**Request for Proposal (RFP)**

**For MIC2**

**Fraud Management**

**Technical Specifications**

**Table of contents**

[1. Technical Specifications 3](#_Toc166768645)

[I. General 3](#_Toc166768646)

[II Fraud Management System 3](#_Toc166768647)

[2. Fraud Management System Requirements 4](#_Toc166768648)

[I. General Requirements 4](#_Toc166768649)

[II. Data Acquisition Layer/Mediation Requirements 5](#_Toc166768650)

[III. Fraud Types 6](#_Toc166768651)

[IV. Analysis Requirements 7](#_Toc166768652)

[V. Users Interfaces 7](#_Toc166768653)

[VI. Alarms and Alerts Requirements 8](#_Toc166768654)

[VII. Reporting Requirements 8](#_Toc166768655)

[VIII. Audit logs Requirements 8](#_Toc166768656)

[IX. Hardware and Software Requirements 9](#_Toc166768657)

[X. System Security Requirements 9](#_Toc166768658)

[XI. Operational Requirements 9](#_Toc166768659)

[XII. Warranty 10](#_Toc166768660)

[XIII. Performance 10](#_Toc166768661)

[XIV. Company profile 10](#_Toc166768662)

[XV. Future Development/roadmap 10](#_Toc166768663)

[XVI. Implementation timeline 10](#_Toc166768664)

[XVII. Training 10](#_Toc166768665)

[XVIII. Support 10](#_Toc166768666)

[XIX. Documentation 11](#_Toc166768667)

# 

# Technical Specifications

## General

* Vendor(s) shall include in their offer a detailed BoQ for all relevant Hardware, Software, that are needed to implement the 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 based on OPEX paid monthly

### 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
* SMS Fraud
* Roaming Fraud
* International Revenue Sharing Fraud (IRSF)
* Wangiri Fraud
* Data Fraud
* etc…

# 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 1 month. Data older than 1 month will be backed-up. System database has to have direct integration with standard DB like Oracle or MS-SQL.
* The system should store aggregated data for reporting up to 1 year of historical data on daily, weekly, monthly level.
* The solution shall allow MIC2 to configure its own rules within the Fraud Management System without dependency on vendors at no extra cost
* The system availability should be better than 90%
* The system should be highly scalable to easily accommodate both current and projected volumes of data (e.g., increased traffic)
* 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 proposed solution should provide robust fraud detection and risk scoring capabilities incorporating:
* Advanced rule/scenario based detection (explain in details how this will be done)
* Dynamic User Profiling and anomaly detection (explain in details how this will be done)
* Machine Learning based Predictive Scoring models (explain in details how this will be done)
* The solution shall detect suspicious activity based on customers’ previous activity
* System shall have the capability to analyze large data volumes with speed & accuracy, and deliver the information to end user
* System should be able to generate alerts via email in case the user does not take action on any of the triggered / fired rule in specified time in system
* The proposed solution should support rapid deployment of new fraud scenarios when required. The system should support testing of these scenarios on a test environment before moving them to production
* The proposed solution should be modular thus allowing for the incorporation of new features/ functionality when necessary, when required
* The solution should have flexible architecture of AI/ML model that is scalable horizontally and vertically to adapt to the changing business load scenarios
* Applying vendors shall provide upon request, in addition to the required documents, a demo to explain to MIC2 their solution composed of:
  + - Technical presentation
    - Live demonstration on a testbed or on a live operating network

## 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:
  + SMSC (InMobile)
  + MSS (Nokia)
  + Packet Core (HUAWEI)
  + DNS
  + NGBSS (HUAWEI)
  + CRM
  + TAPIN/TAPOUT/NRTRDE (EDCH)
* Other needed sources to be identified
* Provide the list of formats supported and not supported"
* Specify any other network element needed to fully comply to MIC2 requirements
* The system should support different connection protocols and handle but not limited to the following:
  + TCPIP
  + FTP/SFTP
  + HTTP
  + SOAP
* 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. In addition, 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
* The system should detect any missing CDR not billed from
  + - Voice
    - SMS
    - Data
* Please explain in details how this will be done (comparison of which data sources and what are the criteria)

## Fraud Types

III-1 **Interconnect Bypass Fraud**

* Bypass Types
  + Simbox fraud to explain how it is detected
  + Gray Routing and Over-The-Top (OTT) Interconnect Bypass fraud to explain how it is detected
* Bypass detection capabilities. Please elaborate
  + Test Call Services (TCG) performing 20000 test calls per month
  + CDR Analysis
  + Signalling Analytics
  + Protocol Signature/Pre-Call Detection

III-2 **SMS Fraud**

* Please provide examples, methodologies and mechanisms used to apply the rule for each type
  + SMS Bypass
  + A2P Fraud
  + SMS Spoofing
  + SMS Malware/Spamming
* Tracking of Silent SMS to a certain destination

III-3 **Roaming Fraud**

* + The system should support Near Real Time Roaming Data Exchange (NRTRDE).
  + The system should support HUR
  + The system should detect High Usage (Voice, SMS and Data) within a defined timeframe using different data sources such as (TAP, HUR and NRTRDE)
  + High count of MO/MT calls
  + Long Duration of MO/MT calls
  + High count of SMS MO&MT
  + High Data volume
  + The system should detect HU to risky destinations; threshold should be dynamically set by MIC2
  + The system should detect Outbound Roaming Prepaid or Postpaid subscriber with
  + Data calls
  + or/and MO calls

While roaming in network not found in list of Camel operators with prepaid roaming agreement with MIC2

* + The system should detect several IMSIs from same operator making excessive traffic (MO or Data) within a short period.

III-4 **Other fraud type**s

Please justify and provide the rule description for the below:

* High usage in local, International and premiums rate calls
* Wangiri Fraud (Voice & SMS)
* Dealer fraud (false subscriptions; re-activation of old accounts, etc...)
* Subscription fraud (data alteration, duplicated info, etc...)
* VoIP & SIP Fraud
* International Revenue Sharing Fraud (IRSF)
* CLI spoofing
* Free Data usage on corresponding Rating Group
* Usage abnormalities for all type of SMS services (Premium rate, Bulk ...)
* Artificially Inflated Traffic (AIT) and Artificially Generated Traffic (AGT)
* Prepaid subscriber with depleted voice balance/bundle able to make voice calls not to emergency services
* Velocity check (calls made from geographically distant places within a short period of time)
* Prepaid subscriber with total Data bundles balance null but making successful data session
* SIM stuffing to detect multiple SIMs using the same IMEI

## Analysis Requirements

* 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 Workflow GUI that provides a capability to send form letters/emails/SMS

## Users Interfaces

* Explain the types of interfaces that the system supports?
* The system should provide distinct user interfaces / dashboards: for senior executives, system administration, revenue analysis, and general user

### 

## Alarms and Alerts Requirements

* The system should set different thresholds for different cases
* The system should automatically set thresholds for all cases 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

## Reporting Requirements

* Solution should have the capability to provide different access level per user privilege (to explain in details)
* The system should support predefined reports included in the reporting capability. Please describe the list
* To provide Executive Dashboard for management (specify which reports and the dashboard information that will be available)
* The system should allow users to create their own ad-hoc reports
* The system should allow users to schedule the reports
* The system should allow users to export and/or distribute reports
* Allowing authorized employees to create reports based on selected criteria
* Reports should be exported in different formats (CSV, PDF...) to provide all available formats
* The system should support both graphical and drill down report capabilities
* The system should be able to do the following levels of summary for analysis purpose:
* Trending summary (by month/ by week)
* Analytical summary (by month/ by week/ by day/ by hour)

## Audit logs Requirements

* The solution should be integrated with MIC2 SIEM solution to export all the logs
* Solution should provide all types of access logs per user, ip, time…
* Solution should provide detailed query logs related to subscriber or sensitive information query
* The system should support internal audit to detect any system failures.
* The system should provide an Audit Trail that allows monitoring, alarms, logging of user activities, and automatic actions
* The system should provide enough information to identify single transactions, users, time and date and values modified or entered in the transaction. Describe

## Hardware and Software Requirements

* Vendor to provide in details the hardware needed and all third party software that is part of the solution
* List supported databases
* List the count and description of probes that will be used if needed
* List all other software licenses or tools needed to be purchased for your system's full operation
* Explain how does the system scale with increase of subscribers and/or call records"
* Explain the system interfaces (Systems, Network Elements, etc.)
* Solution should be fully implemented on premises

## System Security Requirements

* Describe the security on a user level
* Describe the security on a function 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. Describe the security on a user level

## Operational Requirements

* The system should have a backup functionality, recovery procedure and fall back capability.
* Outline your maintenance and downtime requirements

## Warranty

* The application software supplied being free from defects for at-least one year from date of completion of Provisional Acceptance Test
* The solution should be available with Support for 3 years after final acceptance

## 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

## Company profile

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

## 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 for the coming 3 years

## Implementation timeline

* Define the estimated time for system implementation; solution should be implemented on phases approach and to be fully completed within 8 Months of PO issuance.

## Training

* Vendor should provide training to all system users.

Please provide details (days, online, onsite….)

* Specify the related training details for different user levels.

## Support

XIX-1 User Level Support

XIX-1-1 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.

XIX-2 Administrator Level Support

XIX-2-1 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

XIX-2-2 Vendors should state whether they have local presence in Lebanon, the Gulf Cooperation Council area (GCC). The level of support that can be provided for the system by the local office should be outlined as well as any future training that local employees might receive on the system to enhance the service they can offer to MIC2

## Documentation

* Bidder has to provide the documentation for the project including but not limited to

• Scope, functional and operational requirements, resource requirements, project design/plan, product description, guidance for best practices, implementation guidelines, user acceptance test plan, operations/policy configuration manual, integration document, security implementation, training materials etc.

• Adherence to agreed Service Levels, periodic monitoring and reporting of the same on a monthly basis.

• Bidder should provide the detailed architecture of the solution.

• Rule & Detection Engine, Prevention Module, Case Management tool and their underlying infrastructure components are required to be in High Availability mode.

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