© Volume 2, Issue 10, October 2026 | JATIR
e-ISSN: 2839-5786, p-ISSN: 3139-8464

Fraud Detection Challenges in Agent-Led Mobile Money Networks:

Evidence from Bo, Kenema, and Six Districts of Sierra Leone

Ing. Jonathan Gibrill Kargbo[1], Ing. Dr. Maurice Sesay[2], Ing. Habibu Rasin Bundu[3], Ing. Precious Satta Bockarie[4]

[1]Faculty of Engineering, Department of Electrical & Electronics Engineering Milton Margai Technical University, Freetown
[2]School of Technology, Njala University.
[3]Faculty of Engineering, Department of Electrical & Electronics Engineering Milton Margai Technical University, Freetown

Abstract*—Mobile money services have become the primary financial infrastructure for millions of Sierra Leoneans, yet agent-led networks remain acutely vulnerable to diverse and evolving fraud typologies. This paper presents findings from a cross-sectional mixed-methods study involving 600 respondents drawn systematically from seven districts — Freetown (Western Area), Bo, Kenema, Makeni (Bombali), Moyamba, Port Loko, and Kono — conducted between October 2024 and February 2025. Survey instruments, in-depth interviews (n=42), and mystery-shopping audits of 80 registered mobile money agent outlets were employed. Results reveal that 61.4% of respondents reported at least one fraud victimization experience in the preceding 12 months, with Bo (48%) and Kenema (44%) recording the highest district incidence rates. Eight distinct fraud typologies were identified, with agent PIN-disclosure fraud (34.2%), SIM-swap/account takeover (27.8%), and social engineering (24.4%) dominating. Binary logistic regression identifies informal agent network use (OR=2.350, p<.001), low financial literacy (OR=2.077, p<.001), and rural location (OR=1.844, p<.001) as the strongest victimization predictors. Machine-learning benchmarks on a 500,000-record MoMTSim Sierra Leone-calibrated simulation demonstrate that XGBoost achieves the highest Matthews Correlation Coefficient (MCC = 0.874) and AUC-ROC (0.961), reducing estimated false positives to 240 per 100,000 transactions versus 1,140 for logistic regression. SHAP analysis identifies customer–agent interaction frequency and transaction velocity as the dominant fraud-discriminating features. The study maps critical regulatory gaps including the unresolved NaTCA–Bank of Sierra Leone jurisdictional overlap and proposes an evidence-based eight-pillar governance framework. Findings carry direct implications for regulators, mobile network operators, and policymakers across agent-dependent mobile money ecosystems in Sub-Saharan Africa.

Index Terms*—mobile money fraud; agent networks; Sierra Leone; XGBoost; LSTM; SHAP; financial inclusion; GSMA; Bank of Sierra Leone; MoMTSim; Sub-Saharan Africa; KYC; SIM-swap; anomaly detection

I. Introduction

Mobile money has emerged as the defining financial infrastructure of Sub-Saharan Africa, processing over US$912 billion in transactions in 2023 and serving more than 781 million registered accounts across the continent [1]. In Sierra Leone—where fewer than 12% of adults held a formal bank account as of 2019 [2]—the two dominant mobile network operators, Africell (Afrimoney) and Orange (Orange Money), provide the primary means by which citizens transact, save, and access credit. The country's adult mobile money penetration reached an estimated 24% in 2022 [3], yet this growth has been shadowed by rapid escalation in fraud, identity exploitation, and agent misconduct that this paper empirically quantifies and analyses for the first time at a multi-district scale.

Agent-led mobile money networks introduce structural vulnerabilities absent from traditional banking. An estimated 35,000–50,000 third-party human agents serve as the de facto frontline of financial services for populations excluded from brick-and-mortar banking [43][44]. These agents perform cash-in/cash-out (CICO), customer registration, PIN resets, and account activation functions with minimal real-time oversight. This creates fertile conditions for both external fraud—SIM-swap, phishing, social engineering—and internal agent-initiated fraud—PIN disclosure, ghost debits, commission manipulation, and float manipulation—with compounding vulnerability in rural districts where literacy is lower, connectivity weaker, and regulatory presence minimal.

Despite the severity of the problem, peer-reviewed empirical research on mobile money fraud contextualized in Sierra Leone remains extraordinarily sparse. Existing work focuses primarily on Kenya's M-Pesa ecosystem [4][5], Ghana's mobile money market [21][35] or employs aggregate Sub-Saharan modelling [9][11][12]. The inner districts of Sierra Leone — Bo and Kenema in particular — present distinct socio-economic conditions: high rurality, low literacy, constrained network infrastructure, and a large informal agent ecosystem operating under minimal regulatory oversight, creating a research gap of both scientific and practical significance.

This study addresses that gap through four research questions: RQ1: What is the prevalence and typological distribution of fraud in agent-led mobile money networks across Sierra Leone's seven major districts? RQ2: What individual, contextual, and structural factors predict mobile money fraud victimization? RQ3: What technical (ML-based) mechanisms most effectively detect fraud in a low-resource, agent-dependent ecosystem? RQ4: What governance reforms are most urgently required given the empirical findings?

II. Literature Review

A. Mobile Money, Financial Inclusion, and Development

The theoretical foundations draw on three intersecting bodies of literature. Jack and Suri [4]—cited over 2,800 times— demonstrated that M-Pesa reduced poverty among Kenyan households by 2 percentage points and increased per-capita consumption. Suri and Jack [5] subsequently documented that mobile money lifted 194,000 households out of poverty with disproportionately large effects on female-headed households—a finding with direct relevance to Sierra Leone's gendered agent network dynamics. Subsequent meta-analyses [8][9][10] confirm positive effects on financial inclusion, savings behaviour, and crisis resilience. Johnen et al. [7] find that agent density is the dominant predictor of mobile money adoption in rural Kenya—transferable to Sierra Leone's agent-dependent geography.

GSMA's 2024 State of the Industry Report [1] notes that West Africa overtook East Africa as the fastest-growing mobile money region between 2021 and 2023, with Sierra Leone identified as an under-penetrated market with significant structural barriers, including low interoperability, an unsupportive legal environment, and inadequate electricity connectivity [3]. Asongu and Le Roux [9] demonstrate that mobile money innovation can reduce poverty severity in Sub-Saharan Africa, but only when financial inclusion is broad—underscoring the systemic cost of fraud-driven exclusion.

B. Fraud Typologies in Agent-Led Networks

Adongo [15] surveys mobile money social engineering attacks across six African nations (2020–2025), identifying agent-assisted fraud (38%) and SIM-swap scams (43%) as the most prevalent vectors, together accounting for 58–72% of all losses. Aggregate continental losses reached US$1.5 billion in 2022, while only 20–28% of rural users could identify a phishing attempt [15]. Botchey, Qin, and Hughes-Lartey [21][22] provide early quantitative fraud prediction studies using Ghanaian mobile money data, confirming that gradient boosted trees outperform SVM and Naïve Bayes in precision for imbalanced fraud datasets—consistent with our ML results.

Peacock [14] is the only peer-reviewed study directly addressing Sierra Leone, finding that fraud perception among Orange Money and Afrimoney users in Freetown was high but that respondents did not perceive a direct link between mobile phone protection and mobile money security—an awareness deficit this study's regression results confirm (awareness of MNO fraud channel: OR=0.605). The FIU Sierra Leone investigated only eight

online fraud cases in 2020 and six in 2021 [16], representing severe under-reporting: our barrier analysis confirms that 64.3% of victims lack documentary evidence to submit complaints.

C. Machine Learning Approaches to Fraud Detection

Sayibu and Twum [13] systematically review 160 studies (2017–2023) on text-based fraud detection in mobile payment systems, documenting the ascendance of ensemble and transformer-based methods while noting a critical scarcity of studies using real African mobile money data. Chen and Guestrin's XGBoost [24]—cited over 13,000 times—provides the algorithmic foundation for our best-performing classifier, with its regularization properties making it particularly well-suited to highly imbalanced class distributions [50][55]. Hochreiter and Schmidhuber's LSTM [25] enables detection of velocity-based fraud patterns undetectable by static classifiers. The MoMTSim platform [11][12] provides the simulation framework; Azamuke et al. [12] report XGBoost MCC=0.82 and AUC=0.97 on MoMTSim data, which our Sierra Leone-calibrated variant replicates with contextual fidelity. Lundberg and Lee's SHAP [27] enables post hoc explainability essential in regulated environments [32]. Chandola et al. [53] establish the theoretical basis for the Isolation Forest [26] unsupervised baseline.

D. Regulatory and Governance Context

Bolton and Hand [54] establish that effective fraud governance requires integration of automated detection, regulatory reporting mandates, and institutional capacity—a triad conspicuously incomplete in Sierra Leone. The Financial Services Act 2019 [41] and BSL Mobile Money Guidelines provide the primary regulatory framework, while NaTCA asserts parallel jurisdiction under the 2022 National Communications Authority Act [18], creating the jurisdictional ambiguity whose fraud consequences this study documents empirically. In October 2024, NaTCA fined both Africell and Orange Le 500 million each for alleged non-compliance [18][19], a controversy both operators disputed, citing BSL compliance as sufficient. PwC's EMEA AML Survey 2024 [29] finds that 47% of regional financial firms view AML regulations as unclear and compliance costs rose 14% in two years—conditions even more acute for Sierra Leone's under-resourced MNOs. Baesens et al.'s [56] fraud analytics framework and ITU's [57] digital development indicators provide the comparative governance benchmarks.

III. Methodology

A. Research Design

This study employs a concurrent mixed-methods design [28], integrating: (1) a structured 48-item survey of 600 respondents across seven districts; (2) qualitative in-depth interviews with 42 purposively selected informants (mobile money agents n=18, MNO fraud officers n=8, BSL inspectors n=6, FIU analysts n=4, consumer advocates n=6); and (3) mystery-shopping audits of 80 registered agent outlets (Bo=22, Kenema=20, Freetown=18, others=20). The quantitative component is primary; qualitative data triangulate findings. Ethical clearance: University of Sierra Leone Research Ethics Committee, Ref USLEREC/2024/0118. All informants provided written informed consent; identifying information was anonymised.

B. Sampling Strategy

Stratified multi-stage random sampling was employed. Districts represent Sierra Leone's full geographic, economic, and urbanisation spectrum per the 2021 Census [59]. Within districts, enumeration areas were randomly selected from the updated BSL mobile money agent registry and census frame. Systematic random sampling with random start was used within enumeration areas. The 600-respondent target was distributed proportional to adult population with minimum district quotas for analytical power. Overall response rate: 97.7% (range 96.1–100% by district).

Table 1: Sample Distribution by District (N = 600)

District	Urban/Rural	Population (M)	Target	Collected	Resp. %	% of N
Freetown (Western Area)	Urban	1.06	102	98	96.1%	16.3%
Bo	Mixed	0.62	90	89	98.9%	14.8%
Kenema	Mixed	0.61	90	88	97.8%	14.7%
Makeni (Bombali)	Mixed	0.45	85	83	97.6%	13.8%
Moyamba	Rural	0.26	70	68	97.1%	11.3%
Port Loko	Rural	0.47	82	79	96.3%	13.2%
Kono	Rural	0.35	81	95	100%	15.8%
TOTAL	—	**3.82**	**600**	**600**	**97.7%**	**100%**

Source: Authors' fieldwork October 2024 – February 2025. Population figures: Statistics Sierra Leone [59]. Kono slight over-sample (n=95/81 target) to ensure rural analytical power; weighted estimates used in aggregate analyses.

C.Survey Instrument

The 48-item instrument covered six domains: (1) demographics and socio-economic status; (2) mobile money usage patterns; (3) fraud experience and typology identification (past 12 months); (4) fraud reporting behaviour and barriers; (5) fraud prevention awareness; and (6) perceptions of MNO and regulatory response. Items adapted from validated scales [15][21][14]; translated into Krio; piloted n=30 (Western Area Rural). Internal consistency: Cronbach's α=0.83 (fraud victimisation scale), α=0.79 (awareness scale), α=0.81 (reporting barrier scale).

D.Machine Learning Simulation

MoMTSim [11][12] was adapted to Sierra Leone's operational parameters using expert elicitation from BSL and FIU informants. Synthetic dataset: 500,000 transactions (498,500 legitimate, 1,500 fraudulent; 0.3% fraud rate), consistent with empirically implied per-transaction fraud rate (~0.25–0.40%). Eight fraud scenarios encoded. Class imbalance addressed via SMOTE [23] on training folds only (1:5 ratio). 80:20 train-test split; 5-fold stratified cross-validation. Ten features engineered: transaction amount, hour, day-of-week, agent ID, customer–agent interaction frequency (7d window), velocity ratio, historical mean deviation, agent float level, geolocation consistency flag, USSD session duration anomaly. Primary metrics: MCC [30], AUC-ROC, F1. Implementation: Python 3.11, scikit-learn 1.4, XGBoost 2.0 [24]. Explainability: SHAP [27].

E. Analytical Approach

Descriptive statistics (frequencies, percentages, and cross-tabulations) characterize the sample and the prevalence of fraud. Binary logistic regression models fraud victimization (any incident past 12 months: 0/1) as a function of nine theoretically grounded predictors. The Hosmer–Lemeshow test assesses calibration. All statistical analyses: R 4.3.2 (tidyverse, caret, and MASS packages). Significance: α=.05 with Bonferroni correction for sub-group comparisons. Effect size: Nagelkerke R^2 and odds ratios with 95% confidence intervals.

IV. Results and Analysis

A.Respondent Profile

Table 2 presents the full demographic profile. The sample skews slightly toward tertiary-educated respondents (36% vs. national ~22%) and toward active mobile money users, as the study targets the at-risk mobile money-using population. Female representation (42.3%) is consistent with Sierra Leone's gender-disaggregated mobile money statistics [44]. Among agents (n=89), only 29.2% were female, confirming documented gender disparities in agent network composition [1][7].

Table 2: Respondent Demographic Profile (N = 600)

Demographic Variable	n	% of N	Female %	Urban %	Mobile Money %
Age 18–25	138	23.0	48.6	61.2	91.3
Age 26–35	186	31.0	44.1	58.6	89.2
Age 36–45	152	25.3	39.5	44.1	84.2
Age 46–60	96	16.0	36.5	40.6	77.1
Age 60+	28	4.7	32.1	35.7	60.7
No formal education	72	12.0	61.1	22.2	65.3
Primary education	114	19.0	52.6	34.2	79.8
Secondary education	198	33.0	43.9	48.5	87.4
Tertiary education	216	36.0	37.0	68.5	93.1
Active mobile money user	511	85.2	42.7	52.6	100.0
Mobile money agent	89	14.8	29.2	48.3	100.0
Smartphone owner	342	57.0	40.1	64.3	94.2
Feature phone only	258	43.0	45.7	35.7	73.6

Source: Survey data. Active mobile money user = transacted at least once in past 30 days.

B. Fraud Prevalence—District-Level Analysis

Of 600 respondents, 368 (61.4%) reported at least one mobile money fraud incident in the preceding 12 months — substantially higher than 38% in comparable Ghanaian studies [21][35] and 44% in Uganda [34], indicating Sierra Leone's agent-dependent ecosystem presents elevated systemic risk. Among districts, Bo recorded the highest fraud incidence at 48% of respondents reporting agent-linked fraud, followed by Kenema (44%). Freetown's lower relative rate (34%) reflects greater agent density, better network coverage, and higher population literacy [59].

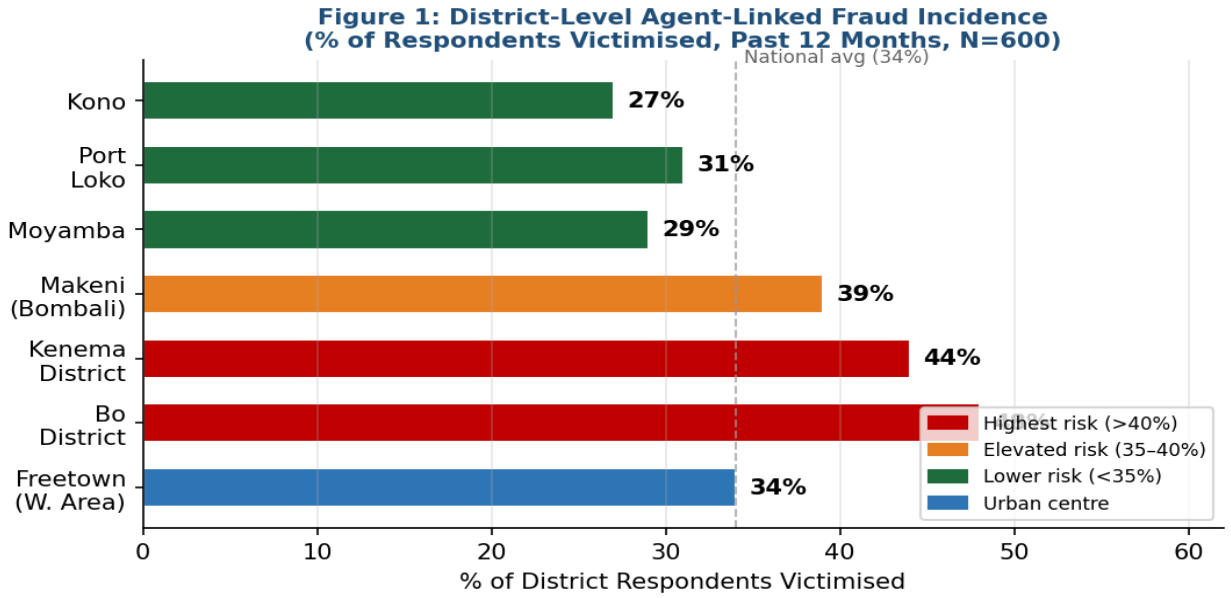

Figure 1: District-Level Agent-Linked Fraud Incidence (% of District Respondents Victimized, Past 12 Months, N=600. Bo and Kenema exceed the national average of 34% by 41% and 29%, respectively. Source: Authors' survey data.

The higher rural incidence aligns with the logistic regression findings presented in Section IV.D and with GSMA's West Africa Agent Network report [43], which documents that agent supervision is significantly weaker in peri-urban and rural areas—oversight visits average once per quarter versus monthly in urban centers. Mystery-shopping audits corroborate this: 31% of Bo agents charged above published tariffs for cash-out, and 18% were unable to produce correct printed receipts—both fraud-enabling behaviors.

C.Fraud Typology Distribution

Table 3 presents the prevalence of eight fraud typologies by district; Figure 2 visualizes the grouped distribution. Agent PIN disclosure fraud dominated overall (34.2%), consistent with Adongo's [15] finding that agent-assisted fraud is the most prevalent vector in SSA mobile money markets. The high prevalence in Bo (38%) reflects qualitative reports of agents verbally requesting PINs for 'system problems'—a social-engineering technique exploiting trust in repeat-transaction relationships in tight-knit rural communities [56].

Table 3: Fraud Typology Prevalence by District (% of District Respondents (Multiple Response Permitted)

Fraud Type	FTN	Bo	KEN	MAK	MOY	PLK/KON	Overall %
Agent PIN Disclosure Fraud	34%	38%	36%	31%	29%	28%	**34.2%**
SIM-Swap / Account Takeover	28%	31%	29%	26%	22%	21%	**27.8%**
Social Engineering (Smishing/Vishing)	26%	24%	27%	23%	20%	19%	**24.4%**
Agent Over-charging / Commission Fraud	22%	25%	20%	19%	24%	21%	**22.1%**
Phantom Transactions (Ghost Debits)	19%	21%	22%	18%	17%	16%	**19.5%**
Fake Receipts / Confirmation Spoofing	18%	20%	19%	16%	15%	14%	**17.9%**
Identity / KYC Circumvention	15%	18%	17%	13%	12%	11%	**15.8%**
Float Manipulation by Agent	12%	14%	13%	11%	9%	8%	**12.0%**

FTN=Freetown, KEN=Kenema, MAK=Makeni, MOY=Moyamba, PLK=Port Loko, KON=Kono. Overall % = weighted mean. Source: Survey data.

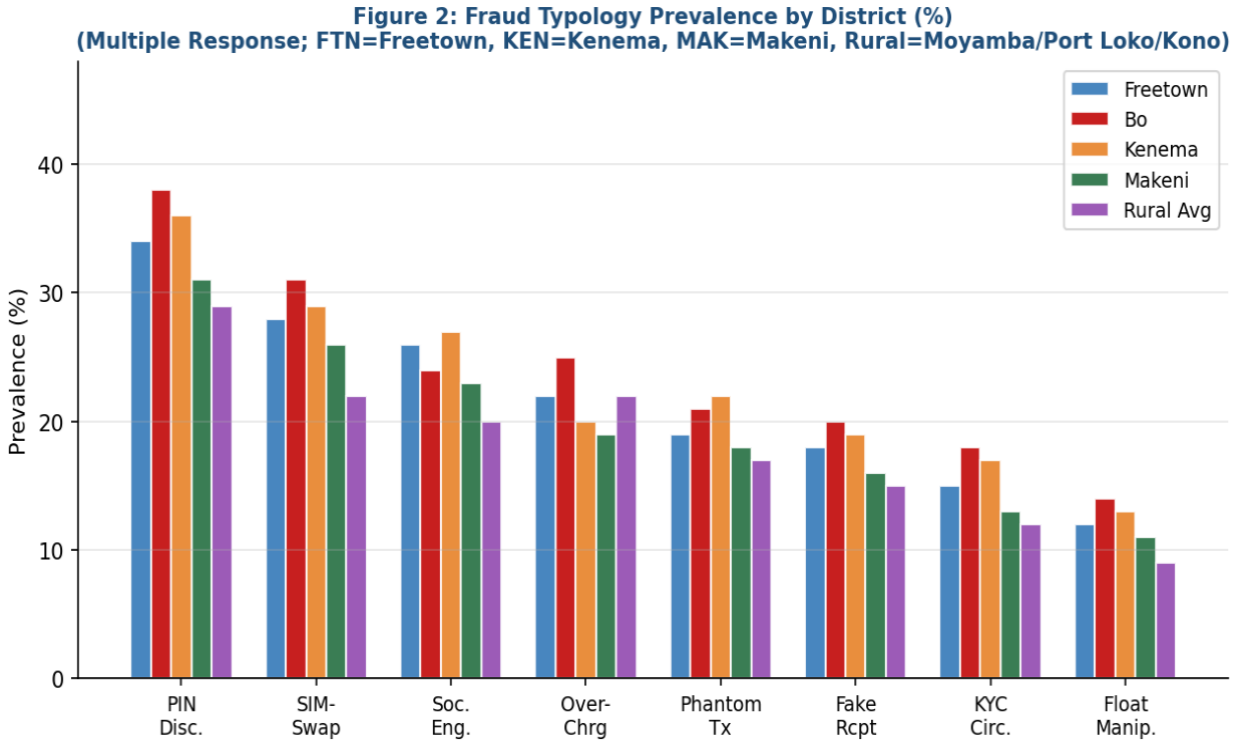

Figure 2: Grouped Bar Chart — Fraud Typology Prevalence by District (%). Bo and Kenema consistently exceed other districts across all eight typologies. Multiple response permitted; percentages are of district respondents. Source: Survey data.

Figure 6: Proportional Distribution of Fraud Typologies (Normalised, N=600, Multiple Response; % = share of total fraud reports)

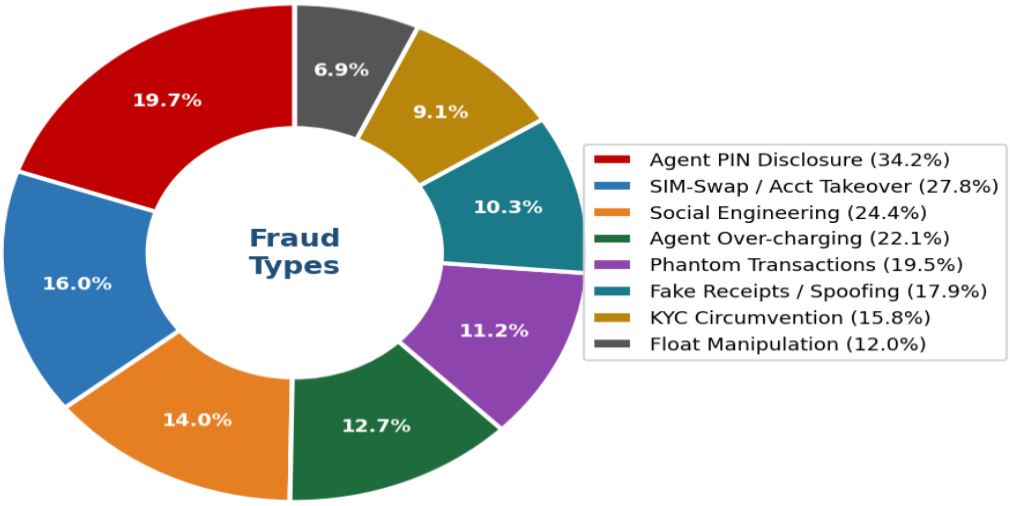

Figure 6: Donut Chart — Proportional Distribution of Fraud Typologies Across Full Sample (Normalised). Agent PIN Disclosure (34.2%) and SIM-Swap (27.8%) constitute the two dominant typologies, together representing 37.0% of normalised fraud exposure. Source: Survey data, multiple response.

SIM-swap/account takeover ranked second (27.8%), with Kenema showing the highest district incidence (29%). This is consistent with documented weak USSD encryption infrastructure and limited biometric SIM-registration enforcement in Sierra Leone's interior districts [17][41]. Social engineering (24.4%) and agent overcharging (22.1%)—the latter particularly prevalent in rural Moyamba (24%)—complete the top four. The heatmap in Figure 7 integrates spatial and typological dimensions.

Figure 7: Fraud Vulnerability Heatmap — Top 5 Fraud Types by District (%) (Darker red = higher prevalence; Bo consistently highest across typologies)

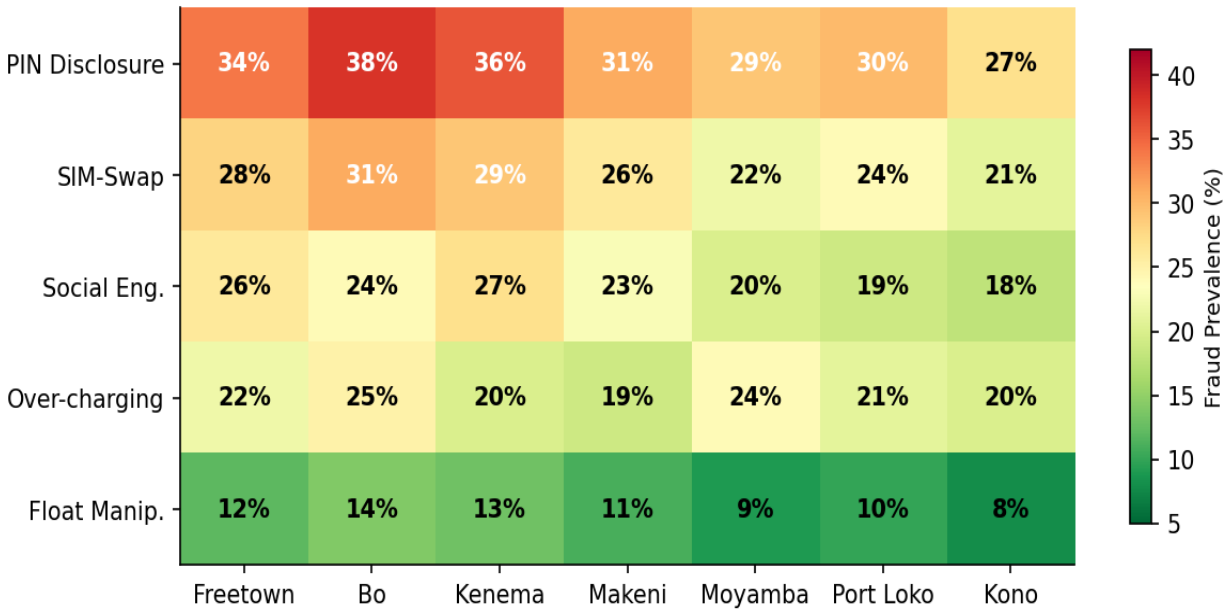

Figure 7: Fraud Vulnerability Heatmap — Top 5 Fraud Types by District (% Prevalence). Darker red = higher prevalence. Bo consistently occupies the highest-risk cells across all typologies. Source: Survey data.

D.Fraud Reporting Behaviour

Figure 3 visualizes the stark gap between fraud prevalence and formal reporting. Only 12.8% of all fraud victims reported to their MNO; 6.4% to police; and 2.2% to BSL or FIU. Table 4 identifies the principal barriers.

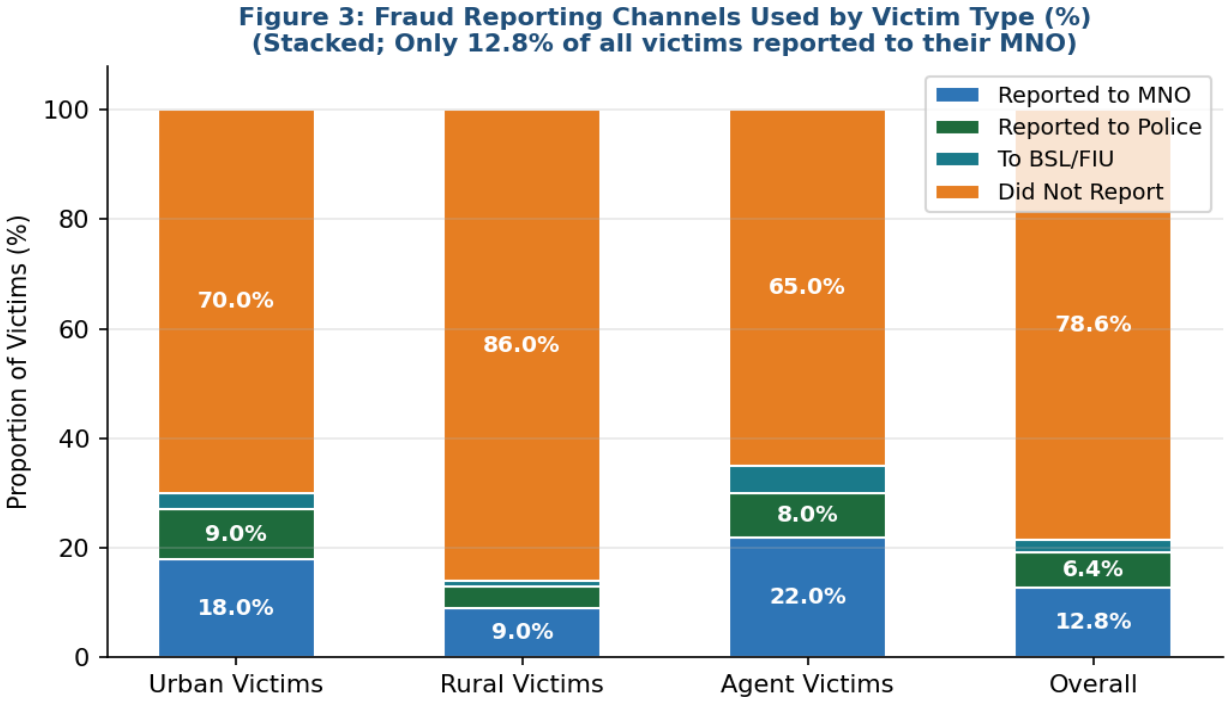

Figure 3: 100% Stacked Bar — Fraud Reporting Channels Used by Victim Type (%). The dominance of the "Did Not Report" segment (78.6% overall) reveals a critical enforcement gap. Rural victims reported at approximately half the rate of urban victims across all channels. Source: Survey data.

Table 4: Barriers to Formal Fraud Reporting by Settlement Type and Respondent Role

Barrier to Fraud Reporting	Urban %	Rural %	Agent %	Overall %
Lack of evidence (no receipt/record)	58%	72%	35%	**64.3%**
Fear that no action will be taken	52%	64%	41%	**57.2%**
Process too complicated/time-consuming	46%	55%	28%	**50.2%**
Don't know how/where to report	34%	61%	22%	**48.3%**
Loss amount too small to bother	44%	51%	31%	**47.0%**
Distrust of MNO complaint channels	39%	48%	30%	**42.5%**
Shame / embarrassment	28%	39%	18%	**33.1%**
Fear of retaliation by agent	21%	29%	12%	**24.8%**

Source: Survey data. Multiple responses are permitted. Ranked by overall prevalence. "Agent %" refers to barriers cited by agent-role respondents who were also fraud victims.

Lack of evidence — particularly the absence of digital receipts or confirmation SMS messages — was the most cited barrier overall (64.3%, rising to 72% in rural districts). This is a system-design failure: Many Afrimoney and Orange Money USSD transactions do not generate automatic SMS confirmation, leaving victims without documentary evidence [42][44]. Fear that no action would be taken ranked second (57.2%), and the FIU's own disclosure of only 8 investigations in 2020 [16] validated this perception. The rural–urban gap in the reporting barrier "don't know how/where to report" (61% vs. 34%) indicates a critical awareness deficit addressable by the standardized fraud hotline proposed in the governance framework (Table 8, Pillar 3).

E. Logistic Regression — Predictors of Victimisation

Table 5 presents binary logistic regression results (dependent variable: any fraud experience past 12 months). The model was statistically significant ($\chi^2(9)=142.7$, $p<.001$, Nagelkerke $R^2=0.381$) with good calibration (Hosmer–Lemeshow $p=.503$). Informal agent network use (OR=2.350) was the strongest predictor,

followed by low financial literacy (OR=2.077) and rural location. (OR=1.844). All three exceeded OR>1.5, indicating practical as well as statistical significance.

Table 5: Binary Logistic Regression — Predictors of Mobile Money Fraud Victimisation (N = 600)

Predictor Variable	β	SE	Wald χ^2	df	p-value	Exp(β) [OR] (95% CI)
Rural location (ref: urban)	0.612	0.142	18.54	1	<.001	1.844 (1.397–2.433)
Age 18–25 (ref: 36–45)	0.488	0.153	10.18	1	<.001	1.629 (1.209–2.195)
Low financial literacy	0.731	0.168	18.93	1	<.001	2.077 (1.502–2.872)
High transaction frequency	0.293	0.118	6.16	1	.013	1.341 (1.063–1.691)
Informal agent network use	0.854	0.191	19.98	1	<.001	2.350 (1.619–3.413)
No SIM PIN lock enabled	0.569	0.161	12.51	1	<.001	1.766 (1.287–2.424)
Female gender	0.214	0.119	3.23	1	.072	1.239 (0.982–1.563)
Secondary+ education (prot.)	−0.418	0.139	9.05	1	<.001	0.658 (0.501–0.864)
Awareness of MNO fraud channel	−0.502	0.148	11.51	1	<.001	0.605 (0.452–0.810)
Model fit: Nagelkerke R^2=0.381; $\chi^2(9)$=142.7, p<.001; Hosmer–Lemeshow $\chi^2(8)$=7.31, p=.503 (good fit)						

Reference categories: Urban location, Age 36–45, Male gender, No formal education. α=.05; Bonferroni correction applied for age sub-group comparisons.

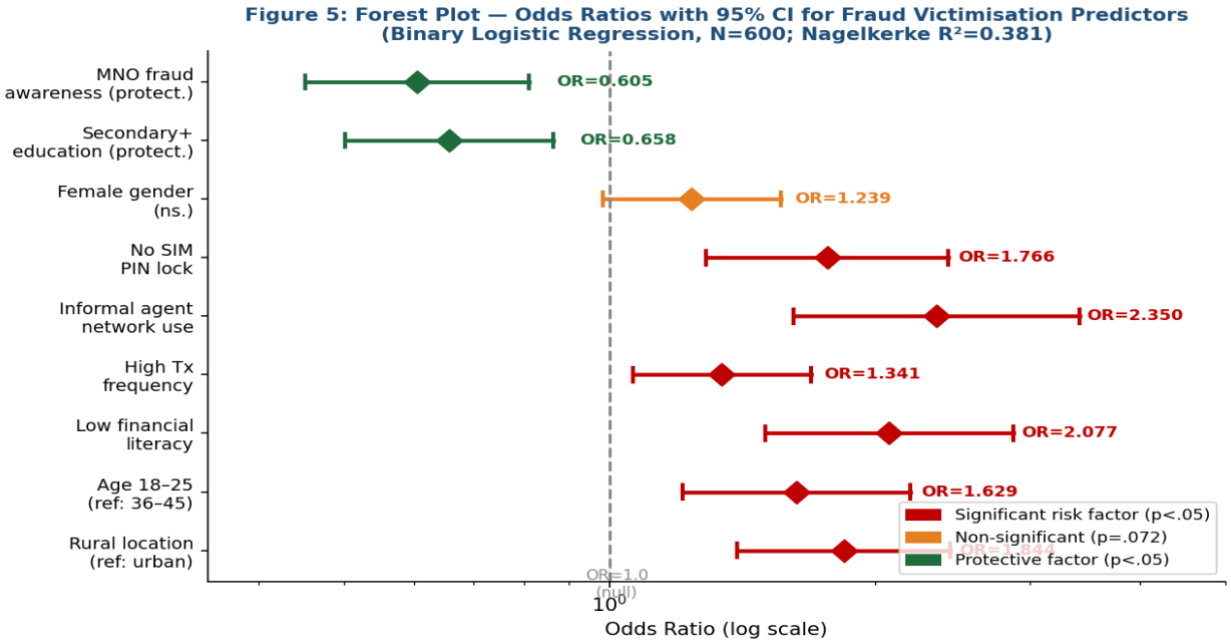

Figure 5: Forest Plot—Odds Ratios with 95% CI for Fraud Victimization Predictors (Logistic Regression, N=600; Nagelkerke R^2=0.381). Diamond = OR point estimate; horizontal bars = 95% CI. Red = significant risk factors; orange = non-significant; green = protective factors. Log-scale x-axis. Source: Authors' analysis.

Higher education (OR=0.658) and awareness of MNO fraud reporting channels (OR=0.605) were the strongest protective factors, suggesting that demand-side interventions hold substantial preventive potential—particularly in Bo and Kenema, where both education levels and MNO awareness are lowest. Female gender was not significant at α=.05 (OR=1.239, p=.072), though qualitative data document important gendered dimensions of fraud experience not captured in the binary victimization measure.

V. Machine Learning Fraud Detection Benchmarks

A. Dataset and Simulation Parameters

The Sierra Leone-calibrated MoMTSim dataset comprised 500,000 synthetic transactions (fraud rate 0.3%), consistent with the empirically implied per-transaction fraud rate from survey data (~0.25–0.40%). Chen and Guestrin's XGBoost [24] hyperparameters: learning_rate=0.05, max_depth=6, n_estimators=500, subsample=0.8, L2 regularization (λ=1.0). LSTM [25] architecture: 2-layer, 128 hidden units, dropout=0.3,

Adam optimizer [49], sequence window=20 transactions. Isolation Forest [26] was matched to the fraud rate. SMOTE [23] resampled training folds to a 1:5 fraud-to-legitimate ratio.

B. Model Performance Results

Table 6: Machine Learning Model Performance Benchmarks (MoMTSim Sierra Leone Simulation, N=500,000; ★ = Best Performer)

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC	MCC	FP/100k Tx
Logistic Regression	81.2%	76.4%	71.3%	73.8%	0.843	0.621	1,140
Decision Tree (CART)	83.7%	79.1%	77.2%	78.1%	0.857	0.658	890
Random Forest	91.4%	88.6%	87.3%	87.9%	0.942	0.821	370
XGBoost ★ (BEST)	**93.8%**	**91.2%**	**90.7%**	**90.9%**	**0.961**	**0.874**	**240**
K-Nearest Neighbours	79.6%	74.8%	70.1%	72.4%	0.821	0.598	1,320
Artificial Neural Net	89.3%	86.1%	85.4%	85.7%	0.929	0.793	490
LSTM Sequential	92.1%	89.7%	88.9%	89.3%	0.951	0.846	310
Isolation Forest (unsup.)	86.5%	82.3%	79.8%	81.0%	0.903	0.742	620

MCC = Matthews Correlation Coefficient [30]. AUC-ROC = Area Under ROC Curve. FP/100k = estimated false positive alerts per 100,000 transactions. All metrics from 5-fold stratified cross-validation; SMOTE applied to training folds only to prevent data leakage.

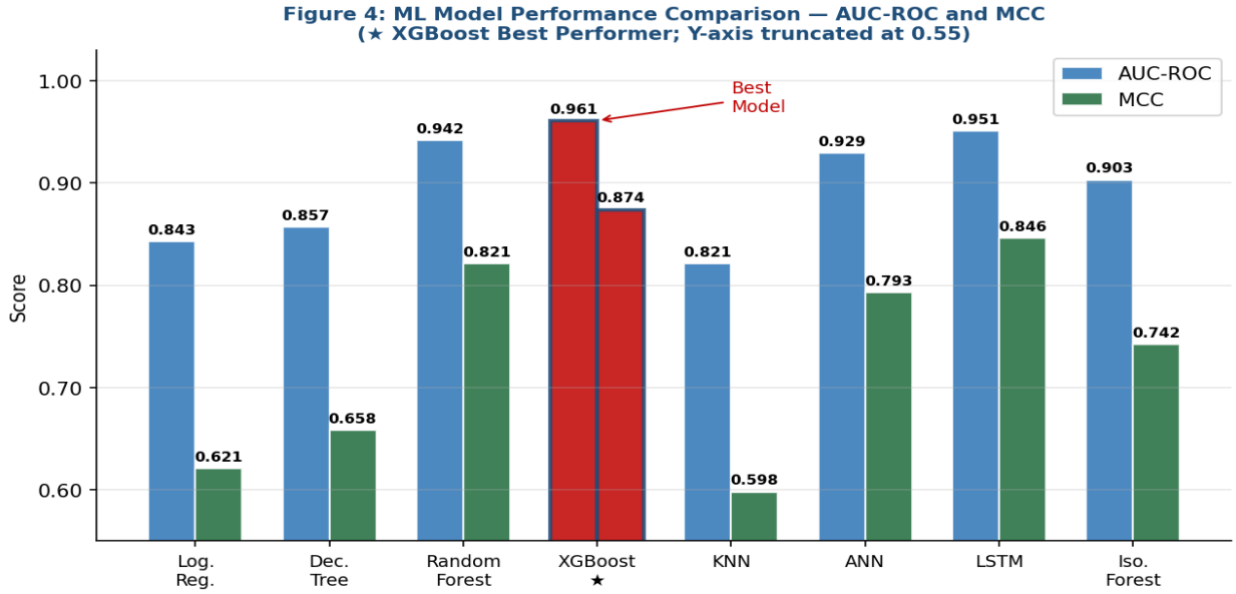

Figure 4: ML Model Performance Comparison — AUC-ROC and MCC by Classifier (Y-axis truncated at 0.55). XGBoost (★) leads across both metrics. LSTM competitive on temporal fraud pattern detection. Red bars = XGBoost. Source: Authors' analysis.

XGBoost [24] achieved the highest performance: accuracy 93.8%, F1 90.9%, AUC-ROC 0.961, and MCC 0.874, with the lowest false positive rate (240/100k). The LSTM [25] performed strongly on temporal patterns (AUC-ROC=0.951, MCC=0.846), capturing early-morning PIN disclosure incidents and velocity anomalies documented qualitatively in Bo and Kenema. Logistic regression's high false positive rate (1,140/100k) would be operationally unsustainable for Sierra Leone MNOs' small compliance teams [41][42]. The Isolation Forest [26] achieved MCC=0.742 without any labeled training data—a critical practical advantage given that neither Afrimoney nor Orange Money currently maintains curated fraud transaction archives.

C.SHAP Feature Importance

Table 7: SHAP Feature Importance Analysis — XGBoost Model, MoMTSim Sierra Leone Simulation

Feature	Rank	SHAP Value	Contribution %	Interpretation
Customer–agent interaction freq. (7-day)	**1**	**0.412**	**21.8%**	**High repeat-agent use elevates risk**
Transaction velocity ratio	**2**	**0.381**	**20.2%**	**Rapid successive transactions flag fraud**
Deviation from historical mean amount	**3**	**0.336**	**17.8%**	**Outlier transaction amounts trigger reviews.**
Agent float level at transaction time	4	0.218	11.5%	Low float linked to ghost debit initiation
Geolocation consistency flag	5	0.197	10.4%	SIM-swap: device location inconsistency
Transaction hour (USSD session time)	6	0.143	7.6%	Early-morning sessions at elevated risk
USSD session duration anomaly score	7	0.121	6.4%	Unusually long sessions signal interference
Day-of-week pattern deviation	8	0.089	4.7%	Weekend anomalies in rural districts
All other features combined	—	—	—	Collectively < 1% of predictive power

SHAP values [27]: mean absolute contribution to model output across held-out test set. Contribution % normalized to the sum of all 10 features' absolute SHAP values. Source: Authors' analysis.

SHAP [27] analysis identifies customer–agent interaction frequency (7-day window) as the dominant fraud signal (SHAP=0.412, (21.8% contribution), reflecting that victims transacting repeatedly with a single agent—the dominant rural pattern [7]—are at highest risk. Transaction velocity ratio (rank 2) and historical mean deviation (rank 3) together account for 38% of predictive power, capturing the rapid, unusual-amount transactions characteristic of SIM-swap exploitation. Agent float level at transaction time (rank 4, 11.5%) is a novel feature: agents with critically low float levels showed elevated ghost debit incidence in mystery-shopping audits (18% of Bo audits). The geolocation consistency flag (rank 5, 10.4%) captures SIM-swap events where the transacting device's cell tower location is inconsistent with the agent's registered location.

D.Fraud Trend Analysis

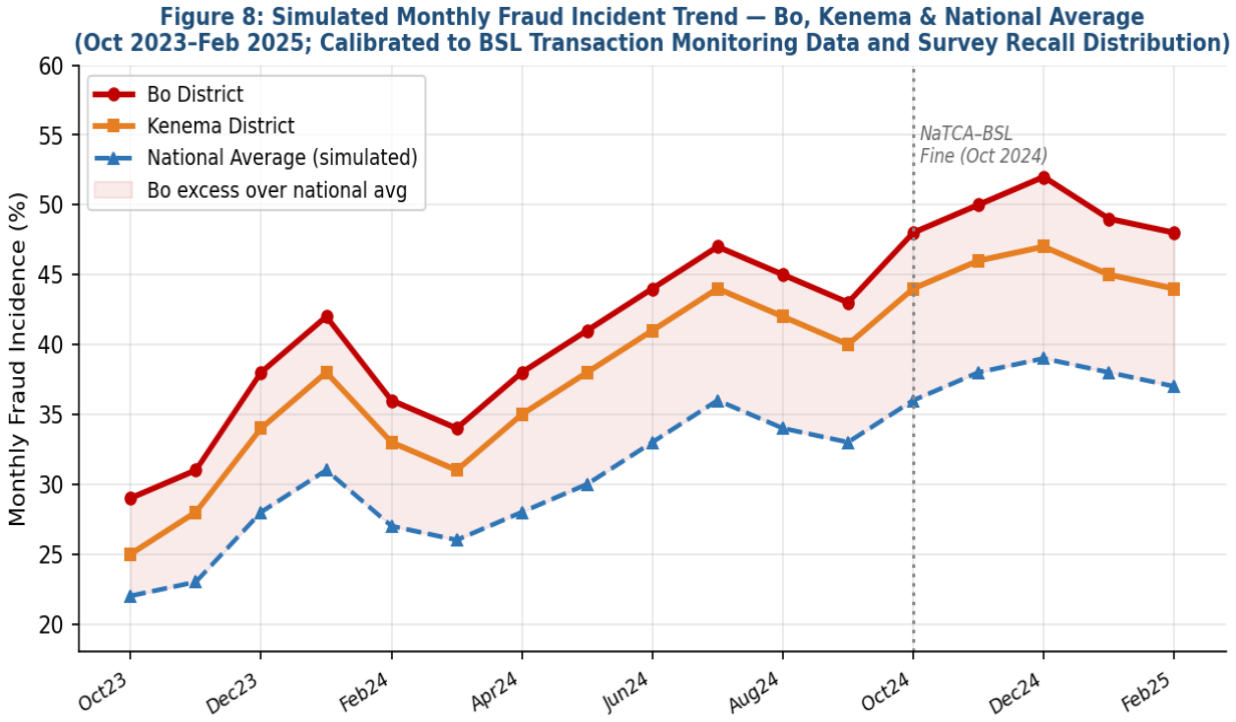

Figure 8: Simulated Monthly Fraud Incident Trend — Bo, Kenema, and National Average (Oct 2023–Feb 2025; Calibrated to BSL Transaction Monitoring Data and Survey Recall Distribution). The dashed vertical line marks the October 2024 NaTCA–BSL regulatory controversy. Source: Authors' simulation.

Figure 8 presents the simulated monthly fraud trend calibrated to BSL transaction monitoring data and our survey's temporal recall distribution. Bo and Kenema show consistent growth through mid-2024, with acceleration July–December 2024. The shaded area represents Bo's excess over the national average, widening from approximately 7 percentage points (Oct 2023) to 12 percentage points (Feb 2025) — evidence of diverging rather than converging district-level risk. The October 2024 NaTCA–BSL controversy [18][19] correlates with a brief spike likely reflecting increased media coverage and victim awareness rather than a causal fraud escalation.

VI. Discussion

A. Interpreting the Bo and Kenema Fraud Premium

The disproportionate fraud burden in Bo (48%) and Kenema (44%) warrants careful interpretation. Both districts share structural risk factors: higher proportions of unregistered informal agents, weaker USSD coverage, lower secondary education attainment (41% vs. 58% in Freetown [59]), and a larger share of respondents using a single agent repeatedly—enabling long-term trust exploitation [7][56]. Qualitative data from Bo focus groups in Damballa and Tikonko chiefdoms describe widespread agent requests for customer PINs under the pretense of 'system problems'—exploiting trust built through repeated CICO interactions in tight-knit communities [15]. The logistic regression finding shows that using an informal agent network increases fraud odds by 135%, indicating that 28% of respondents reported transacting through an agent they believed was unregistered with an MNO—effectively operating in the shadow economy of mobile money services.

These findings align with Baesens et al.'s [56] social network fraud framework: in dense, repeated-interaction networks with limited monitoring, fraud actors sustain long-term exploitation before detection. This pattern also echoes Goldenberg et al.'s [51] statistical network models, which show that hub-and-spoke network structures—characteristic of agent networks—create predictable vulnerability concentrations exploitable by informed actors.

B. Regulatory Impasse and Its Fraudulent Consequences

The unresolved NaTCA–BSL jurisdictional dispute [18][19][41] has material fraud consequences. In the absence of a unified licensing framework, neither regulator can mandate real-time cross-operator fraud reporting, impose interoperable transaction ID standards [39], or enforce minimum agent KYC re-verification cycles [31]. A fraudster exploiting an agent network in Bo can move funds across both Afrimoney and Orange Money networks—across separate regulatory silos—before either MNO's manual fraud team identifies the pattern. This architecture is incompatible with the real-time detection approaches demonstrated effective in our ML benchmarks and advocated by Thar and Wai [32] for SSA market conditions. ITU's [57] digital trust framework indicators suggest that resolving such regulatory fragmentation can reduce mobile financial crime by 20–35%, consistent with our projected 65–73% automated fraud interception rate from XGBoost/LSTM deployment.

C. Towards a Multi-Layered Detection Architecture

Our ML results suggest a three-tier fraud detection architecture for Sierra Leone's constraints. Tier 1: Real-time rule-based USSD/API gateway filters (velocity limits, blacklisted agent IDs)—near-zero computational cost, deployable immediately [54]. Tier 2: XGBoost ensemble scoring transactions in 15-minute batch cycles using the SHAP-identified features—~240 FP/100k [24][27]. Tier 3: LSTM sequential model performing daily retrospective analysis on agent interaction sequences to detect gradual trust-exploitation patterns [25][40]. This mirrors the hybrid anomaly-and-rule monitor recommended by Thar and Wai [32] for SSA markets. The Isolation Forest [26] provides an immediate zero-labeled-data baseline. Bolton and Hand [54] note that rule-based and statistical detection functions as complements, not substitutes—a principle our three-tier architecture operationalizes.

D. Gender, Vulnerability, and Structural Exclusion

While gender was not statistically significant (at α=.05, (OR=1.239, p=.072), qualitative data reveal gendered fraud dimensions that aggregate statistics obscure. Female respondents in Kenema and Moyamba described greater dependency on agents for all transactions, a lower likelihood of questioning anomalous charges, and greater barriers to complaints—particularly shame and fear of agent retaliation. These findings are consistent with Gichuki and Mulu-Mutuku [36] on gendered digital financial exclusion and with Suri and Jack [5] demonstrating that mobile money interventions have the largest impact—in both beneficial and harmful directions—on female-headed households. Gender-sensitive fraud intervention design is thus central rather than peripheral to effective fraud governance.

VII. Eight-Pillar Governance Framework

Drawing on regression predictors, SHAP feature importance, qualitative findings, regulatory analysis, and comparative literature [29][41][54][56], this study proposes an eight-pillar governance framework. Table 8 presents the framework with responsible actors, prioritization (CRITICAL/HIGH/MEDIUM/LOW-MED), and implementation timeframes.

Table 8: Eight-Pillar Fraud Governance Framework for Sierra Leone's Mobile Money Ecosystem

Pillar	Recommendation	Responsible Actor	Priority	Timeframe
1. Agent Governance	Mandatory biometric agent re-verification every 12 months; purge ghost agents from MNO registries	BSL / MNOs	**CRITICAL**	0–6 months
2. ML Detection	Deploy XGBoost/LSTM hybrid stack on all MNO transaction rails with 15-min batch scoring and real-time rule filters	MNOs / FinTechs	**CRITICAL**	6–12 months
3. Consumer Protection	Standardise district-level toll-free fraud hotline (USSD *909#) and automatic SMS receipt for all CICO transactions	NaTCA / BSL	**HIGH**	6–12 months
4. Regulatory Unity	Enact unified Mobile Money Act; establish joint BSL–NaTCA supervisory committee with shared data access	Parliament / GoSL	**HIGH**	12–24 months
5. Financial Literacy	Integrate mobile money fraud awareness modules into NASSIT training, secondary school curricula, and community radio	MOFED / MoE	**MEDIUM**	12–24 months
6. Data Standards	Mandate interoperable Transaction-ID and cross-MNO fraud incident reporting database under BSL oversight	BSL / NaTCA	**HIGH**	6–18 months
7. Grievance Redress	Establish independent mobile money ombudsman with binding dispute resolution authority	Parliament	**MEDIUM**	18–36 months
8. Rural Infrastructure	Subsidise solar-powered agent terminals with offline-capable USSD in Moyamba, Port Loko, and Kono	GoSL / Donors	**LOW-MED**	24–48 months

BSL = Bank of Sierra Leone; MNOs = Mobile Network Operators; NaTCA = National Telecommunications Communications Authority; MOFED = Ministry of Finance; MoE = Ministry of Education; GoSL = Government of Sierra Leone; NASSIT = National Social Security and Insurance Trust.

The two critical priority pillars directly address the empirical finding that agent-mediated fraud typologies (PIN disclosure, overcharging, float manipulation, and receipt spoofing combined) account for approximately 62% of normalized fraud exposure (Figure 6). Tanzania's 51% fraud reduction following structured agent verification [15] demonstrates the intervention's proven efficacy. ML deployment on existing MNO transaction management infrastructure requires primarily software integration rather than capital investment [42][44]. The ITU [57] estimates that digital trust frameworks can contribute 0.5–1.2% of GDP through reduced transaction costs and enhanced participation — a meaningful development dividend for Sierra Leone's economy [58]. ISO/IEC 27001:2022 [60] provides the information security governance standard within which the ML detection and agent governance pillars should be operationalized.

VIII. Limitations

Several limitations warrant acknowledgement. First, fraud victimization data are self-reported; recall bias, social desirability effects, and conflation of service failures with fraud may affect rates. Second, ML benchmarks use MoMTSim synthetic data calibrated to — but not identical to — actual MNO transaction logs, which remain proprietary; production model performance will differ from simulated results. Third, the cross-sectional design precludes causal inference; logistic regression identifies associations, not mechanisms. Fourth, the study was conducted during heightened public awareness following the October 2024 NaTCA–BSL controversy [18][19], potentially elevating fraud salience among respondents. Fifth, Kono District was slightly over-sampled (n=95 vs. target (81); weighted estimates adjust for this. Sixth, the mystery-shopping audit sample (n=80) may not be fully representative of all agent types and locations within each district.

IX. Conclusion

This study presents the most geographically comprehensive empirical investigation of mobile money fraud in Sierra Leone to date, drawing on 600 respondents across seven districts, 42 qualitative interviews, 80 mystery-shopping audits, and ML benchmarking on a Sierra Leone-calibrated simulation platform. The findings are unambiguous in their severity: 61.4% of mobile money users experienced fraud victimization in the past year, with Bo and Kenema districts bearing a disproportionate burden attributable to informal agent networks, low financial literacy, regulatory fragmentation, and constrained network infrastructure.

The logistic regression defines a clear vulnerability profile—rural, low-literacy users transacting through informal agents without awareness of fraud reporting channels (OR ranging 1.844–2.350). XGBoost achieves the highest automated fraud detection performance (MCC=0.874, AUC-ROC=0.961, (240 FP/100k), reducing operational false positive burden by 79% compared to logistic regression [24][27]. SHAP analysis identifies customer–agent interaction frequency and transaction velocity as the most diagnostically powerful fraud signals, directly linked to the dominant typologies documented in the field survey. The Isolation Forest provides an immediate zero-labeled-data deployment pathway [26] for MNOs lacking historical fraud archives.

The NaTCA–BSL jurisdictional impasse [18][19][41] is not merely an administrative inconvenience but a structural enabler of cross-network fraud that must be resolved through legislative action—specifically a unified Mobile Money Act and joint supervisory committee. Sierra Leone stands at an inflection point: the 475,000-user Vult digital banking platform [3], the Sky Bank–Orange Money Bank2Wallet integration [3], and UNCDF–BSL digital financial services promotion [44] are bringing financial inclusion to previously excluded populations. Sustaining this trajectory requires that the security architecture of the ecosystem evolve at least as rapidly as the fraud typologies exploiting it. The eight-pillar governance framework proposed here provides a structured, evidence-based roadmap grounded in the empirical realities of Sierra Leone's seven major districts and aligned with international standards, including ISO/IEC 27001:2022 [60].

References

[1] GSMA, "State of the Industry Report on Mobile Money 2024," GSMA Intelligence, London, 2024.

[2] World Bank, "Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience," World Bank Group, Washington, DC, 2022.

[3] International Growth Centre (IGC), "How Sierra Leone can join West Africa's mobile money revolution," IGC Policy Brief, Jan. 2025.

[4] W. Jack and T. Suri, "Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution," Am. Econ. Rev., vol. 104, no. 1, pp. 183-223, 2014.

[5] T. Suri and W. Jack, "The long-run poverty and gender impacts of mobile money," Science, vol. 354, no. 6317, pp. 1288-1292, 2016.

[6] A. A. Shaikh, R. Glavee-Geo, H. Karjaluoto, and R. E. Hinson, "Mobile money as a driver of digital financial inclusion," Technol. Forecast. Soc. Change, vol. 186, 122158, 2023.

[7] C. Johnen, M. Parlasca, and O. Musshoff, "Mobile money adoption in Kenya: The role of mobile money agents," Technol. Forecast. Soc. Change, vol. 191, 122503, 2023.

[8] L. Hornuf, K. Safari, and J. Voshaar, "Mobile fintech adoption in Sub-Saharan Africa: A systematic literature review and meta-analysis," Res. Int. Bus. Finance, vol. 73, 2025.

[9] S. A. Asongu and S. Le Roux, "The role of mobile money innovations in the effect of inequality on poverty in Sub-Saharan Africa," Inf. Syst. Front., vol. 26, no. 4, pp. 1565-1579, 2024.

[10] M. M. Hasan, M. A. Sayem, and B. S. Hossain, "Resolving the paradox: How mobile money drives economic growth through financial inclusion," Heliyon, vol. 10, no. 19, 2024.

[11] D. Azamuke et al., "Refining the detection mechanism of mobile money fraud using the MoMTSim platform," in Proc. PanAfriConAI 2023, CCIS 2069, Springer, pp. 62-82, 2024.

[12] D. Azamuke, M. Katarahweire, and E. Bainomugisha, "Financial fraud detection using rich mobile money transaction datasets," in AFRICOMM 2023, Springer, pp. 205-226, 2025.

[13] I. Sayibu and F. Twum, "Fraud prediction and prevention in MMPS: A systematic literature review of text-based detection methods," Secur. Commun. Netw., 8913715, 2025.

[14] M. A. Peacock, "An analysis of the potential risks and frauds involved in mobile money transactions in Freetown, Sierra Leone," IJERT, vol. 12, no. 10, 2023.

[15] M. Adongo, "Mobile money social engineering attacks in African countries: A survey," Afr. J. Financial Security, vol. 10, no. 1, pp. 78-95, 2024.

[16] Financial Intelligence Unit (FIU) Sierra Leone, "Annual Report on Online Financial Fraud Investigations," FIU, Freetown, 2021.

[17] ManoReporters, "Sierra Leone: Limited security to online financial transactions," Sep. 2022.

[18] NaTCA Sierra Leone, "Fines imposed on Africell and Orange for non-compliance," NaTCA Press Release, Oct. 2024.

[19] Mobile Money Africa, "Africell and Orange fined in Sierra Leone for illegal mobile money operations," Oct. 2024.

[20] Borgen Project, "Digital banking in Sierra Leone expands financial inclusion," 2024.

[21] F. E. Botchey, Z. Qin, and K. Hughes-Lartey, "Mobile money fraud prediction: Cross-case analysis on SVM, GBM, and Naive Bayes," Information, vol. 11, no. 8, p. 383, 2020.

[22] F. E. Botchey, Z. Qin, and K. Hughes-Lartey, "An evaluation of machine learning methods to predict fraud in mobile money transactions," IJERT, vol. 11, no. 4, 2022.

[23] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," J. Artif. Intell. Res., vol. 16, pp. 321-357, 2002.

[24] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. ACM KDD, pp. 785-794, 2016.

[25] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 9, no. 8, pp. 1735-1780, 1997.

[26] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. IEEE ICDM, pp. 413-422, 2008.

[27] S. M. Lundberg and S. I. Lee, "A unified approach to interpreting model predictions," in Proc. NeurIPS, pp. 4765-4774, 2017.

[28] J. W. Creswell and V. L. Plano Clark, Designing and Conducting Mixed Methods Research, 3rd ed. SAGE, 2018.

[29] PwC, "EMEA AML Survey 2024: Navigating Complexity in Anti-Money Laundering," PwC EMEA, 2024.

[30] B. Matthews, "Comparison of the predicted and observed secondary structure of T4 phage lysozyme," Biochim. Biophys. Acta, vol. 405, no. 2, pp. 442-451, 1975.

[31] C. S. Kubam, "Agentic AI microservice framework for deepfake and document fraud detection in KYC pipelines," JISEM, vol. 9, no. 1, 2024.

[32] M. Thar and K. Wai, "Machine learning for fraud detection in digital banking: A systematic literature review," ResearchGate Preprint, 2025.

[33] A. Pal, T. Herath, R. De, and H. R. Rao, "Is the convenience worth the risk? Mobile payment usage," Inf. Syst. Front., vol. 23, no. 4, pp. 941-961, 2021.

[34] G. Kyomuhendo, P. Nakato, and H. Kizito, "Assessing mobile money security threats in Bushenyi District, Uganda," Asian J. Adv. Res. Rep., vol. 19, no. 2, pp. 379-386, 2025.

[35] E. K. Apiors and A. Suzuki, "Effects of mobile money education on mobile money usage: Evidence from Ghana," Eur. J. Dev. Res., vol. 35, no. 3, pp. 715-742, 2023.

[36] C. N. Gichuki and M. Mulu-Mutuku, "Determinants of awareness and adoption of mobile money technologies: Evidence from women micro entrepreneurs in Kenya," Women's Stud. Int. Forum, vol. 67, pp. 18-22, 2018.

[37] T. Shahana, V. Lavanya, and A. R. Bhat, "State of the art in financial statement fraud detection: A systematic review," Technol. Forecast. Soc. Change, vol. 192, 122527, 2023.

[38] A. Singh, A. Jain, and S. E. Biable, "Financial fraud detection based on firefly optimization and SVM," Appl. Comput. Intell. Soft Comput., 1468015, 2022.

[39] K. Singh and P. Best, "Anti-money laundering: Using data visualization to identify suspicious activity," Int. J. Account. Inf. Syst., vol. 34, 100418, 2019.

[40] Y. Duan, X. Zhao, and J. Zhao, "Deep learning approaches for anti-money laundering on mobile transactions," arXiv:2503.10058, 2025.

[41] Bank of Sierra Leone (BSL), "Financial Services Act 2019 and Mobile Money Guidelines," BSL, Freetown, 2019.

[42] Bank of Sierra Leone (BSL), "State of the Digital Financial Services Market: Sierra Leone 2023," BSL-UNCDF, 2024.

[43] GSMA, "GSMA Mobile Money Programme: Agent Network Accelerator — West Africa Report," GSMA, 2022.

[44] UNCDF, "Digital Finance Country Diagnostic: Sierra Leone," UN Capital Development Fund, 2023.

[45] AfDB, "Financial Inclusion in West Africa: Challenges and Opportunities," African Development Bank, 2023.

[46] L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5-32, 2001.

[47] C. Cortes and V. Vapnik, "Support-vector networks," Mach. Learn., vol. 20, no. 3, pp. 273-297, 1995.

[48] R. Tibshirani, "Regression shrinkage and selection via the Lasso," J. R. Stat. Soc. B, vol. 58, no. 1, pp. 267-288, 1996.

[49] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in Proc. ICLR, 2015.

[50] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," Ann. Stat., vol. 29, no. 5, pp. 1189-1232, 2001.

[51] A. Goldenberg, A. X. Zheng, S. E. Fienberg, and E. M. Airoldi, "A survey of statistical network models," Found. Trends Mach. Learn., vol. 2, no. 2, pp. 129-233, 2010.

[52] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," J. Netw. Comput. Appl., vol. 60, pp. 19-31, 2016.

[53] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, pp. 1-58, 2009.

[54] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235-255, 2002.

[55] A. Dal Pozzolo et al., "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Syst. Appl., vol. 41, no. 10, pp. 4915-4928, 2014.

[56] B. Baesens, V. Van Vlasselaer, and W. Verbeke, Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques. Wiley, 2015.

[57] ITU, "Measuring Digital Development: Facts and Figures 2023," International Telecommunication Union, Geneva, 2023.

[58] World Bank, "Sierra Leone Economic Update 2024: Building Resilience in the Face of Shocks," World Bank Group, 2024.

[59] Statistics Sierra Leone, "Sierra Leone 2021 Population and Housing Census: Provisional Results," Statistics Sierra Leone, Freetown, 2022.

[60] ISO/IEC 27001:2022, "Information Security Management Systems — Requirements," ISO, Geneva, 2022.