**Request for Proposal (RFP)**

**For MIC2**

**Fraud Management**

**Technical Specifications**

**Table of contents**

[1. Technical Specifications 3](#_Toc137212917)

[1.1. General 3](#_Toc137212918)

[1.1.1. Fraud Management System 3](#_Toc137212919)

[2. Fraud Management System Requirements 4](#_Toc137212920)

[2.1. General Requirements 4](#_Toc137212921)

[2.2. Data Acquisition Layer/Mediation Requirements 4](#_Toc137212923)

[2.3. Fraud Types 5](#_Toc137212924)

[2.4. Detection Capabilities 5](#_Toc137212925)

[2.5. Analysis Requirements 5](#_Toc137212926)

[2.6. Users Interfaces 6](#_Toc137212927)

[2.7. Alarms and Alerts Requirements 6](#_Toc137212932)

[2.8. Reporting Requirements 6](#_Toc137212938)

[2.9. Audit logs Requirements 6](#_Toc137212939)

[2.10. Hardware and Software Requirements 7](#_Toc137212940)

[2.11. System Security Requirements 7](#_Toc137212941)

[2.12. Operational Requirements 7](#_Toc137212942)

[2.13. Warranty 7](#_Toc137212943)

[2.14. Financials 7](#_Toc137212944)

[2.15. Performance 7](#_Toc137212945)

[2.16. Easy Configuration and Maintenance 8](#_Toc137212946)

[2.17. Company profile 8](#_Toc137212947)

[2.18. Successful installations at similar environment 8](#_Toc137212948)

[2.19. Future Development/roadmap 8](#_Toc137212949)

[2.20. Implementation timeline 8](#_Toc137212950)

[2.21. Training 8](#_Toc137212951)

[2.22. Support 8](#_Toc137212952)

# 

# Technical Specifications

## General

* Vendor(s) shall include in their offer a detailed BoQ for all relevant Hardware, Software, that are needed to implement Vendor(s)‘s SaaS (Software as a Service) solution at MIC2 premises. Hardware are the responsibility of MIC2.
* Vendor(s)’s submitted proposal, documents, manuals, drawings; etc… must be in English.
* Vendor(s) proposed solution should comply with the RFP requirement. However, RFP is MIC2 basic requirements and the Vendor(s) may include in their proposal value added, cost-effective and OPEX saving features. Vendor value added solutions/features shall be included separately in the main BoQ, detailed in separate section in the technical specification, executive summary, and indicated in the commercial copy.
* Vendor(s) shall consider network scalability in the dimensioning design of the stand-alone and main node systems. This has to be reviewed and agreed upon prior to deployment.
* Vendor(s) solution shall consider redundancy and continuity of service for the stand-alone and main node systems with geographical and traffic sharing.
* Vendor(s) shall consider in the rollout plan minimal outages for the integration of the proposed solution with contingency and recovery plans and procedures.
* Interconnectivity and interoperability with all operational network elements.
* Vendor(s) shall provide the Engineering Services for the above scope (these include transportation, design, installation, commissioning, test, integration, pre/post optimization)
* The proposed solution should be as a SaaS (Software-as-a-Service) basis.
  + **Failure to provide a solution based on OPEX paid monthly as detailed above, this will be considered a disqualification of the vendor from the bidding process. The failure will be considered as a killing factor.**

### Fraud Management System

MIC2 is seeking a Fraud Management system that will support its initiative to establish Fraud Management function and to effective handle optimizing the revenue stream for both Post and Prepaid services by providing, not limited to:

* Bypass Fraud
* International Revenue Sharing Fraud (IRSF)
* Wangiri Fraud
* Roaming Fraud
* etc… (other Frauds provided by the vendor, please list)

# Fraud Management System Requirements

## General Requirements

* The system should run in parallel to all existing operational systems and should not cause any effect or disturbance to any of the business or network processes.
* The system should store all collected Data for minimum 2 months. Data older than 2 month will be backed-up. System database has to have direct integration with standard DB like Oracle or MS-SQL.
* The system should be able to perform reports based on different criteria. Report section must be flexible enough to allow extracting data for ad-hoc reports, but also to provide some standard regular fixed reports
* The system availability should be better than 90%
* The System have to be sized for at-least 10 concurrent users
* The system should provide an Audit Trail that allows monitoring, alarms, logging of user activities, and automatic actions
* The system should be highly scalable to easily accommodate both current and projected volumes of data (e.g., increased traffic)
* The system should be able to do the following levels of summary for analysis purpose:

1- Trending summary (by month/ by week)

2- Analytical summary (by month/ by week/ by day/ by hour)



## Data Acquisition Layer/Mediation Requirements

* The system must provide a mediation with the ability to read data encoded in standard and proprietary data formats encountered with common Network Elements and OSS/BSS. Provide the list of formats supported and not supported
* "The system should support different connection protocols and handle but not limited to the following:

1. TCPIP
2. FTP/SFTP
3. HTTP
4. SOAP
5. Other Industry Standards – Please List

* The system should be able to manage CDRs from different switches with different CDR formats
* The system should be flexible to enable in-house personnel to define new data feeds. Also vendors should commit to provide support for new data feed types as part of their service
* The system must be flexible enough to add relevant fields from the data sources when required without any vendor dependency
* The system must highlight the data sources for which incomplete data are received
* System should be able to do all necessary verification to ensure correct format and content of collected CDR

## Fraud Types

* Bypass Fraud
* SIM Boxes
* Premicells
* GSM/UMTS Gateways
* VoIP Bypass
* Interconnect Fraud
* Third country
* Grey Routing
* Wangiri Fraud
* National and international Roaming fraud and unauthorized GPRS/DATA roaming fraud
* International Revenue Sharing Fraud (IRSF)
* SMS Fraud
* Prepaid Fraud
* Voucher Modification
* Duplicate Voucher Printing
* Signalling Attacks

## Detection Capabilities

* Test Call Services (TCG) performing at-least 20,000 test calls per month
* CDR Analysis
* Signalling Analytics
* Protocol Signature/Pre-Call Detection
* The system should monitor Data usage free of charge on corresponding Rating Group
* The system should monitor usage abnormalities for all types of services.
* The system should support Near Real Time Roaming Data Exchange (NRTRDE).
* The system should support HUR as well
* The system should detect velocity checks (calls made from geographically distant places within a short period of time)
* High usage in local, national, international, premiums rate and roaming calls
* The system should detect and prevent network operators from suppressing the generation of usage data on the switch or certain routes or trunks.

## Analysis Requirements

* The system should provide an intelligent module ( AI/ML module ) that performs complex analysis. It shall work based on historical data and new data flow in the system
* The system should provide a Workflow GUI that correlates data from all sources relative to the fraud case and present it to the investigator"
* The system should provide a capability for the investigator to have notes on the individual cases.
* The System should be able to track / calculate revenue losses and averted losses
* The system should provide a Workflow GUI that provides a capability to send form letters/emails/SMS
* The system should be able to calculate the losses identified for a case
* The system should be able to calculate the estimated savings of a detection

## Users Interfaces

* Explain the types of interfaces that the system supports
* The system should provide distinct user interfaces: for senior executives, tool administration, fraud analysis, system manager

## Alarms and Alerts Requirements

* The system should set different thresholds for new customers
* The system should automatically set thresholds for all subscribers based on history
* Rule to be tested before put into production ( Alarm if it didn't pass the testing step ), please explain how your system handle
* If there any rules that require the vendor to create, please explain how your system handle
* Alert if the system when AI / ML module automatically modified thresholds, explain process
* Alert if manual threshold changes did occur, explain if system allow and how
* Explain in detail what happens when an alert is deemed fraud
* Explain in detail what happens when an alert is deemed legitimate

## Reporting Requirements

* The system should support predefined reports included in the report capability
* The system should allow users to can create their own ad-hoc reports
* The system should allow users to schedule the reports
* The system should allow users to exported and/or distribute reports
* Describe the formats used to export the reports
* The system should support both graphical and drill down report capabilities
* Reports to be detailed and summarized

## Audit logs Requirements

* The system should support internal audit to detect any system failures
* Audit trails to be detailed
* The system should provide enough information to identify single transactions, users, time and date and values modified or entered in the transaction

## Hardware and Software Requirements

* List supported hardware and Operating systems (Indicate your recommended option and why?)
* List supported databases (Indicate your recommended option and why?)
* List all other software licenses or tools needed to be purchased for your systems full operation
* Explain how does the system scale with increase of subscribers and/or call records
* Explain the system interfaces (Systems, Network Elements, etc.)
* System have to be in MIC2 premises and full control of MIC2 IT department

## System Security Requirements

* Describe the security on a user level
* Describe the security on a functional level
* Explain if the authorization can be given based on a function, field, screen, or row level
* Describe & Explain data security and encryption of data fields facility
* Data cannot be transmitted by any method outside MIC2 premises

## Operational Requirements

* The system should have a backup functionality, recovery procedure and fall back capability.
* The maintenance and downtime requirements should be clearly outlined

## Warranty

* The application software supplied being free from defects for at-least one year from date of completion of Customer Acceptance Test
* The system will be on SaaS basis, so all deliveries, maintenance, updates, upgrades are the sole responsibility of the Vendor as part of their service

## Financials

* The system should be based on SaaS (Software as a Service) Model.
  + **Failure to abide with the above statement will disqualify the vendor from the bidding process.**

## Performance

* A new data feed should be able to be configured by a trained person
* DB query time should be technically reasonable
* Vendors should state whether the fraud management system will be able to support the expected growth in subscribers, call and events volumes

## Easy Configuration and Maintenance

* The system should be easily configured and continuously running properly despite various changes

## Company profile

* The vendor should provide Company profile, references and history, Years in business, information related to proposed solution experience

## Successful installations at similar environment

* Provide other successful installations at similar business companies

## Future Development/roadmap

* Describe the strategic plan, technical objectives and the major milestones to upgrade the system based on the latest technologies and fraud types

## Implementation timeline

* Define the estimated time for system implementation

## Training

* The vendor should provide training to all users and outline how and where the training will be provided, MIC2 prefer training in MIC2 premises

## Support

* User-Level Support

This level should cover support to end-users on resolving issues at the application level. This involves answering queries about the functionality and daily operation of the system that may have been forgotten or misunderstood during the training provided

* Administrator Level Support

This level of support will be required in case of system failure or to answer queries from the MIC2 system administrator regarding ongoing maintenance and system configuration

--------------- End of document --------------.