller makes a decision based solely on automated processing that produces legal effects concerning, or significantly affecting, the data subject. Article 28(3) makes a Data Protection Impact Assessment mandatory, to be filed with the Commission, for evaluation or scoring (profiling) and for automated decision-making with legal or similar significant effects [22]. A fraud system that scores customers and then blocks a card, freezes an account or declines a transfer without human review may fall within these provisions. Whether it does, and whether any exception applies, is a legal question that institutions should settle with counsel; this review makes no finding on it.

6.2 Central Bank guidance on fraud monitoring

The Central Bank of Nigeria issued Guidelines on Instant Payment Functionalities for Financial Institutions by circular on 12 March 2026, effective 1 July 2026. According to a law-firm summary, they require every financial institution to activate enterprise-wide fraud monitoring covering both inflows and outflows, and they call for security and Data Protection Impact Assessments to ensure compliance with the Data Protection Act [23]. Fraud monitoring is therefore becoming a mandatory and continuously running function, which increases the number of automated decisions that may need explanation and review.

6.3 What this means for model design

The directive also expects a controller to disclose the capabilities of the technology it uses, in particular the use of algorithms for profiling, the risks involved and how they are mitigated (Art. 42) [22]. Taken together, these sources imply that a fraud model intended for Nigerian use should supply, for each alert, an explanation that is faithful to the model, understandable to an investigator and retained for audit. The evaluation gap reported by Zafar and Wu [11] matters here: if explanations are

© 2026 JAIET All Rights Reserved CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

never tested directly, an institution cannot show that its explanations meet that standard.

VII. GAPS AND RESEARCH AGENDA

Table 3 sets out eight gaps drawn from the evidence above, each with a suggested response. The gaps and responses are the authors' synthesis rather than findings reported by the sources.

Table 3: Research gaps and suggested responses

Gap	Evidence	Suggested response
1. No open real data	Nigerian studies use synthetic, undocumented or non-Nigerian data (Table 2); access to reliable data is named as the main obstacle [14]; PaySim exists because public mobile-money data are lacking [13]	Supervised secure environment in which code goes to the data and only metrics leave
2. One-benchmark reliance	European dataset in 72.7% of 44 studies [7]	Report results on at least two independent datasets and state each dataset's limits
3. Metrics detached from workload	AUC-PR reported in 11.4% of studies [7]	Report original prevalence, AUC-PR, precision at a fixed alert volume and the false-alert ratio
4. Untested explanations	About 80% use predictive performance as a proxy [11]	Test explanation faithfulness and stability; run small investigator usability studies
5. Resampling and explanations	Explainability–imbalance paradox [11]	State whether explanations were computed on data with the original class distribution
6. Incomplete labels and drift	Falling reporting [4], [3]; drift recurs in reviews [5]	Evaluate on later time periods; model label delay and under-reporting
7. Social-engineering fraud	47% of 2025 fraud volume [4]; none of the six studies examined (Table 2) reports modelling customer-authorised fraud	Combine device, session and behavioural signals; build evaluation sets from investigated cases
8. Deployment readiness	Cost, staff competency and IT infrastructure shape adoption [18]; leaders' fraud strategies rely on analytics capacity [19]	Report integration cost, staffing and investigator workflow; run pilots with banks

The first gap is the one on which most of the others depend. Without a legitimate route to real Nigerian labelled data, studies will continue to be built on synthetic sets and compared with each other as if they measured the same thing. A route could take the form of a regulator- or NIBSS-supervised secure environment in which researchers submit code and receive only metrics, which limits the movement of personal data out of the institution. Shared reporting standards (original prevalence, AUC-PR, precision at a fixed number of alerts per day, and the false-alert ratio) would let studies be compared even before real data are available.

VIII. A REPORTING STANDARD FOR NIGERIAN STUDIES

8.1 Why alert volume matters

An illustration shows why precision at a fixed alert volume belongs in every study. Take one million card transactions at the 0.17% prevalence of the European dataset [8]: about 1,700 are fraudulent and 998,300 are legitimate. A detector with a false positive rate of 1%, which sounds small, raises about 9,983 false alerts, about 5.9 for every fraudulent transaction even if it finds all of them. At a false positive rate of 0.1% the figure falls to about 998 false alerts, or 0.6 per fraudulent transaction. The illustration is arithmetic and not a result from any study, but it shows that the difference between 99% and 99.9% specificity decides whether an investigation team can cope. Reporting accuracy alone hides this difference.

8.2 A checklist

Table 4 turns the gaps into a checklist that a Nigerian study can follow and a reader can verify. Items 1 and 2 address data provenance, items 3 to 5 address evaluation, items 6 and 7 address explanation, and item 8 addresses regulation.

© 2026 JAIET All Rights Reserved

CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

Table 4: Reporting checklist for fraud-detection studies on Nigerian payments

Item	What to report	Why it matters
1. Data provenance	Source, period, channel and how labels were assigned; for synthetic data, what the generator was calibrated to	Lets readers judge transfer to Nigerian payments [12], [8], [14]
2. Prevalence	Fraud share in the training, validation and test sets	Precision depends on prevalence [7]
3. Split	Time-ordered split with later data held out	Tests for drift [5]
4. Metrics	AUC-PR, precision and recall at a fixed daily alert volume, and the false-alert ratio	Matches investigator capacity [7]
5. Baselines	At least one simple or rule-based baseline and one independent dataset	Shows whether complexity pays and reduces one-benchmark reliance [7]
6. Explanation method	Method used, the reference data, and whether resampling was applied	Faithfulness depends on the background data [11]
7. Explanation test	A direct test of faithfulness or stability, or a user study with investigators	Closes the evaluation gap [11]
8. Regulatory mapping	Whether an alert leads to automated action, and where human review occurs	Data Protection Act, s. 37(1)–(3) [20]; GAID Arts. 18 and 28 [22]

8.3 For banks and payment providers

Institutions evaluating a published model or a vendor product can use the same checklist as a procurement test. They should ask for precision at their own alert capacity rather than accuracy, for results on a time-ordered hold-out, and for a sample of explanations that their own investigators have reviewed. They should also record how reporting changes affect their labels, since a fall in reported cases may reflect changes in reporting and not less fraud [3], [4].

IX. CONCLUSION

The evidence reviewed here supports a cautious reading. International research on card-fraud detection leans on one European dataset and on measures that hide operational cost. The six Nigerian-context detection studies examined rest on synthetic, undocumented or non-Nigerian data, use different metrics, and only two state an explanation method. Explanations are seldom tested, and Nigerian law and regulation are raising the stakes for automated decisions. Practitioners should treat published accuracy figures as demonstrations of method, not forecasts of performance in their own institutions, and should ask for precision at original prevalence, alert volume and evidence about explanations. Researchers can contribute most by securing legitimate access to real data, by agreeing evaluation standards such as the checklist proposed here, and by testing explanations with the investigators who use them.

DECLARATIONS

Conflict of interest: The authors declare no conflict of interest.

Funding: This research received no external funding.

Ethics: Not applicable; the review uses only published and publicly available sources and no personal data.

Data availability: No new datasets were generated. All sources are listed in the references.

Author contributions:

Kufre Ambrose Edet: Conceptualization, Investigation, Verification, Writing – original draft.

Patience Usoro Usip: Supervision, Writing – review and editing.

Kubiat Akpan Ekpo: Investigation, Validation, Writing – review and editing.

Use of AI tools: An AI language assistant was used to help search for sources, draft and edit the manuscript, and check its arithmetic. The authors selected the sources, checked every figure and reference against the publisher's or issuer's own page, and take full responsibility for the content.

Prior publication: This manuscript is original, is not under consideration elsewhere, and reports no new experiments. The authors have a separate published JAIET paper on an

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

unsupervised ensemble for debit-card fraud detection; this review does not reuse its data or results.

REFERENCES

[1] Nairametrics, "Nigeria's financial sector suffers N52.26 billion loss to fraud in 2024 – NIBSS report," Feb. 26, 2025. [Online]. Available: https://nairametrics.com/2025/02/26/nigerias-financial-sector-suffers-n52-26-billion-loss-to-fraud-in-2024-nibss-report/

[2] "Nigeria's Digital Payment Fraud Drops in 2025 — NIBSS," *Newscentral TV*, Jan. 22, 2026. [Online]. Available: https://newscentraltv.com/?p=380296

[3] G. Ejalonibu, E. Obot, and L. Nandi, "Electronic payment fraud trends in Nigeria's banking sector – 2025 data, emerging risks, and legislative imperatives," working paper, NILDS institutional repository, Jan. 2026. [Online]. Available: https://ir.nilds.gov.ng/handle/123456789/3473

[4] "Nigeria: Losses to fraud in banks decline, CBN intensifies measures," *allAfrica*, Jan. 22, 2026. [Online]. Available: https://allafrica.com/stories/202601230595.html

[5] H. Yang, Z. Shukur, and S. Sahran, "A review of artificial intelligence for financial fraud detection," *Applied Sciences*, vol. 16, no. 4, Art. no. 1931, 2026, doi: 10.3390/app16041931.

[6] E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," *PeerJ Computer Science*, vol. 9, Art. no. e1278, 2023, doi: 10.7717/peerj-cs.1278.

[7] N. Baisholan, J. E. Dietz, S. Gnatyuk, M. Turdalyuly, E. T. Matson, and K. Baisholanova, "A systematic review of machine learning in credit card fraud detection under original class imbalance," *Computers*, vol. 14, no. 10, Art. no. 437, 2025, doi: 10.3390/computers14100437.

[8] J. Soyemi and J. R. Olasina, "A hybrid stacked ensemble framework for fraud detection in Nigerian financial ecosystems: Evaluation with localized synthetic data," *Int. J. Wireless and Microwave Technologies*, vol. 16, no. 4, pp. 233–250, 2026, doi: 10.5815/ijwmt.2026.04.13.

[9] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in *Proc. IEEE Symp. Series on Computational Intelligence (SSCI)*, Cape Town, South Africa, 2015, pp. 159–166, doi: 10.1109/SSCI.2015.33.

[10] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Advances in Neural Information Processing Systems*, vol. 30, 2017, pp. 4765–4774.

[11] U. Zafar and F. Wu, "Methodological challenges in explainable AI for fraud detection: A systematic literature review," *Artificial Intelligence Review*, vol. 59, Art. no. 115, 2026, doi: 10.1007/s10462-026-11516-7.

[12] G. A. Idowu and J. E. Owolabi, "Ensemble-based fraud detection in Nigerian banking: A synthetic data benchmark and cost-sensitive analysis," *Unilag J. Mathematics and Applications*, vol. 6, no. 1, pp. 107–129, 2026.

[13] E. A. Lopez-Rojas, A. Elmir, and S. Axelsson, "PaySim: A financial mobile money simulator for fraud detection," in *Proc. European Modeling and Simulation Symposium (EMSS)*, 2016, pp. 249–255.

[14] J. Onyeama, "Credit card fraud detection in the Nigerian financial sector: A comparison of unsupervised TensorFlow-based anomaly detection techniques, autoencoders and PCA algorithm," arXiv preprint arXiv:2407.08758, 2024. [Online]. Available: https://arxiv.org/abs/2407.08758

[15] T. Oguntunde and C. O. Abioye, "Development of comparative fake transactions alert detection models using machine learning," *Univ. Ibadan J. Science and Logics in ICT Research*, vol. 15, no. 1, pp. 121–129, 2025.

[16] C. C. Enehikhare and V. Odumuyiwa, "Comparative analysis of machine learning models for fraud detection in imbalanced credit card transaction datasets," *Univ. Ibadan J. Science and Logics in ICT Research*, vol. 14, no. 1, pp. 25–37, 2025.

[17] J. Adejoh, N. Owoh, M. Ashawa, S. Hosseinzadeh, A. Shahrabi, and S. Mohamed, "An adaptive unsupervised learning approach for credit card fraud detection," *Big Data and Cognitive Computing*, vol. 9, no. 9, Art. no. 217, 2025, doi: 10.3390/bdcc9090217.

[18] J. S. Alaba, S. J. Ahmed, A. P. Farida, and V. O. Oluwatosin, "Adoption of AI-driven fraud detection system in the Nigerian banking sector: An analysis of cost, compliance, and competency," *Economic Review of Nepal*, vol. 8, no. 1, pp. 16–33, 2025, doi: 10.3126/ern.v8i1.80740.

© 2026 JAIET All Rights Reserved CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 11, pp 11-19, November-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.311002
Available Online at https://www.jaiet.com

[19] I. A. Ayodeji, "Fraud detection and prevention in the Nigerian financial industry," D.I.T. dissertation, Walden Univ., 2024. [Online]. Available: https://scholarworks.waldenu.edu/dissertations/16614

[20] Federal Republic of Nigeria, *Nigeria Data Protection Act, 2023*, s. 37 (Automated decision making).

[21] Nigeria Data Protection Commission, "Your rights as a data subject," ndpc.gov.ng. [Online]. Available: https://ndpc.gov.ng (accessed Nov. 11, 2026).

[22] Nigeria Data Protection Commission, *Nigeria Data Protection Act 2023: General Application and Implementation Directive (GAID) 2025*, NDPC/NDP ACT-GAID/01/2025, Mar. 20, 2025, Arts. 18, 28 and 42.

[23] A. Alex-Adedipe and M. Imonitie, "Key regulatory update: CBN guidelines on instant payment functionalities and mobile banking security," Pavestones Legal, *Mondaq*, Apr. 15, 2026. [Online]. Available: https://www.mondaq.com/nigeria/financial-services/1773436/key-regulatory-update-cbn-guidelines-on-instant-payment-functionalities-and-mobile-banking-security

AUTHORS BIOGRAPHY



Kufre Ambrose Edet is an Information Technology professional, educator, and researcher pursuing a Master of Science degree in Information Technology at the National Open University of Nigeria. His professional experience includes computer education, ICT training, and technology support. His research interests include artificial intelligence, explainable machine learning, financial fraud detection, and decision support systems, particularly their application to practical challenges in Nigeria.



Prof. Patience Usoro Usip is a Computer Science academic at the University of Uyo, Akwa Ibom State, Nigeria, where she serves as Head of the Department of Computer Science. Her research specialisation is Knowledge Representation and Reasoning, with particular interests in knowledge graphs, ontologies, Semantic Web technologies, and intelligent knowledge management systems. Her scholarly contributions include research on semantic knowledge retrieval, ontology-based systems, multilingual knowledge representation, and machine learning applications.



Kubiat Akpan Ekpo is an Information Technology professional and researcher at the National Open University of Nigeria (NOUN), where he currently serves as the Faculty of Computing Coordinator at the Uyo Study Centre. He holds a Master of Science degree in Computer Security and Forensics and is currently pursuing a PhD in Cyber Security at the Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), NOUN. His research specialisation is Large Language Models, with particular interests in Prompt Attacks, Artificial Intelligence, Incident Response and Digital Forensics, as well as Governance, Risk, and Compliance (GRC).

Citation of this Article:

Kufre Ambrose Edet, Patience U. Usip, & Kubiat Akpan Ekpo. (2026). Machine Learning for Fraud Detection in Nigerian Card and Mobile-Money Payments: Evidence, Data Gaps and Explainability Requirements. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(11), 11-19. Article DOI: https://doi.org/10.47001/JAIET/2026.311002

***** End of the Article *****