Validated 8/10/2025

PRINCIPLES GUIDING FRAUD MANAGEMENT

(ECOWAS Regional Roaming Initiative)

Table of Contents

Executive Summary....3
1. Background:....4
2. Purpose:....5
2.1 National and Regional Anti-Fraud Committees....5
2.2 Potential Fraud Risks....8
2.3 General Guidelines for Fraud Management and Prevention:....11
2.3.1 Anti-FKPI_001:....12
2.3.1.1 Control/KPI Description:....12
2.3.1.2 RACI (Responsible/Accountable/Consult/Inform):....13
2.3.2 Anti-FKPI_002:....13
2.3.2.1 Control/KPI Description:....13
2.3.2.2 RACI (Responsible/Accountable/Consult/Inform):....13
2.3.3 Anti-FKPI_003:....13
2.3.3.1 Control/KPI Description:....13
2.3.3.2 RACI (Responsible/Accountable/Consult/Inform):....14
2.3.4 Anti-FKPI_004:....14
2.3.4.1 Control/KPI Description:....14
2.3.4.2 Responsible Accountable/Consult/Inform (RACI):....15
2.3.5 Anti-FKPI_005:....15
2.3.5.1 Control/KPI Description:....15
2.3.5.2 Responsible/Accountable/Consult/Inform (RACI):....15
2.3.6 Anti-FKPI_006:....15
2.3.6.1 Control/KPI Description:....15
2.3.6.2 Responsible/Accountable/Consult/Inform (RACI):....16
2.3.7 Anti-FKPI_007:....16
2.3.7.1 Control/KPI Description:....16
2.3.7.2 Responsible/Accountable/Consult/Inform (RACI):....16
2.4 Technical Support &Escalation Matrix....16
2.5 Fraud Reporting....17
APPENDIX 1....17
APPENDIX 2....17
APPENDIX 3....19

Executive Summary

ECOWAS Regulation C/Reg.21/12/17 on roaming on Public Mobile Communications Networks in the ECOWAS Region, Article 15(2) requires Member States to set up Committees to check fraud in the area of community roaming.

The NRA DG's Resolutions 1, 2 and 3 required the establishment of National and Regional Committees to develop fraud control mechanisms at the National and Regional levels to effectively deal with fraud issues when the roaming service becomes operational. Based on the above mandate, the Technical Implementation Committee set up a Regional Anti-fraud Committee (RAFC) to be led by Ghana.

The first deliverable of the RAFC was the development of a work plan for fraud management. This work plan detailed proposed/anticipated activities to be undertaken to deliver on this mandate.

The Committee then developed a fraud management status matrix for member states to complete to enable the committee to know the status of countries with regard to fraud management. The Committee then identified the under-listed Terms of Reference (ToR) to guide the works of National and Regional Anti-fraud Committees.

National Antifraud Committees ToR

- Document the current fraudulent activities prevalent in the country.
- Identify potential fraud types that may arise
- Assess existing legal frameworks for fraud management and control

Regional Antifraud Committee ToR

- Identify and highlight potential fraud types that may arise following the implementation.
- Development of Anti-fraud guidelines in the form of fraud mitigation controls and monitoring KPIs.
- Coordinate activities of the various National Anti-Fraud Committees in relation to the ECOWAS Free Roaming Initiative among other fraud typologies
- Take stock and assess the sufficiency of Member State's fraud management infrastructure for effective and efficient fraud management
- Develop protocols to guide the treatment of detected fraud numbers (MSISDNs) by Member States.
- Assess and recommend fraud management systems and tools.
- Develop and implement appropriate fraud reporting requirements and regularly review reports by Member States.
- Provide technical support to Member States for the implementation of controls and KPIs

Based on the fraud management status responses, Member States who had no National Antifraud Committees were helped to establish some. Those with no specific legal framework to manage telecommunications fraud were given guidelines and in some cases, samples of other countries' legal frameworks were shared to guide them in this regard. Almost all the countries had some form of fraud management systems at the operator level in place. Others had both at the operator and NRA levels. Almost all

countries had put in place a robust national identification system, except two (2). Others had theirs ongoing, either at the operators or at the national level, in place.

Based on the deliverables on the ToR and fraud management updates given by countries, the Committee came up with potential fraud risks and antifraud KPIs to serve as fraud mitigation controls. A fraud -reporting template has also been developed to guide operators in Member States in reporting identified fraudulent activities.

Telecommunication fraud is not static but rather dynamic, as such the Regional Antifraud Committee is recommending that operators adhere closely to the identified fraud mitigation controls. Those who do not have the equipment to mitigate any of the anticipated fraud risks, should as a matter of urgency purchase the needed equipment modules and/or software to be compliant with the proposed fraud mitigation controls.

In addition to the above recommendation, there will be the need to have a third-tier fraud management control platform to manage fraud at the regional level.

Potential vendors of Fraud Management Solutions and Tools have been engaged in the fraud risk requirements. The Regional Team will be responsible for delivering any such deployment at both the National and Regional levels.

For operational efficiency and data protection considerations, any solution adopted will be structured in such a manner as to process data and apply detection logic at the national level while alert information and summary details are shared at the regional level.

1. Background:

The ECOWAS Roaming Initiative is an initiative proposed by ECOWAS Ministers of Telecoms/ICTs during their meeting in Niger in 2016. The initiative aims inter alia to:

i. harmonise roaming rates/charges within the ECOWAS region
ii. facilitate cross-border communications and commerce

Under this Policy, Regulation C/REG. 21/12/17 on Roaming on Public Mobile Communications Networks in the ECOWAS region was adopted. The regulation also requires Member States to set up committees to check fraud in the area of community roaming.

In 2019, there was a further call by the Ministers of Communications/Telecommunications/ICT within the sub-region to kick start the ECOWAS Roaming Initiative taking into consideration ECOWAS trade, cross-border connectivity and roaming charges likely to hinder trade progress.

The Director-Generals and Presidents of ECOWAS National Regulatory Authorities (NRAs), cognizant of the potential influx of bypass fraud with the implementation of the ECOWAS Free Roaming Initiative, at their 2nd High-Level Meeting in March 2021, reiterated the need for the establishment of the national and regional anti-fraud

Committees by 31st May 2021 in accordance with Article 20 of Regulation No. C/REG.21/12/17. Furthermore, the NRAs were required to define a technical scheme and effective fraud control mechanisms at the National and Regional levels by **June 30, 2021**.

Inherent fraud risks, associated with general telecom services, particularly roaming, are expected across the sub-region upon enabling SIM import through the initiative. Hence, it is essential to implement robust anti-fraud mechanisms to mitigate any anticipated risks.

2. Purpose:

The purpose of this framework is to elaborate on the key objectives of the anti-fraud agenda of WATRA in relation to the ECOWAS Roaming Initiative as follows:

1. Coordinate the setting up of National and Regional anti-fraud Committees,
    - Ensure administrative coordination
    - Establish technical coordination tools

2. Identify and highlight potential fraud types that may arise following the implementation.

3. Develop mitigating control mechanisms and monitoring KPIs

4. Provide technical support for the implementation of such controls and KPIs

5. Continuous monitoring of Control and KPI effectiveness.

6. Technically review and propose a Fraud Management Solution to Member State Operators where necessary.

2.1 National and Regional Anti-Fraud Committees

The management of fraud is at three levels:

- MNO Level: NRAs are to ensure that each MNO has developed an anti-fraud solution

- NRA Level: The National Regulatory Authorities have to set up a National Committee and a platform as well as mechanisms for collaboration and control of anti-fraud activities, in accordance with the ECOWAS Regulations.

- Regional Level: Ghana will coordinate all fraud reporting activities at the ECOWAS level: while the regional platform will serve as a regional anti-fraud main tool.

Following Ghana's selection as the lead country for Anti-Fraud Management, a team was constituted from its National Anti-Fraud Committee to begin an engagement at the sub-regional level. This later metamorphosed into a **Regional Anti-Fraud Committee (RAFC)** with the nomination of two (2) representatives from each Member State's NRA.

Guidelines and support were provided by the Regional Committee to the respective NRAs to constitute their respective **National Anti-Fraud Committee (NAFC)**.

The composition and mandate of the National and Regional Anti-Fraud committees are as follows:

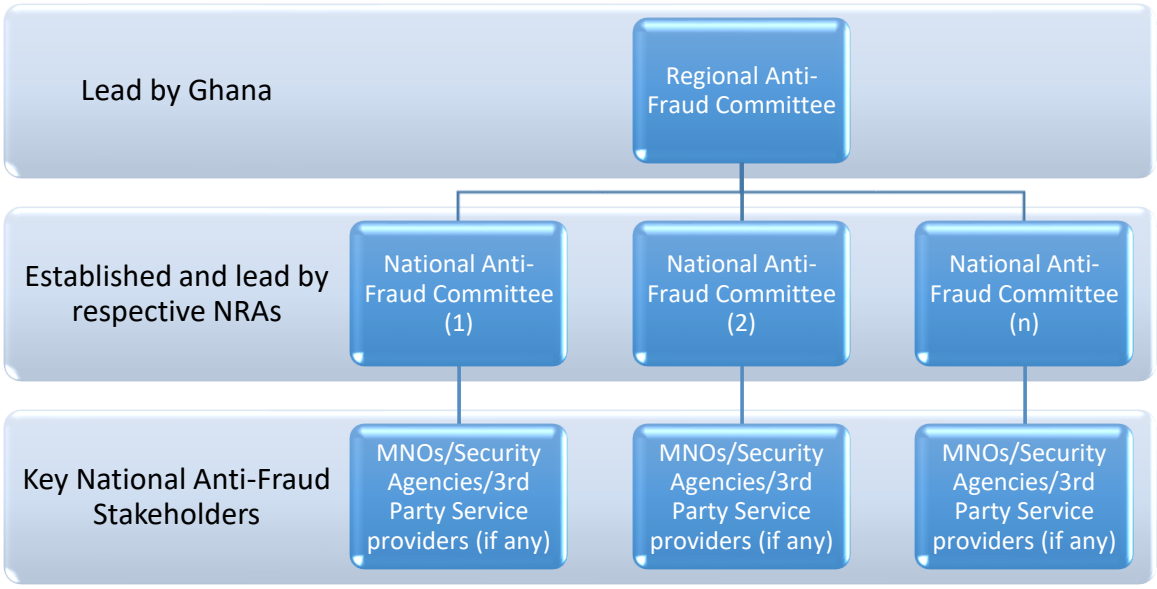
National Anti-Fraud Committee (NAFC)

- **Composition:**
    - Chairperson: Representative from the National Regulatory Authority (NRA)
    - Vice-Chairperson: nominated by members of the NAFC
    - Members: Two (2) representatives from each licensed Mobile Network Operator (MNO), Representatives from relevant State Security Agencies, and the Ministry in charge of Communications.
    - Secretariat: The NRA shall provide secretarial support.
- **Mandate & Objectives:**
    - To serve as the primary national body for all fraud management activities related to roaming.
    - To implement and enforce regional anti-fraud guidelines and KPIs at the national level.
    - To identify, investigate, and submit report of incidents of fraud using standardized templates.
    - To facilitate collaboration and information sharing between national MNOs and with the RAFC.
    - To assess the adequacy of national legal frameworks for prosecuting telecom fraud and recommend necessary reforms.
    - To ensure all national MNOs have functional Fraud Management Systems (FMS) compliant with regional standards.
    - Assess the effectiveness of antifraud controls implemented by MNOs.

Regional Anti-Fraud Committee (RAFC)

- **Composition:**
    - Led by the Lead Country (Ghana).
    - Members: Two (2) technical experts nominated by the NRA of each ECOWAS Member State.
    - Observers: Representatives from WATRA and the ECOWAS Commission.
- **Mandate & Objectives:**
    - To provide strategic direction and coordination of activities of the various National Anti-Fraud Committees in relation to the ECOWAS Regional Roaming initiative among other fraud types.
    - To develop, publish, and maintain these anti-fraud guidelines, controls, and KPIs.
    - To receive, analyse, and act upon fraud reports from all NAFCs.
    - To identify emerging cross-border fraud typologies and develop appropriate mitigation strategies.
    - Develop protocols to guide the handling of detected fraudulent MSISDNs by respective National Anti-Fraud Committees
    - To provide corrective action plans for underperforming member states
    - Assess and recommend fraud management systems and tools.
    - To carry out periodic anti-fraud campaigns across the sub-region with support from the respective NRAs/NAFCs.
    - Develop and implement appropriate fraud reporting requirements and regularly review reports by member states.
    - To build capacity and provide technical support to NAFCs and MNOs.
    - To report periodically to the ECOWAS Committee of Telecoms/ICTs Ministers on the status of fraud within the roaming region.

The Anti-Fraud activities are structured as follows:



2.2 Potential Fraud Risks

The ECOWAS Roaming initiative is susceptible to several fraud types. Below is a categorization based on potential impact and likelihood:

Fraud Type	**Description/ Scenario**	**Risk Level**	**Proposed Mitigation (See Section 2.3)**
SIM Box Bypass	Illegally terminating international calls via local SIMs to avoid international gateway fees. *e.g., A fraudster sets up a device with multiple local SIM cards in Benin to terminate calls destined for Nigerian numbers, bypassing international tariffs.*	High	Ref: Anti-FKPI_003
IRSF/PRS (International Revenue Share/Premium Rate Service) Fraud	Generating calls to high-premium numbers to earn revenue share. *e.g., A roamer's SIM is compromised and used to call premium-rate numbers in a faraway country, generating huge costs for the home operator.*	High	Ref: Anti-FKPI_001

Fraud Type	Description/ Scenario	Risk Level	Proposed Mitigation (See Section 2.3)
Wangiri (One-Ring)	Making missed calls to prompt callbacks to premium numbers. *e.g., A roamer receives a missed call. Upon calling back, they are connected to a premium-rate number, incurring significant charges.*	Medium	Ref: Anti-FKPI_004
Subscription Fraud	Obtaining service with no intention of payment, often using fake IDs. *e.g., A individual uses forged identification to acquire multiple SIMs specifically for launching fraudulent roaming activities.*	Medium	National ID Checks, Ref: Anti-FKPI_004
A2P SMS Spamming	Bypassing legitimate billing/charging routes for termination of bulk application-to-person SMS. *e.g., A content provider bypasses the official A2P channel by using a bank of roaming SIMs to send bulk SMS, evading higher fees.*	Medium	Ref: Anti-FKPI_002, Anti-FKPI_006
CLI Spoofing	Manipulating the calling line identity to mask the true origin of a call. *e.g., A fraudster spoofs a bank's official number to conduct phishing attacks against roamers.*	High	Signalling Security (e.g., STIR/SHAKEN), Ref: Anti-FKPI_004
Test SIM Fraud	Misuse of SIMs intended for testing network interoperability and roaming agreements. e.g., An operator's employee provides a large number of test SIMs to a third party who uses them for personal communication or illicit traffic generation, evading charges.	Medium	Strict bilateral agreements limiting the quantity, usage (data/calls/SMS caps), and lifespan of test SIMs. Regular audits and monitoring for abnormal traffic patterns.

Fraud Type	Description/ Scenario	Risk Level	Proposed Mitigation (See Section 2.3)
			Requires action from responsible network within 96 hours
Permanent Roaming	A subscriber uses a SIM card from a low-cost country permanently in a higher-cost country to benefit from cheaper subscription rates. e.g., A subscriber in Country A (high tariffs) uses a SIM from Country B (low tariffs) with a favorable roaming charges, never returning to the HPMN network.	High	Implement and enforce "roaming usage policies" in terms & conditions. Deploy monitoring tools (Anti-FKPI_005) to identify subscribers with excessive, continuous roaming duration (e.g., >3 months) and take action (e.g., surcharges, service restriction). Requires action from responsible network within 48 hours

Among other fraud types, the ECOWAS Roaming Initiative is expected to be susceptible to the following fraud risks:

- **SIM Box** – Involves the bypass of legitimate international gateway to terminate incoming international traffic via a local MSISDN.

- **CLI spoofing and A-number Refiling** – Refers to the deliberate misrepresentation of a calling number.

- **IRSF/PRS (International Revenue Share/Premium Rate Service Fraud)** – Characterized by the generation of traffic to high tariff and premium rate destinations with the intent of getting a share of accruing revenues.

- **Subscription Fraud** – Occurs by accessing and use of service(s) originally not paid for as part of one's offer through system manipulation.

- **High Usage Fraud** – Involves usage abuse as a result of charging failure and/or other

- **A2P SMS Spamming** – Entails the termination of bulk, system-generated SMS messages via unauthorized routes, bypassing legitimate billing mechanisms and often used for unsolicited or fraudulent communications

2.3 General Guidelines for Fraud Management and Prevention:

- All inbound roaming SIMs must have at least fifteen (15) days usage history of usage in their home country before being allowed to roam on a visited network. SIMs which fail this criterion shall be temporarily denied access to all roaming services. The visited network shall flag and communicate to inbound roamer's home network any roamer exhibiting suspicious activity for further verification of roamer's status. The visited network shall only grant roaming access after a positive verification of inbound roamer's status has been completed.
- All MNOs shall submit a detailed monthly report on all fraud management activities as per the table in Appendix 1.

A. Step-wise Fraud Management Process:

1. Prevention: MNOs should implement proactive controls (e.g., SIM registration,15-day SIM incubation, NRTRDE exchange).
2. Detection: Monitor traffic 24/7 against configured KPI thresholds in the FMS.
3. Response: Upon alert, automatically or manually suspend service as per RACI charts below and initiate investigation.
4. Reporting: Document the incident in the national and regional portals (Appendix 1).
5. Analysis: Regional team correlates data to identify trends and refine detection logic.
6. Refinement: Update FMS rules and controls based on analysis.

B. Standard RACI Matrix (Overview):

- Responsible (R): Entity that performs the task.
- Accountable (A): Entity ultimately answerable for correct completion.
- Consulted (C): Entity that provides input.
- Informed (I): Entity that is kept up-to-date on progress.
  (Detailed RACI is provided for each KPI in sections 2.3.1-7)

C. SIM Incubation & Minimum Spend Threshold:

- The 15-day usage history rule (Section 2.3) is a mandatory incubation period to establish legitimate subscriber behavior.
- NRAs may consider, in addition, a *minimum spend threshold* in the home network as a further credibility indicator, ensuring consumer protection regulations are adhered to.

D. Shared Responsibility & Escalation:

- Fraud management is a shared responsibility between Home and Visited networks, as detailed in the per-KPI RACI.
- Escalation Path: MNO Fraud Team -> National NAFC -> Regional RAFC -> WATRA/ECOWAS. Escalation timelines must be defined in MoU

E. NRTRIE (Near Real-Time Roaming Data Exchange):

- The implementation of NRTRIE mechanisms is mandated for all MNOs to enable near real-time exchange of roaming usage data. This is critical for real-time credit control, fraud monitoring, and averting bill shock, as complemented by Anti-FKPI_005. All MNOs must implement systems to exchange TAP files (or equivalent standardized data records) for outbound roamers within a mutually agreed, minimized time window (e.g., every 2-4 hours). This allows the home network to perform near real-time usage monitoring, credit control, and fraud detection based on actual usage data from the visited network, thereby averting bill shock and significantly improving fraud mitigation capabilities. The chosen medium and format must be agreed upon in bilateral roaming agreements.

F. Roles in Service Suspension:

- The Home Network is responsible for suspending services for outbound roamers based on alerts received from visited networks or its own credit/fraud controls.

G. Penalties for Non-Compliance:

- NRAs, with support from the RAFC, shall develop a framework of conditional financial penalties for MNOs that consistently fail to implement controls, respond to alerts, or provide required data, leading to unresolved billing disputes or avoidable revenue losses for partners.

H. Preventive Controls & Fair Use Policies:

  - Wholesale Roaming Caps: MNOs shall implement wholesale financial caps to limit financial exposure from fraudulent roaming activity.
  - Fair Use Policy (FUP): MNOs may implement FUP for:
    - Permanent Roaming: To prevent subscribers from permanently residing and operating in a visited network.
    - Free Incoming Calls: To prevent abuse of unlimited incoming call offers.
    - Retail Promotions: To define the duration and scope of any discounted roaming offers.
  - Maximum Accounts per Subscriber: Home networks shall implement rules to limit the number of active roaming SIMs per subscriber to a reasonable number (e.g., 2-3).

- Leveraging Advanced Tools: MNOs are encouraged to leverage Artificial Intelligence (AI) and Machine Learning (ML) modules within their FMS for proactive and predictive fraud detection, moving beyond static threshold-based rules.

Specific Fraud Mitigation Controls and KPI Matrix

2.3.1 Anti-FKPI_001:

Monitoring of traffic to hotlist destinations by visiting subscribers (inbound roamers)

2.3.1.1 Control/KPI Description:

While roaming on a visited network, traffic generated by an inbound roamer must be monitored for IRSF/PRS fraudulent activities. The control must be configured on the

visitor network FMS and monitored 24/7. Services must be suspended for numbers that breach the controls and details communicated to the home network and respective regulatory authority. (See Appendix 2 for applicable control threshold)

The home network should be notified to block the suspected range of numbers.
After a period of no response, the visited network should completely block the network of those numbers.

2.3.1.2 RACI (Responsible/Accountable/Consult/Inform):

R - Host/Visited Network Operator
I – National Anti-Fraud Committee
A/C – Home Network Operator.

2.3.2 Anti-FKPI_002:

High Usage Monitoring.
* This KPI will cover the following metrics as provided in appendix 2:
*Average SMS sent by an in-roamer within an hour and 24 hours.
*Average outgoing MOU by an in-roamer within an hour and 24 hours.
*Average data use volume by an in-roamer within an hour and 24 hours.

2.3.2.1 Control/KPI Description:

Inbound roaming transactions/volumes must be monitored for out-of-threshold usage. Such thresholds must be configured on the visitor network FMS and monitored 24/7. The home network should be notified to suspended the services for subscribers that breach the threshold.

***Implement a home network responsible for voice, data and SMS blocking.**

2.3.2.2 RACI (Responsible/Accountable/Consult/Inform):

R - Host/Visited Network Operator
I – National Anti-Fraud Committee
A/C – Home Network

2.3.3 Anti-FKPI_003:

International Traffic Termination Bypass (SIM Box) Monitoring.

2.3.3.1 Control/KPI Description:

Inbound roamers must be monitored for international traffic termination bypass

activities on both the home and visiting networks. A SIM Box detection solution should be deployed and configured to flag such SIM cards.
Detected SIMs must be removed from the Host Network's VLR database and the relevant details communicated to the Home Network.

*The Visited Network is capable of detecting and flagging bypass roamers on its VLR, in coordination with the home network. It is imperative that the visited network communicates all detections to the home network to ensure synchronized fraud mitigation efforts.
*Upon detection, the Visited Network must promptly notify the home network while initiating the blocking of the identified SIM cards**.**

2.3.3.2 RACI (Responsible/Accountable/Consult/Inform):

R - Host/Visited Network Operator
I – National Anti-Fraud Committee
A/C – Home Network

2.3.4 Anti-FKPI_004:

Unusual Call Behaviour and/or Pattern Monitoring.

2.3.4.1 Control/KPI Description:

Rules must be configured in the Fraud Management System (FMS) to monitor and flag unusual call behaviours and patterns during roaming. These behaviours may include, but are not limited to:

- **First call made upon roaming registration**: May indicate automated SIM Box activation.
- **Unusually long-duration calls**: Could suggest artificial traffic generation or call pumping.
- **Calls initiated via call forwarding functionality**: Often exploited in bypass scenarios.
- **High volume of short-duration calls**: Typical of SIM Box or termination fraud.
- **Calls to high-risk destinations or premium-rate numbers**: May indicate revenue-share fraud.
- **SIMs generating traffic without corresponding mobility events**: Suggests non-human usage.
- **Roaming activity inconsistent with subscriber profile or history**: A red flag for misuse.

- **Multiple SIMs exhibiting identical calling patterns**: Could point to coordinated fraud.

Services must be suspended for numbers that breach the control and details communicated to the Home Network.

2.3.4.2 Responsible Accountable/Consult/Inform (RACI):

R - Host/Visited Network Operator and Home Network
I – National Anti-Fraud Committee
A/C – Home Network

2.3.5 Anti-FKPI_005:

Exchange of Roaming Data (NRTRDE).

2.3.5.1 Control/KPI Description:

Outbound roaming transactions are typically processed and billed by the respective Home Operators. However, the initial recording of these transactions is carried out by the Visited Network. It is therefore essential that the Visited Network promptly shares this information with the subscriber's Home Network through an agreed communication channel. This ensures effective monitoring of usage and credit limits, and helps prevent bill shock at the end of the billing cycle.

2.3.5.2 Responsible/Accountable/Consult/Inform (RACI):

R/A - Host/Visited Network Operator
C – Home Network

2.3.6 Anti-FKPI_006:

Set and Monitor Data use limit.

2.3.6.1 Control/KPI Description:

Inbound roaming subscribers access data via visitor Gateway GPRS Support Node (GGSN). A limit in terms of data use volume must be agreed upon and set by Visitor Networks for respective partner subscribers as the basis for high usage monitoring and control.
The agreed threshold must be configured on Visitor Network FMS for effective monitoring.
Note:
** Volumes are of concern and not cost; as each MNO has specific charges.
** Flagged numbers must be communicated to the Home Network.

2.3.6.2 Responsible/Accountable/Consult/Inform (RACI):

R/A - Host/Visited Network Operator
I – National Anti-Fraud Committee
C – Home Network

2.3.7 Anti-FKPI_007:

Prevent SIM swap for Outbound Roamers.

2.3.7.1 Control/KPI Description:

MNOs must prohibit SIM card swaps while a subscriber's number is in outbound roaming status. Such activity poses a significant risk to service integrity, fraud prevention, and billing accuracy.

Fraudsters employ this strategy to take over legitimate service accounts for fraudulent purposes.

2.3.7.2 Responsible/Accountable/Consult/Inform (RACI):

R/A - Home Network.
I – National Anti-Fraud Committee

2.4 Technical Support & Escalation Matrix

A. Dedicated Fraud Desks:
Each NRA and MNO shall establish a dedicated 24/7 fraud desk with published contact details (email, phone) shared with all partner networks and the RAFC.
B. Standard Escalation Path:

Severity Level	Criteria	Action & Timeline	Escalation Path
Level 1 (Critical)	Major revenue loss (>$10k), ongoing attack, critical system breach.	Immediate action required.	MNO Fraud Desk -> Partner MNO Fraud Desk -> NAFC -> RAFC (within 1 hour)
Level 2 (Major)	Significant revenue loss, multiple MSISDNs involved.	Action within 2-4 hours.	MNO Fraud Desk -> Partner MNO Fraud Desk -> NAFC (within 4 hours)
Level 3 (Minor)	Isolated incident, low financial impact.	Action within 24 hours.	MNO Fraud Desk -> Partner MNO Fraud Desk (within 24 hours)

2.5 Fraud Reporting

A centralized reporting tool/portal shall be deployed for direct incident reporting by respective MNOs across countries with roaming agreements.

Mandatory Reporting: Regardless of individual fraud flags or detection mechanisms, each MNO is required to submit fraud detection reports through the centralized portal. This portal operates independently of any operator-specific FMS to ensure consistency and transparency in reporting.

Training and Onboarding: All designated Single Points of Contact (SPOCs) from participating MNOs will undergo training on the proper use of the portal and standardized procedures for reporting fraudulent incidents. This ensures uniformity in data submission and enhances cross-network collaboration in fraud mitigation**.**

The data will be analysed by the Regional Team and the output, form as a check for incidents that will be flagged or otherwise by the Regional FMS solution and also to aid in fine-tuning the logic for the respective FMS solutions (MNO and NAFC) over time.

APPENDIX 1

Recorded incidents of fraud by MNOs within the respective Member States relating to the ECOWAS Regional Roaming Initiative must be reported monthly via the template below:

Date of Incident	Fraud Type	Number of MSISDNs Involved	Home Operator Name/Country	Lost Revenue (USD)	Revenue Loss Prevented (USD)	Action Taken	Incident Status

APPENDIX 2

Control thresholds for Fraud KPIs (Sample Data from MNOs from Benin & Ghana)

	Number of Concerns				Percentage	

Fraud Type	Yes	No
SIM Box	6	0
International SIM Box	6	0
CLI spoofing and A-number Refiling	5	1
IRSF/PRS (International Revenue Share/Premium Rate Service Fraud)	6	0
Subscription Fraud	4	2
High Usage Fraud	6	0
A2P SMS Spamming (including flash calling)	6	0

Fraud Type	Yes	No
SIM Box	100%	0%
International SIM Box	100%	0%
CLI spoofing and A-number Refiling	83%	17%
IRSF/PRS (International Revenue Share/Premium Rate Service Fraud)	100%	0%
Subscription Fraud	67%	33%
High Usage Fraud	100%	0%
A2P SMS Spamming (including flash calling)	100%	0%

	Number of Concerns	
KPI	Yes	No
Monitoring of traffic to hotlist destinations by visiting subscribers (inbound roamers)	5	1
High Usage Monitoring	6	0
Average SMS sent by an inbound-roamer within an hour and 24 hours	3	3
Average outgoing MOU by an inbound-roamer within an hour and 24 hours	3	3
Average data use volume by an inbound-roamer within an hour and 24 hours	3	3
International Traffic Termination Bypass (SIM Box) Monitoring	6	0
Unusual Call Behaviour and/or Pattern Monitoring	5	1
Exchange of Roaming Data (NRTRDE/CAMEL)	6	0
Set and Monitor Data use limit	3	3
Prevent SIM swap for Outbound Roamers	1	5
The average daily number of different numbers called	3	3
The average number of outgoing calls per day	3	3

	Number of Concerns	
KPI	Yes	No
Monitoring of traffic to hotlist destinations by visiting subscribers (inbound roamers)	83%	17%
High Usage Monitoring	100%	0%
Average SMS sent by an inbound-roamer within an hour and 24 hours	50%	50%
Average outgoing MOU by an inbound-roamer within an hour and 24 hours	50%	50%
Average data use volume by an inbound-roamer within an hour and 24 hours	50%	50%
International Traffic Termination Bypass (SIM Box) Monitoring	100%	0%
Unusual Call Behaviour and/or Pattern Monitoring	83%	17%
Exchange of Roaming Data (NRTRDE/CAMEL)	100%	0%
Set and Monitor Data use limit	50%	50%
Prevent SIM swap for Outbound Roamers	17%	83%
The average daily number of different numbers called	50%	50%
The average number of outgoing calls per day	50%	50%

The average number of incoming calls per day	3	2			The average number of incoming calls per day	50%	33%
The ratio of MOC/MTC per IMSI	1	5			The ratio of MOC/MTC per IMSI	17%	83%
The average duration for outgoing calls per day	3	3			The average duration for outgoing calls per day	50%	50%
The average duration for incoming calls per day	4	2			The average duration for incoming calls per day	67%	33%
Monitor consumer behaviour to detect fraudulent activity	5	1			Monitor consumer behaviour to detect fraudulent activity	83%	17%
ISDN lines should be locked to prevent unauthorized access	1	5			ISDN lines should be locked to prevent unauthorized access	17%	83%
Average number of calls made daily	2	4			Average number of calls made daily	33%	67%
Average number of calls received daily basis	2	4			Average number of calls received daily basis	33%	67%
Agreed allowance for variation	1	5			Agreed allowance for variation	17%	83%

APPENDIX 3

Three timelines for the Implementation of the Regional Antifraud Mechanism Strategy

This proposed fraud management framework must be implemented according to the following timelines to address any fraud and security fallouts to be identified.

MAIN ACTIVITIES	DETAILS OF ACTIONS TO BE DONE	TIMELINE	STAKEHOLDER	COMMENTS
1. Setting up National Anti-fraud Committees	Each country is to set up a National Antifraud Committee	January 2022	NRAs	Done
2. Setting up of Regional Anti-fraud Committees	Each country is to nominate two (2) experts to serve on the regional antifraud committee	October 2021	GHANA	Done
3. Identify potential fraud types	Regional antifraud committee to discuss and identify potential fraud types	April 2022	Regional antifraud committee	Done

4. Assess existing legal frameworks	Each country is to assess its national laws to find out whether there are specific provisions to prosecute telecom fraudsters and report.	June 30, 2022	NRAs	Done
5. Development of Anti-Fraud Guidelines	Elaborate on regional anti-fraud principle	July 31, 2022	Regional antifraud committee /	Done
6. Member State's fraud management infrastructure	To collect the status of existing national platforms and their characteristics	July 31, 2022	NRA / MNO	Partially done
7. Deployment of a Sub-Regional Anti-Fraud System/Tool(s)	System design, implementation and rule configuration.	TBD	GHANA+ECOWAS/WATRA	To organize
8. Develop standardized protocols to guide Member States in the treatment of detected fraudulent numbers by Member States.	Guidelines describing how detected fraudulent activity should be handled	TBD	GHANA	To organize
9. Develop and implement appropriate fraud reporting requirements	A central reporting tool/portal shall be deployed for direct incident reporting by respective MNOs across the sub-region	TBD	GHANA	To organize
10. Monitoring Regional Anti-fraud system/mechanism	Analyse data on all reported fraudulent activities to know those which has stopped and those persisting	TBD	GHANA	To organize

APPENDIX 4 - ACRONYMS

A2P SMS: Application-to-Person SMS

Anti-FKPI: Anti-Fraud Key Performance Indicator

CLI Spoofing: Calling Line Identity Spoofing

ECOWAS: Economic Community of West African States

FMS: Fraud Management System

FUP: Fair Use Policy

GGSN: Gateway GPRS Support Node

HPMN: Home Public Mobile Network

IRSF/PRS Fraud: International Revenue Share Fraud / Premium Rate Service Fraud

MNO: Mobile Network Operator

MSISDN: Mobile Station International Subscriber Directory Number

NAFC: National Anti-Fraud Committee

NRA: National Regulatory Authority

NRTRDE: Near Real-Time Roaming Data Exchange

RAFC: Regional Anti-Fraud Committee

RACI Matrix: A responsibility assignment chart that defines the roles and responsibilities for tasks. It stands for Responsible, Accountable, Consulted, and Informed.

TAP: Transferred Account Procedure

VLR: Visitor Location Register

VPMN: Visited Public Mobile Network

WATRA: West Africa Telecommunications Regulators Assembly