



REQUEST FOR PROPOSAL FOR AML & Fraud Monitoring TOOL

1. Background

MMRL intends to appoint a suitably qualified and technologically mature technology partner to provide an Enterprise Fraud Management, Monitoring, Detection, Prevention, Investigation, Case Management, AML/CFT, Sanctions Screening and Financial Crime Risk Management Platform capable of supporting multiple FinTech, GSM, Mobile Money, digital financial-services and business operations with experience over twenty years within the fintech business.

The proposed platform must incorporate advanced machine learning, artificial intelligence, behavioural analytics, graph/network analytics, entity resolution, anomaly detection, risk-based decisioning and explainable AI capabilities as native components of the solution.

The solution must not be limited to conventional static rule-based transaction monitoring. Vendors shall demonstrate the ability to identify known, unknown, emerging, coordinated and previously unseen fraud and financial-crime patterns across customers, employees, agents, merchants, dealers, partners, devices, SIMs, accounts, wallets, beneficiaries, transactions and channels.

The platform shall provide a single enterprise financial-crime risk view capable of correlating fraud, AML/CFT, sanctions, insider risk, cyber-enabled fraud, customer behaviour and ecosystem relationships.

The solution should support both centralised Enterprise governance and decentralised business-unit configuration, allowing individual operating units to configure local risk parameters, market dynamics, regulatory requirements, fraud scenarios, AML/CFT typologies, sanctions requirements, thresholds and operating procedures while maintaining central risk governance.

2. Mandatory Vendor Qualification – Pass/Fail

Failure to satisfy any mandatory requirement below should result in disqualification from technical evaluation.

2.1 Native AI/ML Capability

The vendor must demonstrate that AI/ML capabilities are native to the proposed platform and are not dependent on a third-party product that is separately procured and integrated.

The vendor must demonstrate production deployments where machine learning is actively used for fraud or financial-crime detection.

The Vendor shall provide:

- At least 15 reference implementations of comparable scale with other businesses.
- Evidence of production use of ML models.
- Description of algorithms used.
- Model performance metrics.
- Model governance framework.
- Model validation methodology.
- Model monitoring capabilities.
- Evidence of model retraining.
- Evidence of handling model drift.
- Marketing statements such as "AI-powered" or "machine-learning enabled" without demonstrable production evidence shall not be accepted.

3. Advanced Machine Learning Requirements

The platform must support multiple analytical approaches rather than only relying on a single algorithm.

3.1 Supervised Machine Learning

The platform should support models including, but not limited to:



- Logistic Regression.
- Random Forest.
- Gradient Boosting.
- XGBoost/LightGBM or equivalent.
- Decision Trees.
- Neural Networks.
- Deep Learning where justified.
- Ensemble models.
- The vendor must demonstrate how models can distinguish transactions using historical labelled data.

3.2 Unsupervised Machine Learning

The platform must detect previously unknown fraud patterns without requiring predefined fraud rules and required capabilities should include:

- Clustering.
- Outlier detection.
- Isolation Forest or equivalent.
- Autoencoders or equivalent anomaly-detection models.
- Behavioural deviation analysis.
- Peer-group analysis.
- Population profiling.
- Unusual transaction sequence detection.
- This is particularly important for detecting new fraud typologies and emerging social-engineering schemes.

4. Behavioural Analytics

The platform must create dynamic behavioural profiles for:

- Customers
- Service providers.
- Agents.
- Merchants.
- Dealers.
- Employees.
- Devices.
- SIMs.
- Wallets.
- Accounts.
- Beneficiaries.



- Channels.

The system should establish a normal behavioural baseline and identify deviations.

The platform should dynamically increase the risk score without requiring a separate static rule for every combination.

5. Graph & Network Machine Learning

This should be a mandatory requirement rather than an optional feature and the platform must provide graph-based analysis capable of identifying relationships. This system must identify:

- Fraud rings.
- Mule networks.
- Agent and service provider collusion.
- Employee/customer collusion.
- Shared devices.
- Shared identifiers.
- Common beneficiaries.
- Common addresses.
- Common IP addresses.
- Common locations.
- Transaction networks.
- Circular movement of funds.
- Rapid movement across multiple accounts.

Hidden relationships. The system should identify the relationship as a potentially coordinated network even where each individual transaction appears legitimate.

6. Entity Resolution

The platform must provide advanced entity-resolution capability to determine when different records may relate to the same underlying wallet or delivery channel.

This should correlate:

- Customer names.
- Phone numbers.
- IDs/passports/TINs.
- Wallets.
- Accounts.
- Devices.
- SIM cards.
- IP addresses.
- Email addresses.
- Addresses.



- Beneficiaries.
- Agents.
- Merchants.
- Service providers
- Aggregators
- Employees.

The platform should identify relationships despite variations in customer information.

7. Real-Time Risk Decision Engine

The platform must support real-time transaction and activity decisioning with configurable outcomes:

- Allow Monitoring
- Step-up authentication
- Hold
- Reject
- Block
- Refer for investigation

The risk engine should combine features not limited to; Rules, Machine Learning score, credit scoring risks, behavioural score, graph score, sanctions screening risk, AML risk, customer risk, device risk, transaction risk...into an overall enterprise risk score.

8. Dynamic Risk Scoring

Risk scores must not be based solely on transaction value; the model should consider multiple dimensions not limited to...

Risk Dimension	Example
Customer behaviour	Deviation from normal behaviour
Transaction	Unusual value/frequency
Device	New or high-risk device
SIM Swap...	Recent SIM replacement
Location	Abnormal location
Beneficiary	Newly created beneficiary
Agent	High-risk agent
Merchant	High-risk merchant
Employee	Suspicious internal access
Network	Association with known fraud
AML	High-risk transaction pattern
Sanctions	Potential sanctions match
Historical risk	Previous incidents
Velocity	Multiple transactions rapidly
Channel	High-risk channel

The platform must support dynamic risk scoring based on multiple concurrent signals.

9. Concept Drift & Emerging Fraud Detection

This should be a mandatory advanced requirement; Fraud patterns change over time. The platform must detect concept drift, including changes in:

- Customer behaviour.
- Fraudster behaviour.



- Transaction patterns.
- Agent behaviour.
- Channel behaviour.
- Geographic fraud concentration.
- Fraud typologies.
- AML/CFT trends.
- Sanction lists.

The system should alert Fraud/AML/CFT/Risk Management when a model's performance deteriorates or when new behavioural patterns emerge.

10. Continuous Model Learning

The solution should support features not limited to;

- Automated model retraining.
- Controlled model retraining.
- Champion/challenger models.
- Model versioning.
- Model rollback.
- Model performance monitoring.
- Data-quality monitoring.
- Feature monitoring.
- Drift detection.
- False-positive monitoring.
- False-negative monitoring.

A vendor should not be allowed to deploy an Machine Learning model and then require the business to wait for the vendor's next annual software release to improve it.

11. Explainable AI

Every AI-generated alert must provide an understandable explanation of why the transaction/entity was considered high risk.

- Risk Score: 98/100
- SIM swap changed in real time.
- New device detected
- New beneficiary created
- Transaction value certain configurable % customer wallet average
- Beneficiary associated with previous fraud case
- Transaction location inconsistent with customer history
- Device associated with 4 or other more customer accounts



The system must provide feature-level explainability and maintain an audit trail supporting regulatory and investigation requirements.

12. False Positive & False Negative Optimisation

The vendor must demonstrate how the system minimises:

- False positives.
- False negatives.
- Alert duplication.
- Alert fatigue.
- Unnecessary case creation.

The vendor must provide measurable performance metrics not limited to,

- Precision.
- Recall.
- F1 Score.
- ROC-AUC where applicable.
- Detection rate.
- False-positive rate.
- False-negative rate.
- Alert-to-case conversion.
- Fraud prevented.
- Average detection latency.
- Risk classification of the customer base, delivery channels and geographical business coverage to High, Medium and Low.

Vendors should be required to demonstrate these metrics using the business identified data during the PoC.

13. AML/CFT Advanced Monitoring

The solution must support risk-based AML/CFT transaction monitoring, not limited to,

- Structuring.
- Smurfing.
- Rapid movement of funds.
- Circular transactions.
- Layering.
- Unusual cash activity.
- Dormant account activity.
- Unusual cross-border transactions/activity.
- High-risk customer activity.
- Unusual velocity.

Mobile Money Rwanda Ltd
MTN Centre,
Nyarutarama, P.O. Box 1170, Kigali, Rwanda
Tel: (+250) 788327777
Company Code: 113464257



- Multiple accounts controlled by related entities.
- Funnel accounts.
- Mule accounts.
- Unusual agent activity.
- Unusual merchant activity.

The system must support configurable AML/CFT typologies without requiring vendor professional services for every new scenario or any other adjustments.

14. Sanctions Screening

The solution should support screening All customer and wallet categories within our base;

- Customers.
- Beneficiaries.
- Agents.
- Merchants.
- Dealers.
- Employees.
- Partners.
- Companies/entities.
- This should also support features not limited to,
- Fuzzy matching.
- Phonetic matching.
- Alias detection.
- Transliteration.
- Name variation.
- Date-of-birth matching.
- Nationality.
- Country.
- Identification numbers.
- Address matching.

The platform should provide configurable matching thresholds and allow investigators to distinguish true matches, false positives and potential matches.

15. Social Engineering Detection

The platform should have a dedicated social-engineering risk model correlating to scenarios not limited and automatically generate a composite risk score.

- Customer impersonation.
- Fake reversal requests.



- Account takeover.
- SIM-swap followed by transaction.
- Customer-profile manipulation.
- Employee-assisted fraud.
- Agent-assisted fraud.
- Customer/employee collusion.
- Unusual customer-care interactions.
- Any market trends.

16. Insider Risk Analytics

- The platform must monitor employee behaviour using risk-based analytics.
- Excessive customer searches and views of the customer wallets.
- Unusual access patterns.
- Access outside working hours.
- Access to VIP/high-value customers.
- Access without subsequent operational justification.
- Customer-data access before fraudulent activity.
- Repeated access to the same customers.
- Unusual employee/agent relationships.
- Privileged-user activity.
- Administrative manipulation.

The platform should create an Employee Risk Score based on behavioural patterns rather than simple threshold rules.

17. Fraud Intelligence Graph

The solution must provide an enterprise fraud and AML/CFT sanctions graph allowing investigators to navigate relationships.

The system should identify common entities and provide an investigation view of the entire network. This should support detection of organised fraud and collusion.

18. Advanced Rules Engine

The platform must support:

- Rules.
- Rules chaining.
- Event correlation.
- Sequential events.
- Conditional logic.
- Time-window analysis.
- Thresholds.

Mobile Money Rwanda Ltd
MTN Centre,
Nyarutarama, P.O. Box 1170, Kigali, Rwanda
Tel: (+250) 788327777
Company Code: 113464257



- Dynamic thresholds.
- Risk-score combinations.
- Machine Learning scores.
- Graph scores.
- Behavioural scores.
- Geographic conditions.
- Customer segmentation.
- Risk scoring based on desired period or behavior trends
- Credit scoring

19. Model Governance

The vendor must provide a formal Artificial Intelligence /Machine Learning Model Risk Management Framework covering:

- Model development.
- Model validation.
- Model approval.
- Model deployment.
- Model monitoring.
- Model performance.
- Model drift.
- Model retirement.
- Model versioning.
- Model documentation.
- Explainability.
- Bias testing.
- Data lineage.
- Auditability.

The organisation must retain approval authority over production model deployment.

20. Data Science Workbench

To avoid vendor lock-in, the platform should provide a controlled data-science environment enabling authorised internal data scientists to:

- Create features.
- Develop models.
- Test models.
- Train models.
- Compare models.

Mobile Money Rwanda Ltd
MTN Centre,
Nyarutarama, P.O. Box 1170, Kigali, Rwanda
Tel: (+250) 788327777
Company Code: 113464257



- Back-test models.
- Validate models.
- Deploy approved models.
- Monitor models.

The vendor should provide full system documentation and APIs for model integration.

21. Vendor Independence / Avoiding Black-Box AI

The vendor shall not provide a proprietary "black-box" machine-learning capability where the business cannot understand, validate, monitor, challenge, tune or independently assess the model's performance.

This must disclose:

- Model methodology.
- Model inputs.
- Key features.
- Training methodology.
- Model performance.
- Validation approach.
- Model limitations.
- Model monitoring.
- Retraining methodology.

The business shall retain the right to conduct independent model validation.

22. PoC / Proof-of-Capability – Mandatory

The system should demonstrate the solution using a controlled dataset containing historical or synthetic:

- Fraud transactions.
- Legitimate transactions.
- SIM swaps.
- Customer-care events.
- Device changes.
- Beneficiary changes.
- Agent transactions.
- Employee access events.
- AML scenarios.
- Sanctions screening scenarios.
- The vendor must demonstrate that the platform can;
- Detect known fraud.
- Detect unknown fraud.



- Detect coordinated fraud.
- Detect social engineering.
- Detect insider-assisted fraud.
- Identify fraud networks.
- Generate risk scores.
- Explain alerts.
- Reduce false positives.
- Create investigation cases.
- Detect AML typologies.
- Conduct sanctions matching.
- The PoC results should form part of the technical evaluation score.

23. Minimum Technical Performance Requirements

Requirement	Minimum
Real-time decision latency	≤ 500 ms*
Platform availability	$\geq 99.99\%$
API availability	$\geq 99.99\%$
ML model explainability	Mandatory
Graph analytics	Mandatory
Behavioural analytics	Mandatory
Unsupervised ML	Mandatory
Supervised ML	Mandatory
Model drift detection	Mandatory
Model versioning	Mandatory
Champion/challenger	Mandatory
Real-time scoring	Mandatory
Case management	Mandatory
API integration	Mandatory
Audit trail	Mandatory
Data encryption	Mandatory
DR capability	Mandatory

*The actual latency requirement should be validated against the business transaction volumes and integration architecture rather than imposed blindly.

24. Business Continuity & Resilience

The platform must support,

- High availability.
- Active-active or equivalent architecture where required.
- Disaster recovery.
- Automatic failover.
- Data replication.
- No single point of failure.
- Transaction buffering.



- Recovery after system outage.
- Defined RTO.
- Defined RPO.
- Capacity scaling.
- DR testing.
- Cyber-resilience testing.
- Solution must provide production support and defined SLAs.
- Solution must support secure Local data processing and applicable data protection requirements are fully achieved
- Maker-checker approval before production activation.
- Scenario simulation and back-testing.
- Ability to test new rules against historical data.
- Ability to deploy rules with minimal operational downtime.
- Full audit trail of creation, modification, approval, activation and retirement

For a critical financial transaction monitoring platform, the vendor should demonstrate how fraud controls remain operational when downstream systems or connectivity are degraded.

25. Technology Architecture

The vendor must provide a detailed architecture showing features not limited to Channels → API Gateway → Event Streaming → Data Platform → Fraud/AML Engine → ML Models → Risk Engine → Decision Engine → Case Management → SIEM/SOC → Reporting...

The system solution should support:

- REST APIs.
- Event streaming.
- Message queues.
- Real-time data ingestion both FinTech and GSM.
- Batch ingestion.
- Cloud/hybrid/on-premises deployment as applicable.
- Containerisation.
- Horizontal scaling.
- Microservices where appropriate.

26. Internal Capability Transfer

The vendor shall provide a structured technology and knowledge-transfer programme to ensure that the technology team does not become permanently dependent on the vendor and the vendor must train internal:

- Technology teams.
- Fraud management Teams.
- AML/CFT & Sanctions Teams.

Mobile Money Rwanda Ltd

MTN Centre,

Nyarutarama, P.O. Box 1170, Kigali, Rwanda

Tel: (+250) 788327777

Company Code: 113464257



- Risk Management.
- Training must cover:
- Rule configuration.
- ML model management.
- Model monitoring.
- Dashboard configuration.
- Case management.
- API integration.
- System administration.
- Troubleshooting.
- Data analysis.
- Model validation.

27. L1, L2 and L3 Support

The vendor shall provide:

- L1
- 24/7 monitoring.
- Incident logging.
- First-level troubleshooting.
- Alert/platform availability monitoring.
- L2
- Application support.
- Configuration issues.
- Integration issues.
- Rule-engine issues.
- Performance issues.
- L3
- ML model issues.
- Software defects.
- Advanced technical issues.
- Database/performance optimisation.
- Architecture-level incidents.

The vendor must provide onsite support resources during implementation and the agreed stabilisation period, with a defined transition plan to full internal support teams.



28. Automatic technical disqualification should apply where the bidder cannot demonstrate:

- Native ML/AI.
- Real-time risk scoring.
- Behavioural analytics.
- Unsupervised ML.
- Supervised ML.
- Graph/network analytics.
- Entity resolution.
- Explainable AI.
- Model drift detection.
- Model monitoring.
- Model versioning.
- Champion/challenger modelling.
- Real-time APIs.
- AML/CFT monitoring.
- Sanctions screening.
- Insider-risk analytics.
- Social-engineering detection.
- Integrated case management.
- Audit trails.
- High availability.
- DR capability.
- Data encryption.
- Independent model validation capability.
- Internal knowledge transfer.
- Production reference implementations.
- Most importantly:

The bidder must demonstrate that mandatory capabilities are available and operational in the proposed product at the time of bidding.

- ✓ **RFP Submission deadline: 16th October 2026**
- ✓ **RFP Submission to Procurement2.RW@mtn.com**
- ✓ **Copy Theonest.mugabe@mtn.com; mathias.rwanyonga@mtn.com; eric.kamanzi@mtn.com**

Mobile Money Rwanda Ltd

MTN Centre,

Nyarutarama, P.O. Box 1170, Kigali, Rwanda

Tel: (+250) 788327777

Company Code: 113464257

