Validé le 10/08/2025

PRINCIPES DIRECTEURS DE GESTION DE LA FRAUDE

(Initiative régionale de roaming de la CEDEAO)

Table des matières

Résumé 3
1. Contexte 4
2. Objectif 5
2.1 Comités nationaux et régionaux de lutte contre la fraude 6
2.2 Risques potentiels de fraude 8
2.3 Lignes directrices générales pour la gestion et la prévention de la fraude : 12
2.3.1 Anti-FKPI_001 : 14
2.3.1.1 Description du contrôle/KPI : 14
2.3.1.2 RACI (Responsable/Redevable/Consultatif/Informatif) : 14
2.3.2 Anti-FKPI_002 : 15
2.3.2.1 Description du contrôle/KPI : 15
2.3.2.2 RACI (Responsable/Redevable/Consultatif/Informatif) : 15
2.3.3 Anti-FKPI_003 : 15
2.3.3.1 Description du contrôle/KPI : 15
2.3.3.2 RACI (Responsable/Redevable/Consultatif/Informatif) : 16
2.3.4 Anti-FKPI_004 : 16
2.3.4.1 Description du contrôle/KPI : 16
2.3.4.2 Responsable/Redevable/Consultation/Information (RACI) : 16
2.3.5 Anti-FKPI_005 : 17
2.3.5.1 Description du contrôle/KPI : 17
2.3.5.2 Responsable/Redevable/Consultant/Informateur (RACI) : 17
2.3.6 Anti-FKPI_006 : 17
2.3.6.1 Description du contrôle/KPI : 17
2.3.6.2 Responsable/Redevable/Consulter/Informer (RACI) : 17
2.3.7 Anti-FKPI_007 : 17
2.3.7.1 Description du contrôle/KPI : 17
2.3.7.2 Responsable/Redevable/Consultant/Informateur (RACI) : 18
2.4 Matrice d'assistance technique et de recours 18
2.5 Signalement des fraudes 18
ANNEXE 1 19
ANNEXE 2 19
ANNEXE 3 21

Résumé

Le règlement C/Reg.21/12/17 de la CEDEAO sur l'itinérance sur les réseaux publics de communications mobiles dans la région de la CEDEAO, article 15(2), exige des États membres qu'ils mettent en place des comités chargés de lutter contre la fraude dans le domaine de l'itinérance communautaire.

Les résolutions 1, 2 et 3 de la DG de l'ANR exigeaient la création de comités nationaux et régionaux chargés d'élaborer des mécanismes de contrôle de la fraude aux niveaux national et régional afin de traiter efficacement les problèmes de fraude lorsque le service d'itinérance deviendrait opérationnel. Sur la base du mandat susmentionné, le Comité technique de mise en œuvre a créé un Comité régional de lutte contre la fraude (RAFC) dirigé par le Ghana.

La première réalisation du RAFC a été l'élaboration d'un plan de travail pour la gestion de la fraude. Ce plan de travail détaillait les activités proposées/prévues pour remplir ce mandat.

Le comité a ensuite élaboré une matrice de gestion de la fraude à remplir par les États membres afin de lui permettre de connaître la situation des pays en matière de gestion de la fraude. Le comité a ensuite défini le mandat ci-dessous afin de guider les travaux des comités nationaux et régionaux de lutte contre la fraude.

Mandat des comités nationaux de lutte contre la fraude

- Documenter les activités frauduleuses actuellement répandues dans le pays.
- Identifier les types de fraude potentiels qui pourraient survenir.
- Évaluer les cadres juridiques existants en matière de gestion et de contrôle de la fraude

Mandat du comité régional de lutte contre la fraude

- Identifier et mettre en évidence les types de fraude potentiels susceptibles de survenir à la suite de la mise en œuvre.
- Élaboration de lignes directrices antifraude sous la forme de contrôles visant à atténuer la fraude et d'indicateurs clés de performance (KPI) de suivi.
- Coordonner les activités des différents comités nationaux de lutte contre la fraude en relation avec l'initiative de libre circulation de la CEDEAO, entre autres typologies de fraude
- Faire le point et évaluer l'adéquation des infrastructures de gestion de la fraude des États membres pour une gestion efficace et efficiente de la fraude
- Élaborer des protocoles pour guider le traitement des numéros de fraude détectés (MSISDN) par les États membres.
- Évaluer et recommander des systèmes et des outils de gestion de la fraude.
- Élaborer et mettre en œuvre des exigences appropriées en matière de signalement des fraudes et examiner régulièrement les rapports des États membres.
- Fournir un soutien technique aux États membres pour la mise en œuvre des contrôles et des indicateurs clés de performance

Sur la base des réponses relatives à la gestion de la fraude, les États membres qui ne disposaient pas de comités nationaux de lutte contre la fraude ont été aidés à en créer. Ceux qui ne disposaient pas d'un cadre juridique spécifique pour gérer la fraude dans le

domaine des télécommunications ont reçu des lignes directrices et, dans certains cas, des exemples de cadres juridiques d'autres pays ont été partagés afin de les guider à cet égard. Presque tous les pays disposaient d'une forme ou d'une autre de système de gestion de la fraude au niveau des opérateurs. D'autres en disposaient à la fois au niveau des opérateurs et des ANR. Presque tous les pays, à l'exception de deux (2), avaient mis en place un système d'identification national robuste. D'autres étaient en train de le mettre en place, soit au niveau des opérateurs, soit au niveau national.

Sur la base des résultats attendus dans le cahier des charges et des mises à jour sur la gestion de la fraude fournies par les pays, le comité a identifié les risques potentiels de fraude et les indicateurs clés de performance (KPI) antifraude qui serviront de contrôles pour atténuer la fraude. Un modèle de signalement de fraude a également été élaboré afin de guider les opérateurs des États membres dans le signalement des activités frauduleuses identifiées.

La fraude dans le domaine des télécommunications n'est pas statique mais plutôt dynamique. Le Comité régional de lutte contre la fraude recommande donc aux opérateurs de se conformer strictement aux mesures de contrôle identifiées pour atténuer la fraude. Ceux qui ne disposent pas de l'équipement nécessaire pour atténuer les risques de fraude anticipés doivent acheter de toute urgence les modules et/ou logiciels nécessaires pour se conformer aux mesures de contrôle proposées.

Outre la recommandation ci-dessus, il sera nécessaire de disposer d'une plateforme de contrôle de gestion de la fraude de troisième niveau pour gérer la fraude au niveau régional.

Les fournisseurs potentiels de solutions et d'outils de gestion de la fraude ont été engagés dans le cadre des exigences en matière de risques de fraude. L'équipe régionale sera chargée de mettre en œuvre ces déploiement au niveau national et régional.

Pour des raisons d'efficacité opérationnelle et de protection des données, toute solution adoptée sera structurée de manière à traiter les données et à appliquer la logique de détection au niveau national, tandis que les informations d'alerte et les détails récapitulatifs seront partagés au niveau régional.

1. Contexte :

L'initiative de la CEDEAO en matière d'itinérance est une initiative proposée par les ministres des télécommunications/TIC de la CEDEAO lors de leur réunion au Niger en 2016. Cette initiative vise notamment à :

i. harmoniser les tarifs/frais d'itinérance au sein de la région de la CEDEAO
ii. faciliter les communications et le commerce transfrontaliers

Dans le cadre de cette politique, le règlement C/REG. 21/12/17 relatif à l'itinérance sur les réseaux publics de communications mobiles dans la région de la CEDEAO a été adopté. Ce règlement exige également des États membres qu'ils mettent en place des comités chargés de lutter contre la fraude dans le domaine de l'itinérance communautaire.

En 2019, les ministres des Communications/Télécommunications/TIC de la sous-région ont lancé un nouvel appel pour lancer l'initiative de roaming de la CEDEAO, compte tenu du commerce de la CEDEAO, de la connectivité transfrontalière et des frais de roaming susceptibles d'entraver les progrès commerciaux.

Conscients de l'afflux potentiel de fraudes par contournement avec la mise en œuvre de l'initiative de libre itinérance de la CEDEAO, les directeurs généraux et les présidents des autorités nationales de régulation (ANR) de la CEDEAO, lors de leur 2réunion de haut niveau en mars 2021, ont réitéré la nécessité de créer des comités nationaux et régionaux de lutte contre la fraude avant le 31 mai 2021, conformément à l'article 20 du règlement n° C/REG.21/12/17. En outre, les ANR ont été invitées à définir un dispositif technique et des mécanismes efficaces de contrôle de la fraude aux niveaux national et régional avant le **30 juin 2021.**

Des risques de fraude inhérents aux services de télécommunications généraux, en particulier à l'itinérance, sont à prévoir dans toute la sous-région dès lors que l'importation de cartes SIM sera autorisée dans le cadre de cette initiative. Il est donc essentiel de mettre en place des mécanismes antifraude solides afin d'atténuer les risques anticipés.

2. Objectif :

L'objectif de ce cadre est de préciser les principaux objectifs du programme de lutte contre la fraude de l'ARTAO en relation avec l'initiative d'itinérance de la CEDEAO, comme suit :

1. Coordonner la mise en place de comités nationaux et régionaux de lutte contre la fraude,
    - Assurer la coordination administrative
    - Mettre en place des outils de coordination technique

2. Identifier et mettre en évidence les types de fraude potentiels pouvant survenir après la mise en œuvre.

3. Développer des mécanismes de contrôle atténuants et des indicateurs clés de performance (KPI) de surveillance.

4. Fournir un soutien technique pour la mise en œuvre de ces contrôles et indicateurs clés de performance

5. Surveiller en permanence l'efficacité des contrôles et des indicateurs clés de performance.

6. Examiner sur le plan technique et proposer une solution de gestion de la fraude aux opérateurs des États membres, si nécessaire.

2.1 Comités nationaux et régionaux de lutte contre la fraude

La gestion de la fraude s'effectue à trois niveaux :

- Niveau des opérateurs de réseaux mobiles : les ANR doivent s'assurer que chaque opérateur de réseau mobile a mis en place une solution de lutte contre la fraude

- Au niveau des ANR : les autorités réglementaires nationales doivent mettre en place un comité national et une plateforme, ainsi que des mécanismes de collaboration et de contrôle des activités de lutte contre la fraude, conformément à la réglementation de la CEDEAO.

- Au niveau régional: le Ghana coordonnera toutes les activités de signalement des fraudes au niveau de la CEDEAO, tandis que la plateforme régionale servira d'outil principal de lutte contre la fraude au niveau régional.

À la suite de la sélection du Ghana comme pays chef de file pour la gestion de la lutte contre la fraude, une équipe a été constituée à partir de son comité national de lutte contre la fraude afin d'entamer un engagement au niveau sous-régional. Celle-ci s'est ensuite transformée en un **comité régional de lutte contre la fraude (RAFC)** avec la nomination de deux (2) représentants de l'ARN de chaque État membre.

Le Comité régional a fourni des lignes directrices et un soutien aux ARN respectives afin qu'elles constituent leur propre **comité national de lutte contre la fraude (RAFC)**.

La composition et le mandat des comités nationaux et régionaux de lutte contre la fraude sont les suivants :

Comité national de lutte contre la fraude (NAFC)

- **Composition :**
    - Président : représentant de l'autorité nationale de régulation (ANR)
    - Vice-président : nommé par les membres du NAFC
    - Membres : deux (2) représentants de chaque opérateur de réseau mobile (ORM) agréé, des représentants des agences de sécurité de l'État concernées et du ministère chargé des communications.
    - Secrétariat : L'ANR assure le secrétariat.
- **Mandat et objectifs :**
    - Servir d'organisme national principal pour toutes les activités de gestion de la fraude liées à l'itinérance.
    - Mettre en œuvre et appliquer les directives régionales en matière de lutte contre la fraude et les indicateurs clés de performance (KPI) au niveau national.

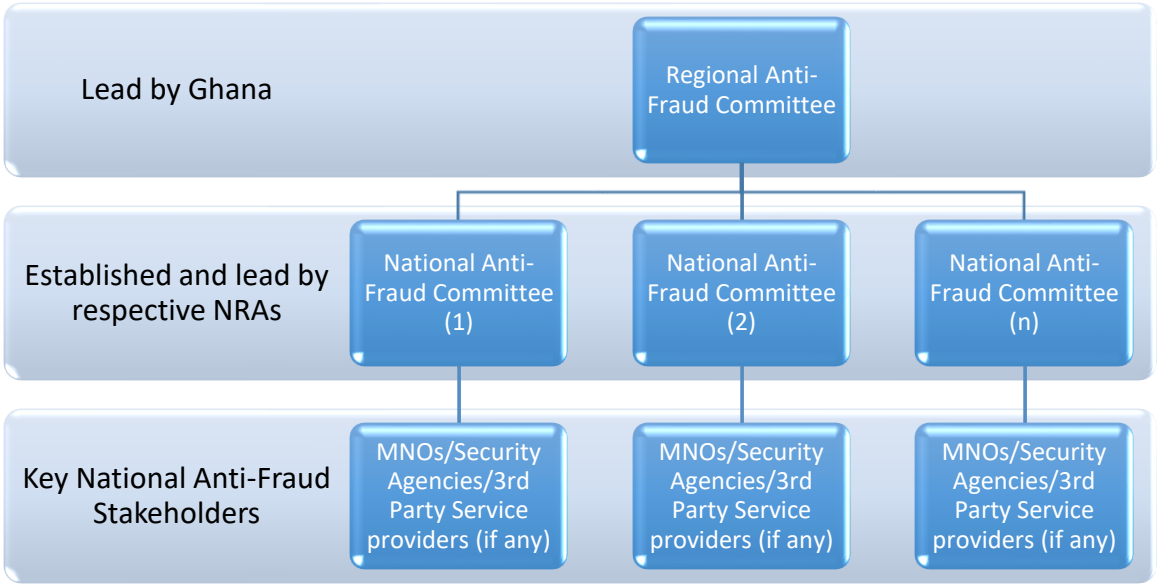
- Identifier, enquêter et soumettre des rapports sur les incidents de fraude à l'aide de modèles standardisés.
- Faciliter la collaboration et le partage d'informations entre les opérateurs de réseaux mobiles nationaux et avec le RAFC.
- Évaluer l'adéquation des cadres juridiques nationaux pour poursuivre les fraudes dans le domaine des télécommunications et recommander les réformes nécessaires.
- Veiller à ce que tous les opérateurs nationaux de réseaux mobiles disposent de systèmes de gestion de la fraude (FMS) fonctionnels et conformes aux normes régionales.
- Évaluer l'efficacité des contrôles antifraude mis en œuvre par les opérateurs de réseaux mobiles.

Comité régional de lutte contre la fraude (RAFC)

- **Composition :**
  - Dirigé par le pays chef de file (Ghana).
  - Membres : Deux (2) experts techniques désignés par l'ANR de chaque État membre de la CEDEAO.
  - Observateurs: représentants de l'ARTAO et de la Commission de la CEDEAO.
- **Mandat et objectifs :**
  - Fournir une orientation stratégique et coordonner les activités des différents comités nationaux de lutte contre la fraude dans le cadre de l'initiative régionale de l'CEDEAO en matière d'itinérance, entre autres types de fraude.
  - Élaborer, publier et maintenir ces lignes directrices, contrôles et indicateurs clés de performance en matière de lutte contre la fraude.
  - Recevoir, analyser et donner suite aux signalements de fraude provenant de tous les NAFC.
  - Identifier les nouveaux types de fraude transfrontalière et élaborer des stratégies d'atténuation appropriées.
  - Élaborer des protocoles pour guider le traitement des MSISDN frauduleux détectés par les comités nationaux de lutte contre la fraude respectifs.
  - Fournir des plans d'action corrective aux États membres dont les performances sont insuffisantes.
  - Évaluer et recommander des systèmes et des outils de gestion de la fraude.

- Mener des campagnes antifraude périodiques dans toute la sous-région avec le soutien des ANR/NAFC respectives.
- Élaborer et mettre en œuvre des exigences appropriées en matière de signalement des fraudes et examiner régulièrement les rapports des États membres.
- Renforcer les capacités et fournir un soutien technique aux NAFC et aux ORM.
- Rendre compte périodiquement au Comité des ministres des télécommunications/TIC de la CEDEAO de la situation en matière de fraude dans la région d'itinérance.

Les activités de lutte contre la fraude sont structurées comme suit :



2.2 Risques potentiels de fraude

L'initiative d'itinérance de la CEDEAO est susceptible d'être exposée à plusieurs types de fraude. Vous trouverez ci-dessous une classification basée sur l'impact potentiel et la probabilité :

Type de fraude	Description/scénario	Niveau de risque	Mesures d'atténuation proposées (voir section 2.3)
Contournement de la carte SIM	Terminaison illégale d'appels internationaux via des cartes SIM locales afin d'éviter les frais de passerelle internationale. *Par exemple, un fraudeur installe un appareil équipé de plusieurs cartes SIM locales au Bénin afin de terminer des appels destinés à des numéros nigérians, contournant ainsi les tarifs internationaux.*	Élevé	Réf. : Anti-FKPI_003
IRSF/PRS (Partage des revenus internationaux/Service à tarif majoré) Fraude	Génération d'appels vers des numéros surtaxés afin de percevoir une part des revenus. *Exemple : la carte SIM d'un utilisateur en itinérance est piratée et utilisée pour appeler des numéros surtaxés dans un pays lointain, générant des coûts énormes pour l'opérateur d'origine.*	Élevé	Référence : Anti-FKPI_001
Wangiri (One-Ring)	Passer des appels manqués pour inciter à rappeler des numéros d' s surtaxés. *Par exemple, un utilisateur en itinérance reçoit un appel manqué. Lorsqu'il rappelle, il est connecté à un numéro surtaxé, ce qui entraîne des frais importants.*	Moyen	Référence : Anti-FKPI_004
Fraude à l'abonnement	Obtenir un service sans intention de payer, souvent à l'aide de fausses	Moyen	Vérification des identités nationales, Réf. : Anti-FKPI_004

Type de fraude	Description/scénario	Niveau de risque	Mesures d'atténuation proposées (voir section 2.3)
	pièces d'identité. *Par exemple, une personne utilise une fausse pièce d'identité pour acquérir plusieurs cartes SIM dans le but spécifique de se livrer à des activités frauduleuses en itinérance.*		
Spam SMS A2P	Contournement des voies de facturation/de paiement légitimes pour l'acheminement de SMS en masse d'application à personne. *Par exemple, un fournisseur de contenu contourne le canal A2P officiel en utilisant un ensemble de cartes SIM d'itinérance pour envoyer des SMS en masse, échappant ainsi à des frais plus élevés.*	Moyen	Référence : Anti-FKPI_002, Anti-FKPI_006
Usurpation d'identité CLI	Manipulation de l'identité de la ligne appelante afin de masquer la véritable origine d'un appel. *Par exemple, un fraudeur usurpe le numéro officiel d'une banque pour mener des attaques de phishing contre des utilisateurs en itinérance.*	Élevé	Sécurité de la signalisation (par exemple, STIR/SHAKEN), Réf. : Anti-FKPI_004
Fraude aux cartes SIM de test	Utilisation abusive de cartes SIM destinées à tester l'interopérabilité des réseaux et les accords d'itinérance. Par exemple, un employé d'un	Moyen	Accords bilatéraux stricts limitant la quantité, l'utilisation (plafonds de données/appels/SMS) et la durée de vie des

Type de fraude	Description/scénario	Niveau de risque	Mesures d'atténuation proposées (voir section 2.3)
	opérateur fournit un grand nombre de cartes SIM de test à un tiers qui les utilise pour ses communications personnelles ou pour générer du trafic illicite, échappant ainsi aux frais.		cartes SIM de test. Audits et surveillance réguliers pour détecter les modèles de trafic anormaux. Nécessite une intervention du réseau responsable dans les 96 heures.
Itinérance permanente	Un abonné utilise en permanence une carte SIM d'un pays à bas coût dans un pays à coût élevé afin de bénéficier de tarifs d'abonnement moins élevés. Par exemple, un abonné du pays A (tarifs élevés) utilise une carte SIM du pays B (tarifs bas) avec des frais d'itinérance avantageux, sans jamais revenir sur le réseau HPMN.	Élevé	Mettre en œuvre et appliquer les « politiques d'utilisation de l'itinérance » dans les conditions générales. Déployer des outils de surveillance (Anti-FKPI_005) pour identifier les abonnés dont la durée d'itinérance est excessive et continue (par exemple, > 3 mois) et prendre des mesures (par exemple, surcoûts, restriction de service). Nécessite une action de la part du réseau responsable dans les 48 heures.

Parmi les autres types de fraude, l'initiative d'itinérance de la CEDEAO devrait être exposée aux risques de fraude suivants :

- **SIM Box** – Consiste à contourner la passerelle internationale légitime pour acheminer le trafic international entrant via un MSISDN local.

- **Usurpation d'identité CLI et réenregistrement de numéro A** – Désigne la falsification délibérée d'un numéro d'appel.

- **IRSF/PRS (fraude liée au partage des revenus internationaux/aux services à taux majoré)** – Se caractérise par la génération de trafic vers des destinations à tarif élevé et à taux majoré dans le but d'obtenir une part des revenus générés.

- **Fraude à l'abonnement** – Se produit en accédant et en utilisant des services qui n'étaient pas initialement payés dans le cadre de l'offre d'une personne grâce à la manipulation du système.

- **Fraude à l'utilisation intensive** – Implique une utilisation abusive résultant d'un défaut de facturation et/ou d'autres

- **Spam SMS A2P** – Implique l'envoi massif de SMS générés par un système via des voies non autorisées, contournant les mécanismes de facturation légitimes et souvent utilisés pour des communications non sollicitées ou frauduleuses.

2.3 Directives générales pour la gestion et la prévention de la fraude :

- Toutes les cartes SIM en itinérance entrante doivent avoir au moins quinze (15) jours d'historique d'utilisation dans leur pays d'origine avant d'être autorisées à utiliser l'itinérance sur un réseau visité. Les cartes SIM qui ne répondent pas à ce critère se verront temporairement refuser l'accès à tous les services d'itinérance. Le réseau visité doit signaler et communiquer au réseau d'origine de l'itinérant entrant tout itinérant présentant une activité suspecte afin de vérifier son statut. Le réseau visité n'accordera l'accès à l'itinérance qu'après avoir vérifié le statut de l'itinérant entrant.
- Tous les opérateurs de réseaux mobiles doivent soumettre un rapport mensuel détaillé sur toutes les activités de gestion de la fraude, conformément au tableau figurant à l'annexe 1.

A. Processus de gestion de la fraude par étapes :

1. Prévention : les ORM doivent mettre en œuvre des contrôles proactifs (par exemple, enregistrement de la carte SIM, incubation de la carte SIM pendant 15 jours, échange NRTRDE).
2. Détection : surveiller le trafic 24 heures sur 24, 7 jours sur 7, par rapport aux seuils KPI configurés dans le FMS.
3. Réponse : en cas d'alerte, suspendre automatiquement ou manuellement le service conformément aux tableaux RACI ci-dessous et ouvrir une enquête.
4. Signalement : documenter l'incident sur les portails nationaux et régionaux (annexe 1).
5. Analyse : l'équipe régionale corrèle les données afin d'identifier les tendances et d'affiner la logique de détection.
6. Affinement : mettre à jour les règles et les contrôles du FMS sur la base de l'analyse.

B. Matrice RACI standard (aperçu) :

- Responsable (R) : entité qui exécute la tâche.

- Responsable (A) : Entité qui répond en dernier ressort de la bonne exécution de la tâche.
- Consulté (C) : entité qui fournit des informations.
- Informé (I) : entité tenue informée de l'avancement. *(Une matrice RACI détaillée est fournie pour chaque KPI dans les sections 2.3.1-7)*

C. Incubation SIM et seuil de dépenses minimum :

- La règle relative à l'historique d'utilisation sur 15 jours (section 2.3) est une période d'incubation obligatoire visant à établir le comportement légitime de l'abonné.
- Les ARN peuvent également envisager un *seuil minimum de dépenses* sur le réseau domestique comme indicateur supplémentaire de crédibilité, afin de garantir le respect des réglementations en matière de protection des consommateurs.

D. Responsabilité partagée et escalade :

- La gestion de la fraude est une responsabilité partagée entre les réseaux d'origine et les réseaux visités, comme le détaille le RACI par KPI.
- Voie d'escalade: Équipe de lutte contre la fraude des opérateurs de réseaux mobiles -> NAFC national -> RAFC régional -> ARTAO/CEDEAO. Les délais d'escalade doivent être définis dans le protocole d'accord.

E. NRTRIE (échange de données d'itinérance en temps quasi réel) :

- La mise en œuvre des mécanismes NRTRIE est obligatoire pour tous les OTM afin de permettre l'échange en temps quasi réel des données d'utilisation de l'itinérance. Cela est essentiel pour le contrôle du crédit en temps réel, la surveillance de la fraude et la prévention des factures exorbitantes, comme le complète l'Anti-FKPI_005. Tous les opérateurs de réseaux mobiles doivent mettre en œuvre des systèmes permettant d'échanger des fichiers TAP (ou des enregistrements de données normalisés équivalents) pour les utilisateurs en itinérance sortante dans un délai minimisé convenu d'un commun accord (par exemple, toutes les 2 à 4 heures). Cela permet au réseau d'origine d'effectuer une surveillance de l'utilisation en temps quasi réel, un contrôle du crédit et une détection de l' e de fraude sur la base des données d'utilisation réelles du réseau visité, évitant ainsi les factures exorbitantes et améliorant considérablement les capacités de lutte contre la fraude. Le support et le format choisis doivent faire l'objet d'un accord dans le cadre d'accords d'itinérance bilatéraux.

F. Rôles dans la suspension du service :

- Le réseau d'origine est chargé de suspendre les services des utilisateurs en itinérance à l'étranger sur la base des alertes reçues des réseaux visités ou de ses propres contrôles de crédit/fraude.

G. Sanctions en cas de non-conformité :

- Les ARN, avec le soutien du RAFC, élaboreront un cadre de sanctions financières conditionnelles pour les ORM qui ne mettent pas en œuvre les contrôles, ne répondent pas aux alertes ou ne fournissent pas les données requises, ce qui entraîne des litiges de facturation non résolus ou des pertes de revenus évitables pour les partenaires.

H. Contrôles préventifs et politiques d'utilisation équitable :

  - Plafonds d'itinérance de gros : les ORM doivent mettre en œuvre des plafonds financiers de gros afin de limiter l'exposition financière liée aux activités d'itinérance frauduleuses.
  - Politique d'utilisation équitable (FUP) : Les ORM peuvent mettre en œuvre une FUP pour :
    - Itinérance permanente : pour empêcher les abonnés de résider et d'opérer de manière permanente dans un réseau visité.
    - Appels entrants gratuits : pour empêcher l'abus des offres d'appels entrants illimités.
    - Promotions au détail : définir la durée et la portée de toute offre d'itinérance à prix réduit.
  - Nombre maximal de comptes par abonné : les réseaux d'origine doivent mettre en place des règles visant à limiter le nombre de cartes SIM d'itinérance actives par abonné à un nombre raisonnable (par exemple, 2 ou 3).
- Utilisation d'outils avancés : les opérateurs de réseaux mobiles sont encouragés à utiliser des modules d'intelligence artificielle (IA) et d'apprentissage automatique (ML) dans leur FMS pour une détection proactive et prédictive des fraudes, allant au-delà des règles statiques basées sur des seuils.

Contrôles spécifiques de lutte contre la fraude et matrice des indicateurs clés de performance

2.3.1 Anti-FKPI_001 :

Surveillance du trafic vers les destinations figurant sur la liste noire par les abonnés en visite (itinérants entrants)

2.3.1.1 Description du contrôle/KPI :

Lorsqu'il est en itinérance sur un réseau visité, le trafic généré par un itinérant entrant doit être
surveillé afin de détecter toute activité frauduleuse IRSF/PRS. Le contrôle doit être configuré sur le
FMS du réseau visiteur et surveillé 24 heures sur 24, 7 jours sur 7. Les services doivent être suspendus pour les numéros qui
enfreignent les contrôles et les détails doivent être communiqués au réseau d'origine et à l'autorité de régulation compétente. (Voir l'annexe 2 pour le seuil de contrôle applicable)

Le réseau d'origine doit être informé afin de bloquer la plage de numéros suspectés.
Après une période sans réponse, le réseau visité doit bloquer complètement le réseau de ces numéros.

2.3.1.2 RACI (Responsable/Redevable/Consulter/Informer):

R - Opérateur du réseau hôte/visité
I – Comité national de lutte contre la fraude
A/C – Opérateur du réseau d'origine.

2.3.2 ANTI-FKPI_002 :

Surveillance de l'utilisation intensive.
* Cet indicateur clé de performance couvrira les mesures suivantes, telles que fournies à l'annexe 2 :
* Nombre moyen de SMS envoyés par un utilisateur en itinérance dans l'heure et dans les 24 heures.
* Moyenne des minutes de communication sortantes par un utilisateur en itinérance dans l'espace de couverture pendant une heure et 24 heures.
* Volume moyen de données utilisées par un utilisateur en itinérance au cours d'une heure et de 24 heures.

2.3.2.1 Contrôle/Description de l'indicateur clé de performance :

Les transactions/volumes d'itinérance entrants doivent être surveillés afin de détecter toute utilisation dépassant les seuils fixés. Ces seuils doivent être configurés sur le FMS du réseau visiteur et surveillés 24 heures sur 24, 7 jours sur 7.
Le réseau d'origine doit être informé afin de suspendre les services des abonnés qui dépassent le seuil.

***Mettre en place un réseau d'origine responsable du blocage des appels vocaux, des données et des SMS.**

2.3.2.2 RACI (Responsable/Redevable/Consulter/Informer) :

R - Opérateur du réseau hôte/visité
I – Comité national de lutte contre la fraude
A/C – Réseau d'origine

2.3.3 ANTI-FKPI_003 :

Surveillance du contournement de la terminaison du trafic international (SIM Box).

2.3.3.1 Description du contrôle/KPI :

Les itinérants entrants doivent être surveillés afin de détecter tout contournement de la terminaison du trafic international sur les réseaux d'origine et visiteurs. Une solution de détection des boîtiers SIM doit être déployée et configurée pour signaler ces cartes SIM. Les cartes SIM détectées doivent être supprimées de la base de données VLR du réseau hôte et les détails pertinents doivent être communiqués au réseau d'origine.

*Le réseau visité est capable de détecter et de signaler les itinérants contournant le réseau sur son VLR, en coordination avec le réseau d'origine. Il est impératif que le réseau visité communique toutes les détections au réseau d'origine afin de garantir la synchronisation des efforts de lutte contre la fraude.
*Dès la détection, le réseau visité doit immédiatement informer le réseau d'origine tout en initiant le blocage des cartes SIM identifiées**.**

2.3.3.2 RACI (Responsable/Redevable/Consulter/Informer) :

R - Opérateur réseau hôte/visité
I – Comité national de lutte contre la fraude
A/C – Réseau d'origine

2.3.4 ANTI-FKPI_004 :

Surveillance des comportements et/ou schémas d'appels inhabituels.

2.3.4.1 Description du contrôle/KPI :

Des règles doivent être configurées dans le système de gestion de la fraude (FMS) afin de surveiller et de signaler
les comportements et modèles d'appels inhabituels en itinérance. Ces comportements peuvent inclure, sans s'y limiter:

- **Premier appel passé lors de l'enregistrement en itinérance** : peut indiquer l'activation automatisée d'une carte SIM Box.
- **Appels d'une durée inhabituellement longue** : cela pourrait suggérer une génération artificielle de trafic ou un gonflement des appels.
- **Appels initiés via la fonctionnalité de transfert d'appel** : souvent exploités dans les scénarios de contournement.
- **Volume élevé d'appels de courte durée** : typique de la fraude par SIM Box ou par terminaison.
- **Appels vers des destinations à haut risque ou des numéros surtaxés** : peut indiquer une fraude au partage des revenus.
- **Cartes SIM générant du trafic sans événements de mobilité correspondants** : suggère une utilisation non humaine.
- **Activité d'itinérance incompatible avec le profil ou l'historique de l'abonné** : signe avant-coureur d'une utilisation abusive.
- **Plusieurs cartes SIM présentant des schémas d'appel identiques** : peut indiquer une fraude coordonnée.

Les services doivent être suspendus pour les numéros qui enfreignent le contrôle et les détails communiqués au réseau d'origine.

2.3.4.2 Responsable, Redevable, consulter, informer (RACI) :

R - Opérateur du réseau hôte/visité et réseau d'origine
I – Comité national de lutte contre la fraude
A/C – Réseau d'origine

2.3.5 ANTI-FKPI_005 :

Échange de données d'itinérance (NRTRDE).

2.3.5.1 Description du contrôle/KPI :

Les transactions d'itinérance sortantes sont généralement traitées et facturées par les opérateurs d'origine respectifs. Cependant, l'enregistrement initial de ces transactions est effectué par le réseau visité. Il est donc essentiel que le réseau visité partage rapidement ces informations avec le réseau d'origine de l'abonné via un canal de communication convenu. Cela garantit un contrôle efficace de l'utilisation et des limites de crédit, et contribue à éviter les factures exorbitantes à la fin du cycle de facturation.

2.3.5.2 Responsable/Redevable/Consulter/Informer (RACI) :

R/A - Opérateur du réseau hôte/visité
C – Réseau d'origine

2.3.6 ANTI-FKPI_006 :

Définir et surveiller la limite d'utilisation des données.

2.3.6.1 Contrôle/Description des indicateurs clés de performance :

Les abonnés en itinérance entrants accèdent aux données via le nœud de support GPRS (GGSN) de la passerelle visiteur. Une limite en termes de volume d'utilisation des données doit être convenue et définie par les réseaux visiteurs pour les abonnés partenaires respectifs, afin de servir de base à la surveillance et au contrôle des utilisations élevées.
Le seuil convenu doit être configuré sur le FMS du réseau visiteur pour permettre une surveillance efficace.
Remarque :
** Ce sont les volumes qui sont pris en compte et non les coûts, car chaque opérateur mobile applique des tarifs spécifiques.
** Les numéros signalés doivent être communiqués au réseau domestique**.**

2.3.6.2 Responsable/Redevable/Consulter/Informer (RACI) :

R/A - Opérateur du réseau hôte/visité
I – Comité national de lutte contre la fraude
C – Réseau d'origine

2.3.7 ANTI-FKPI_007 :

Empêcher l'échange de cartes SIM pour les utilisateurs en itinérance sortante.

2.3.7.1 Contrôle/Description des indicateurs clés de performance :

Les opérateurs de réseaux mobiles doivent interdire les échanges de cartes SIM lorsque le numéro d'un abonné est en itinérance sortante. Une telle activité présente un risque important pour l'intégrité du service, la prévention de la fraude et l'exactitude de la facturation.

Les fraudeurs utilisent cette stratégie pour prendre le contrôle de comptes de services légitimes à des fins frauduleuses.

2.3.7.2 Responsable/Redevable/Consulter/Informer (RACI) :

R/A - Réseau domestique.
I – Comité national de lutte contre la fraude

2.4 Assistance technique et matrice d'escalade

A. Services dédiés à la lutte contre la fraude :
Chaque ARN et chaque ORM doit mettre en place un service dédié à la fraude, disponible 24 heures sur 24 et 7 jours sur 7, dont les coordonnées (e-mail, téléphone) sont communiquées à tous les réseaux partenaires et au RAFC.
B. Processus d'escalade standard :

Niveau de gravité	Critères	Action et calendrier	Procédure d'escalade
Niveau 1 (critique)	Perte de revenus importante (> 10 000 $), attaque en cours, violation critique du système.	Action immédiate requise.	Service de lutte contre la fraude des opérateurs de réseaux mobiles (MNO) -> Service de lutte contre la fraude des opérateurs de réseaux mobiles partenaires -> NAFC -> RAFC (dans l'heure)
Niveau 2 (majeur)	Perte de revenus importante, plusieurs MSISDN concernés.	Action dans les 2 à 4 heures.	Service de lutte contre la fraude des opérateurs mobiles -> Service de lutte contre la fraude des opérateurs mobiles partenaires -> NAFC (dans les 4 heures)
Niveau 3 (mineur)	Incident isolé, faible impact financier.	Action dans les 24 heures.	Service de lutte contre la fraude des opérateurs mobiles -> Service de lutte contre la fraude des opérateurs mobiles partenaires (dans les 24 heures)

2.5 Signalement des fraudes

Un outil/portail centralisé de signalement doit être mis en place pour permettre aux opérateurs de téléphonie mobile concernés de signaler directement les incidents dans les pays ayant conclu des accords d'itinérance.

Signalement obligatoire : indépendamment des signaux d'alerte individuels ou des mécanismes de détection, chaque opérateur mobile est tenu de soumettre des rapports de détection de fraude via le portail centralisé. Ce portail fonctionne indépendamment de tout système de gestion des fraudes spécifique à un opérateur afin de garantir la cohérence et la transparence des signalements.

Formation et intégration : tous les points de contact uniques (SPOC) désignés par les opérateurs de réseaux mobiles participants suivront une formation sur l'utilisation correcte du portail et les procédures standardisées de signalement des incidents frauduleux. Cela garantit l'uniformité de la soumission des données et renforce la collaboration entre les réseaux en matière de lutte contre la fraude**.**

Les données seront analysées par l'équipe régionale et les résultats serviront à vérifier les incidents qui seront signalés ou non par la solution FMS régionale, ainsi qu'à affiner la logique des solutions FMS respectives (opérateurs de réseaux mobiles et NAFC) au fil du temps.

ANNEXE 1

Les incidents de fraude enregistrés par les opérateurs de réseaux mobiles dans les États membres respectifs dans le cadre de l'initiative régionale d'itinérance de la CEDEAO doivent être signalés chaque mois à l'aide du modèle ci-dessous :

Date de l'incident	Type de fraude	Nombre de MSISDN concernés	Nom/pays de l'opérateur d'origine	Perte de revenus (USD)	Perte de revenus évitée (USD)	Mesures prises	Statut de l'incident

ANNEXE 2

Seuils de contrôle pour les indicateurs clés de performance en matière de fraude (échantillon de données provenant d'opérateurs de réseaux mobiles du Bénin et du Ghana)

	Nombre de préoccupations					Pourcentage	
Type de fraude	**Oui**	**Non**			**Type de fraude**	**Oui**	**Non**
Boîte SIM	6	0			Boîtier SIM	100	0
Boîte SIM internationale	6	0			Boîtier SIM international	100	0
Usurpation d'identité CLI et réenregistrement du numéro A	5	1			Usurpation d'identité CLI et réenregistrement du numéro A	83	17
IRSF/PRS (fraude liée au partage des revenus internationaux/aux services à taux majoré)	6	0			IRSF/PRS (fraude liée au partage des revenus internationaux/aux services à taux majoré)	100	0

Fraude à l'abonnement	4	2			Fraude à l'abonnement	67	33
Fraude liée à une utilisation excessive	6	0			Fraude liée à une utilisation intensive	100	0
Spam SMS A2P (y compris les appels flash)	6	0			Spam SMS A2P (y compris les appels flash)	100	0

	Nombre de préoccupations					Nombre de préoccupations	
KPI	**Oui**	**Non**			**KPI**	**Oui**	**Non**
Surveillance du trafic vers les destinations figurant sur la liste noire par les abonnés en visite (itinérants entrants)	5	1			Surveillance du trafic vers les destinations figurant sur la liste des destinations fréquentes des abonnés en visite (itinérants entrants)	83	17
Surveillance de l'utilisation intensive	6	0			Surveillance de l'utilisation intensive	100	0
Moyenne des SMS envoyés par un utilisateur en itinérance entrante en une heure et en 24 heures	3	3			Moyenne des SMS envoyés par un utilisateur en itinérance entrante en une heure et en 24 heures	50	50 %
Moyenne des MOU sortants par un utilisateur en itinérance entrante en une heure et en 24 heures	3	3			MOU sortant moyen d'un utilisateur en itinérance entrant en une heure et en 24 heures	50	50
Volume moyen de données utilisé par un utilisateur en itinérance entrante en une heure et en 24 heures	3	3			Volume moyen de données utilisé par un utilisateur en itinérance entrante en une heure et en 24 heures	50	50
Contrôle du contournement de la terminaison du trafic international (SIM Box)	6	0			Surveillance du contournement de la terminaison du trafic international (SIM Box)	100	0
Surveillance des comportements et/ou schémas d'appels inhabituels	5	1			Surveillance des comportements et/ou schémas inhabituels lors des appels	83	17
Échange de données d'itinérance (NRTRDE/CAMEL)	6	0			Échange de données d'itinérance (NRTRDE/CAMEL)	100	0
Définir et surveiller la limite d'utilisation des données	3	3			Définir et surveiller la limite d'utilisation des données	50	50
Empêcher l'échange de carte SIM pour les utilisateurs en itinérance sortante	1	5			Empêcher l'échange de carte SIM pour les utilisateurs en itinérance à l'étranger	17	83
Nombre moyen quotidien d'appels vers des numéros différents	3	3			Nombre moyen quotidien de numéros différents appelés	50	50
Nombre moyen d'appels sortants par jour	3	3			Nombre moyen d'appels sortants par jour	50	50
Nombre moyen d'appels entrants par jour	3	2			Nombre moyen d'appels entrants par jour	50	33

Le ratio MOC/MTC par IMSI	1	5			Le ratio MOC/MTC par IMSI	17	83
Durée moyenne des appels sortants par jour	3	3			Durée moyenne des appels sortants par jour	50	50
Durée moyenne des appels entrants par jour	4	2			Durée moyenne des appels entrants par jour	67	33
Surveiller le comportement des consommateurs afin de détecter les activités frauduleuses	5	1			Surveiller le comportement des consommateurs afin de détecter les activités frauduleuses	83	1
Les lignes RNIS doivent être verrouillées pour empêcher tout accès non autorisé	1	5			Les lignes RNIS doivent être verrouillées afin d'empêcher tout accès non autorisé.	17	83
Nombre moyen d'appels passés quotidiennement	2	4			Nombre moyen d'appels passés quotidiennement	3	67
Nombre moyen d'appels reçus quotidiennement	2	4			Nombre moyen d'appels reçus quotidiennement	33 %	67
Allocation convenue pour variation	1	5			Indemnité convenue pour variation	17	83

ANNEXE 3

Trois calendriers pour la mise en œuvre de la stratégie régionale de lutte contre la fraude

Le cadre de gestion de la fraude proposé doit être mis en œuvre selon le calendrier suivant afin de traiter tout problème de fraude et de sécurité qui serait identifié.

ACTIVITÉS PRINCIPALES	DÉTAILS DES ACTIONS À MENER	CALENDRIER	PARTIES PRENANTES	COMMENTAIRES
1. Mise en place de comités nationaux de lutte contre la fraude	Chaque pays doit mettre en place un comité national de lutte contre la fraude.	Janvier 2022	ANR	Terminé
2. Mise en place de comités régionaux de lutte contre la fraude	Chaque pays doit désigner deux (2) experts pour siéger au comité régional de lutte contre la fraude	Octobre 2021	GHANA	Terminé
3. Identifier les types de fraude potentiels	Le comité régional de lutte contre la fraude doit discuter et identifier les types de fraude potentiels.	Avril	Comité régional de lutte contre la fraude	Terminé
4. Évaluer les cadres juridiques existants	Chaque pays doit évaluer ses lois nationales afin de déterminer s'il existe des	30 juin 2022	ANR	Fait

	dispositions spécifiques permettant de poursuivre les fraudeurs dans le domaine des télécommunications et de les dénoncer.			
5. Élaboration de lignes directrices anti-fraude	Élaborer un principe régional de lutte contre la fraude	31 juillet 2022	Comité régional de lutte contre la fraude /	Terminé
6. Infrastructure de gestion de la fraude des États membres	Recueillir des informations sur l'état d'avancement des plateformes nationales existantes et leurs caractéristiques	31 juillet 2022	ANR / ORM	Partiellement terminé
7. Déploiement d'un ou plusieurs systèmes/outils sous-régionaux de lutte contre la fraude	Conception du système, mise en œuvre et configuration des règles.	À déterminer	GHANA+CEDEAO /ARTAO	À organiser
8. Élaborer des protocoles normalisés pour guider les États membres dans le traitement des numéros frauduleux détectés par les États membres.	Lignes directrices décrivant la manière dont les activités frauduleuses détectées doivent être traitées.	À déterminer	GHANA	Organiser
9. Élaborer et mettre en œuvre des exigences appropriées en matière de signalement des fraudes.	Un outil/portail central de signalement doit être mis en place pour permettre aux différents opérateurs de réseaux mobiles de la sous-région	À déterminer	GHANA	Organiser
10. Surveiller le système/mécanisme régional de lutte contre la fraude	Analyser les données relatives à toutes les activités frauduleuses signalées afin de déterminer celles qui ont cessé et celles qui persistent.	À déterminer	GHANA	Organiser

ANNEXE 4 - ACRONYMES

SMS A2P : SMS Application-to-Person

Anti-FKPI : Indicateur clé de performance anti-fraude

CLI Spoofing : usurpation d'identité de l'appelant

CEDEAO : Communauté économique des États de l'Afrique de l'Ouest

FMS: Système de gestion de la fraude

FUP : Politique d'utilisation équitable

GGSN : nœud de support GPRS passerelle

HPMN : Réseau mobile public domestique

Fraude IRSF/PRS : fraude internationale liée au partage des revenus / fraude liée aux services à taux majoré

MNO : opérateur de réseau mobile

MSISDN : Numéro d'abonné international de station mobile

NAFC : Comité national de lutte contre la fraude

ANR : Autorité nationale de régulation

NRTRDE : échange de données d'itinérance en temps quasi réel

RAFC : Comité régional de lutte contre la fraude

Matrice RACI : tableau de répartition des responsabilités qui définit les rôles et les responsabilités pour chaque tâche. Il signifie « responsable, redevable, consulté et informé ».

TAP : Procédure de transfert de compte

VLR : Registre de localisation des visiteurs

VPMN : réseau mobile public visité

ARTAO: Assemblée des régulateurs des télécommunications de l'Afrique de l'Ouest