MicroSave
Market-led solutions for financial services

La fraude dans les services financiers mobiles

Joseck Luminzu Mudiri

Une publication de *MicroSave Consulting* (*MSC*)

Sommaire

HISTORIQUE ET CONTEXTE

Pendant de nombreuses années, l'inclusion financière a fait partie des grands défis mondiaux en raison de son coût élevé. Pour offrir des services financiers, il fallait construire des locaux, recruter du personnel et consentir d'importants investissements en capital. Les établissements financiers se concentraient sur les consommateurs à forte valeur ajoutée qui généraient des revenus importants et ignoraient en grande partie le reste de la population.

L'arrivée des télécommunications mobiles, suivie de l'adoption de la téléphonie mobile pour offrir des services financiers, a modifié la dynamique du secteur en rapprochant les services financiers du grand public par le biais des infrastructures de commerce de détail des communautés locales. Le succès rencontré par M-PESA au Kenya depuis son lancement en 2007 a stimulé le développement des services financiers mobiles, notamment dans les pays en développement. Les établissements financiers traditionnels comme les banques ou les institutions de microfinance (IMF) investissent eux aussi dans la distribution de services financiers mobiles.

Comme pour tout autre service financier, la mise en place de services financiers mobiles ne va pas sans risques ni difficultés. Ce rapport s'intéresse à la fraude dans la distribution des services financiers mobiles.

Pourquoi étudier la fraude dans les services financiers mobiles ?

- L'étude de la fraude aide les prestataires de services financiers mobiles à anticiper le cycle de développement de la fraude, qui est étroitement lié au cycle de développement des services : on observe différents types de fraude aux différentes phases de développement des services.
- L'étude permettra aux parties prenantes de mieux comprendre la nature des interventions nécessaires pour lutter contre le risque de fraude.
- L'étude devrait contribuer à réduire le coût de ces interventions en permettant aux nouveaux opérateurs de bénéficier des enseignements provenant d'opérateurs plus anciens et plus expérimentés. Il convient de noter que les premiers opérateurs de services financiers mobiles ont bénéficié des enseignements du secteur des services financiers, des paiements et des télécommunications, ce qui leur a permis de mieux gérer les risques initiaux.
- Une meilleure connaissance de la fraude permet de mieux évaluer les investissements nécessaires pour y répondre. Ceux-ci comprennent les investissements en capital, le développement des plateformes, les ressources humaines et le renforcement des capacités. Ces coûts seront assumés par différentes parties prenantes, comprenant, entre autres, les régulateurs, les opérateurs, les agents et les agences de sécurité.

Définition de la fraude dans le contexte des services financiers mobiles

La fraude est généralement définie comme un acte malhonnête ayant pour but d'obtenir un avantage ou une tromperie commise délibérément pour en tirer un gain illégitime ou illégal. Dans le contexte de l'argent mobile, la fraude est une action délibérément commise par les acteurs des écosystèmes des services financiers mobiles dans le but d'en retirer un gain (pécuniaire ou en monnaie électronique) et/ou de priver d'autres acteurs de leurs revenus et/ou de porter atteinte à la réputation d'autres parties prenantes.

LES PRINCIPAUX CATALYSEURS DE LA FRAUDE

Les éléments suivants sont d'importants catalyseurs de la fraude dans les services financiers :

- ***Faiblesse de la réglementation*** : le manque de surveillance de l'écosystème de l'argent mobile par les régulateurs et leur incapacité à fixer des lignes directrices pour les différentes parties prenantes accroît le risque de fraude dans n'importe quel système. Il ne s'agit pas seulement de la réglementation obligatoire, mais également de la supervision exercée par les autorités financières. Dans un certain nombre de pays, la régulation des services financiers mobiles s'effectue par le biais de la supervision, les régulateurs appliquant de bonnes pratiques dans leur gestion des services.
- ***Niveau de maturité du service d 'argent mobile*** : différents types de fraude se manifestent aux différents stades de la vie des services. Par exemple, les fraudes liées aux transactions B2C et C2B se produiront probablement sur les marchés plus matures, tandis que les enregistrements factices sont courants au sein des services plus récents.
- ***Procédures*** : des procédures peu rigoureuses ou peu standardisées ouvrent la voie à différentes possibilités de fraude. La fraude peut être réduite et limitée par la mise en place de dispositifs de contrôle au sein des systèmes et des organisations.
- ***Surveillance de la conformité*** : les procédures ne peuvent à elles seules empêcher la fraude. Elles ne seront efficaces que si elles sont correctement surveillées et contrôlées. La surveillance de la conformité peut prendre la forme d'audits périodiques, de visites mystère, de contrôles et vérifications par des intervenants extérieurs, etc.
- ***Sensibilisation des consommateurs et communication au sein du système*** : la communication permet aux différents utilisateurs de savoir quelles sont les fraudes courantes et les meilleurs moyens de s'en protéger. L'absence de communication sur le sujet peut accroître le risque de fraude, car les victimes potentielles ne sont pas au courant des risques et des moyens de prévention.
- ***Coût élevé des opérations*** : lorsque les opérations sont coûteuses, les clients peuvent être tentés de réduire ce coût en trichant.
- ***Politiques tarifaires*** : la tarification et les commissions versées aux différents intervenants peuvent alimenter la fraude dans le système. Les barèmes en pourcentage n'ont pas la même incidence que les barèmes par paliers. Dans certains cas, l'opérateur peut choisir de facturer des services à un point donné, ce qui génère un risque d'abus là où ces services sont gratuits.
- ***Aspects culturels*** : la fraude peut être plus élevée sur certains marchés parce que la société y est, dans l'ensemble, plus indulgente à l'égard des fraudeurs. Ce laxisme peut s'expliquer par la faiblesse des structures juridiques ou du système politique.
- ***Saisonnalité*** : la fraude a tendance à augmenter à certaines périodes de l'année. Au moment des fêtes, elle augmente aussi en raison du plus grand nombre de promotions et parce que chacun s'efforce d'attirer des fonds.

La fraude dans les services financiers mobiles est similaire à celle observée dans d'autres services financiers, comme par exemple les services bancaires, les paiements par carte ou les guichets automatiques, Elle n'est pas propre aux services mobiles, ce qui veut dire que les enseignements provenant d'autres domaines peuvent s'appliquer aux services d'argent mobile. L'apparition de la fraude dépend du stade de développement des services financiers. Par conséquent, les manifestations de la fraude évolueront à mesure que les services financiers mobiles évoluent.

CYCLE DE VIE DES SERVICES FINANCIERS MOBILES

Un service performant évolue en trois phases :

1. Phase d'acquisition des clients

À ce stade, l'opérateur souhaite acquérir autant de clients que possible, avec des commissions plus élevées pour l'enregistrement des clients qui constituent la principale source de rémunération des agents. La proposition de valeur des agents n'a pas encore fait ses preuves et les agents consacrent beaucoup de temps à la formation des clients. Selon les marchés, cette phase peut aller jusqu'aux deux premières années d'existence du service. Sur la base de la rémunération des agents, elle couvre la période pendant laquelle les commissions provenant de l'enregistrement des clients représentent plus de 50 % du total des commissions versées aux agents.

2. Phase d'activation des clients

Pendant cette phase, les clients qui ont été recrutés sont maintenant encouragés à faire des opérations. Elle se caractérise par l'accent mis sur le positionnement de marché et le développement des volumes d'opérations. Les commissions sur opérations représentent une partie plus importante de la rémunération des agents, qui sont plus fidèles à la marque. L'opérateur peut réduire les commissions d'enregistrement car les agents commencent à gagner plus d'argent sur les opérations. Cette phase se produit généralement entre le sixième mois d'existence du service et son quatrième anniversaire.

3. Phase de développement de la valeur ajoutée

Le service est arrivé à maturité et les clients ont de nouvelles attentes. Ils veulent pouvoir payer leurs factures de services collectifs, faire des opérations impliquant des comptes bancaires, recevoir leur salaire, faire des paiements marchands, etc. À ce stade, le canal de l'agent reste important, mais il ne peut à lui seul gérer l'éventail et le volume des opérations nécessaires. Le service recrute par conséquent des entreprises clientes pour faire entrer de la monnaie électronique dans l'écosystème du service financier. Cette phase commence approximativement à partir de la troisième année d'existence du service.

Matrice du cycle de développement de la fraude

L'apparition et la fréquence de la fraude dépendent du stade de mise en œuvre du service. À mesure que le service se développe, la nature des fraudes évolue. Il convient de noter que cette évolution est influencée par les facteurs suivants :

a) Évolution de l'approche produit et ajout éventuel de nouveaux produits au mix produit. Certaines formes de fraude plus récentes n'apparaitront qu'avec l'introduction de nouveaux produits. Dans le cas contraire, il n'y aura pas ou peu d'évolution dans les types de fraude rencontrés ;

b) Mesure dans laquelle les organisations détectent, identifient et luttent contre les fraudes rencontrées aux premiers temps du service. Si l'organisation ne fait rien pour lutter contre les fraudes existantes, celles-ci perdureront jusqu'à ce que le système ou le service s'effondre sous le poids de la fraude.

Le tableau ci-dessous récapitule les types de fraude les plus courants et leur probabilité/fréquence aux différents stades du cycle de développement des services. Il forme le cadre de base de ce rapport.

1. FRAUDE LIÉE AUX CONSOMMATEURS[i1]	1. Phase d'acquisition des clients	2. Phase d'activation des clients	3. Phase de fidélisation des clients et d'ajout de valeur
A. Fraude des consommateurs à l'encontre des agents			
Fausse monnaie	Faible	Moyenne	Élevée
Accès non autorisé aux appareils des agents	Faible	Élevée	Moyenne
Fraude sur le canal Web des agents	Faible	Moyenne	Élevée
B. Fraude des consommateurs à l'encontre d'autres consommateurs			
Hameçonnage (*phishing*), usurpation d'identité via SMS (*spoofing*), faux SMS (différents types)	Faible	Élevée	Élevée
Extorsion	Faible	Moyenne	Élevée
Utilisation non autorisée d'un code confidentiel	Faible	Élevée	Moyenne
Fraude sur les bons de retrait	Faible	Élevée	Moyenne
Annulations d'opération non justifiée	Faible	Moyenne	Élevée
C. Fraude des consommateurs à l'encontre de partenaires commerciaux			
Usurpation d'identité d'une entreprise	Faible	Élevée	Élevée
Versements erronés conservés par les bénéficiaires	Faible	Moyenne	Élevée

[1]Cliquer sur le lien hypertexte pour consulter en annexe le détail de ces fraudes, des exemples et des suggestions de mesures de prévention.

2. FRAUDE LIÉE AUX AGENTS[2]	1. Phase d'acquisition des clients	2. Phase d'activation des clients	3. Phase de fidélisation des clients et d'ajout de valeur
A. Fraude des agents à l'encontre des consommateurs			
Accès non autorisé aux codes confidentiels des clients	Moyenne	Élevée	Faible
Utilisation non autorisé du code d'opération des clients	Élevée	Élevée	Faible
Facturation de commissions non autorisées aux clients	Élevée	Moyenne	Faible
Retraits fractionnés	Faible	Moyenne	Élevée
B. Fraude des agents à l'encontre des prestataires de services financiers mobiles			
Dépôts fractionnés	Faible	Élevée	Moyenne
Dépôts directs	Faible	Élevée	Élevée
Transfert parallèle d'argent sur le réseau	Élevée	Élevée	Élevée
Enregistrement de clients sous de faux renseignements	Élevée	Moyenne	Faible
Enregistrement de consommateurs non existants	Élevée	Élevée	Faible
Enregistrement de personnes en tant qu'entreprises	Faible	Moyenne	Élevée
Blanchiment de capitaux sur la plateforme de services financiers mobiles	Faible	Moyenne	Faible
C. Fraude du personnel des agents à l'encontre des agents			
Détournement de fonds	Faible	Élevée	Élevée
Sous-évaluation des encaisses	Faible	Élevée	Élevée
Fraude par imitation	Faible	Élevée	Élevée
Fraude instantanée sur les commissions	Faible	Élevée	Élevée
D. Fraude perpétrée par les master-agents			
Débits non autorisés sur les comptes des agents	Faible	Élevée	Élevée
Prélèvements non autorisés sur les commissions dues aux agents	Faible	Élevée	Faible
Vente illégale d'outils de traitement des opérations	Faible	Élevée	Élevée

[2] Cliquer sur le lien hypertexte pour consulter en annexe le détail de ces fraudes, des exemples et des suggestions de mesures de prévention.

3. FRAUDE LIÉE AUX PARTENAIRES COMMERCIAUX [3]	1. Phase d'acquisition des clients	2. Phase d'activation des clients	3. Phase de fidélisation des clients et d'ajout de valeur
A. Fraude perpétrée par les employés d'organisation B2C et C2B à l'encontre des entreprises			
Les employés et les fraudeurs associent de mauvais numéros de téléphone aux comptes bancaires	Faible	Faible	Élevée
Détournement des encaissements de clients	Faible	Moyenne	Élevée
Transferts illégaux à partir de comptes d'argent mobile d'entreprises	Faible	Élevée	Moyenne
B. Fraude perpétrée par les entreprises à l'encontre de l'opérateur d'argent mobile			
Fraude liée au règlement des frais	Faible	Faible	Élevée
Entente pour appliquer des tarifs plus bas	Faible	Faible	Élevée

4. FRAUDE LIÉE À L'ADMINISTRATION DU SYSTÈME[3]	1. Phase d'acquisition des clients	2. Phase d'activation des clients	3. Phase de fidélisation des clients et d'ajout de valeur
Utilisation malhonnête de mots de passe	Faible	Moyenne	Élevée
Création de faux utilisateurs/utilisateurs non existants	Faible	Élevée	Élevée
Utilisateurs dotés de droits multiples	Faible	Élevée	Élevée
Fraude liée aux canaux multi-accès (Web/téléphone)	Faible	Élevée	Élevée
Faiblesse des mots de passe/codes confidentiels	Élevée	Élevée	Élevée

[3] Cliquer sur le lien hypertexte pour consulter en annexe le détail de ces fraudes, des exemples et des suggestions de mesures de prévention.

5. FRAUDE LIÉE AUX PRESTATAIRES DE SERVICES FINANCIERS MOBILES (Cliquer sur le lien hypertexte pour consulter en annexe le détail de ces fraudes, des exemples et des suggestions de mesures de prévention)	1. Phase d'acquisition des clients	2. Phase d'activation des clients	3. Phase de fidélisation des clients et d'ajout de valeur
A. Fraude financière			
Détournement des recettes du prestataire d'argent mobile	Faible	Moyenne	Élevée
Émission d'argent mobile en faveur d'organisations en échange de fonds non compensés	Faible	Élevée	Élevée
Accès non autorisé à des comptes suspendus/inactifs	Faible	Élevée	Élevée
B. Fraude par les employés des points d'assistance et de soutien opérationnel			
Accès non autorisé aux historiques d'opérations des clients	Faible	Élevée	Élevée
Transferts illégaux au débit des comptes clients	Faible	Élevée	Élevée
Échanges non autorisés de cartes SIM	Faible	Élevée	Élevée
Accès non autorisé aux droits d'accès au système de collègues	Faible	Élevée	Élevée
C. Équipes commerciales au contact des clients			
Pots de vin	Faible	Élevée	Élevée
Fausses réclamations	Faible	Élevée	Élevée
Accès non autorisé aux données transactionnelles des agents	Faible	Élevée	Élevée
Complicité avec des employés pour détourner des fonds appartenant aux agents	Faible	Élevée	Élevée

LES TYPES DE FRAUDE RENCONTRÉS DANS LES SERVICES FINANCIERS MOBILES

1. FRAUDE LIÉE AUX CONSOMMATEURS

La fraude perpétrée par les consommateurs est la fraude initiée par des fraudeurs qui se font passer pour des clients. Ce type de fraude vise les agents, les autres consommateurs, les entreprises et les prestataires de services financiers mobiles. Il s'agit de la fraude la plus courante sur le marché, qui transcende toutes les phases de développement des services. On la rencontre plus fréquemment pendant la phase d'activation des opérations, lorsque les consommateurs ont davantage confiance dans le service, sans pour autant bien connaître tous les risques potentiels. La principale méthode de lutte contre ce type de fraude passe par des actions de sensibilisation des consommateurs, bien qu'il existe aussi de nombreux dispositifs de contrôle qui peuvent être mis en place dans les systèmes et les procédures pour lutter contre ces risques.[4]

Les formes de fraude les plus courantes dans cette catégorie comprennent :

- ***Fausse monnaie (faux billets) : les fraudeurs déposent de la fausse monnaie chez les agents en échange de monnaie électronique, qu'ils retirent immédiatement auprès d'autres agents, de guichets automatiques ou de terminaux de point de vente.***

Mavuno avait été récemment embauché par un agent pour travailler au service des clients de l'argent mobile. Le deuxième jour, un consommateur entre dans le magasin. Il prétend ne pas vraiment connaître le service mais souhaite s'enregistrer et déposer de l'argent. Mavuno, voyant la possibilité d'une commission d'enregistrement, prend le temps de lui expliquer le service. Un autre client entre dans le magasin pour déposer de l'argent. Mavuno vérifie que les billets ne sont pas des faux. Pendant ce temps, le client reçoit un appel et se met à discuter au téléphone. Il réalise soudain qu'il est en retard et demande qu'on lui rende son argent, puis s'excuse et sort du magasin. Le premier consommateur revient au guichet pour continuer sa conversation avec Mavuno. Tout d'un coup, le second client revient, prétend avoir changé d'avis et demande à Mavuno de déposer son argent aussi rapidement que possible. Mavuno s'exécute et confirme le montant avant d'encaisser les espèces. Ce n'est qu'après coup qu'il réalise qu'il a fait l'erreur de ne pas vérifier les billets une seconde fois et que ceux-ci sont des faux.

- ***Phishing : les fraudeurs envoient de faux SMS aux agents, que ce soit au moyen de leur propre téléphone ou en les générant automatiquement à partir d'un ordinateur. Les SMS ont l'air authentique aux yeux des destinataires.***

John avait besoin d'argent pour rembourser ses créanciers. Un jour, il reçoit un appel d'une personne très aimable qui déclare travailler pour une grande chaîne de supermarchés. Cette personne lui explique qu'il vient de gagner un prix de 1 200 US$ suite à un tirage au sort récemment organisé par l'entreprise. Il y a toutefois une condition pour décaisser les fonds : est-ce que John pourrait envoyer de l'argent (100 US$) sur le compte 12345 pour couvrir les frais ? John s'exécute et fait le virement. Lorsqu'il rappelle pour s'enquérir de son prix, la personne lui dit que le virement n'était pas suffisant et qu'il doit en faire un second du même montant. John emprunte l'argent à un ami en lui promettant de le rembourser avec un taux d'intérêt de 10 % par mois. Après le second virement, il essaie de rappeler la personne, mais le numéro ne répond pas. Il essaie pendant deux heures sans succès. Il décide alors d'appeler le centre d'appel de l'opérateur mobile. On lui explique alors qu'il n'y pas eu de promotion de cette nature et que plusieurs clients se sont plaints d'avoir été escroqués de la même manière.

[4] Voir également l'article de blog d'Ignacio Mas intitulé *My PIN is 4321* pour une présentation de ces enjeux.

- ***Les clients escroquent les agents après avoir noué de bonnes relations avec leur personnel, ou nouent des relations avec certains employés pour ensuite les tromper dans le but de voler de l'argent liquide ou de la monnaie électronique.***

Monique travaille chez Zua, un master-agent de grande taille. Abass est un client régulier. Il fait toutes ses opérations au magasin de Zua et lui laisse un pourboire à chaque fois. Ils ont d'excellentes relations. À un moment donné, il l'appelle et lui demande de déposer de l'argent sur son compte d'argent mobile parce qu'il ne peut pas passer au magasin. Il promet de lui apporter l'argent dans moins d'une heure. 45 minutes plus tard, il arrive et lui donne un pourboire. La semaine suivante, il lui demande la même chose et lui laisse de nouveau un pourboire. À la quatrième fois, il lui demande de déposer 1 500 US$, mais cette fois-ci, il disparaît et on n'entend plus jamais parler de lui.

2. FRAUDE LIÉE AUX AGENTS

La fraude liée aux agents est perpétrée au sein des réseaux d'agents. Elle est initiée et commise par les agents ou leurs employés. Elle comprend les fraudes commises par les employés à l'encontre des agents, celles commises par les master-agents à l'encontre des agents qui dépendent d'eux et celles commises par les agents à l'encontre des clients ou du prestataire de services financiers mobiles. La fraude liée aux agents est plus courante au début du cycle de développement des services, favorisée par les lacunes tarifaires du début. Elle évolue au fil du temps pour prendre différentes formes, toucher différentes victimes et avoir différents impacts dans le service.

Les principaux types de fraude liés aux agents sont les suivants :

- ***Fraude des employés à l'encontre des agents***

Jampu est un master-agent qui gère une vingtaine de points de vente. Bhavesh a été embauché par Jampu pour assurer les transferts de fonds entre les différents points de vente. Chaque matin, Bhavesh va d'un point de vente à l'autre pour ramasser les fonds en excès et en déposer aux magasins qui en manquent. Il a toujours rêvé de partir à l'étranger pour avoir de meilleures opportunités. Il se procure un passeport et un visa et achète un billet d'avion. Un jour, il collecte les fonds excédentaires des points de vente sans les redistribuer et part à l'aéroport pour quitter le pays. Lorsque le master-agent fait ses comptes, il se rend compte que Bhavesh s'est sauvé avec plus de 30 000 US$.

- ***Dépôts fractionnés***

Michael souhaite déposer 100 US$ sur son compte, ce qui rapporte 2 US$ à l'agent. Pour permettre à l'agent de recevoir davantage de commissions, il fractionne son opération en 10 remises de 10 US$, qui rapportent chacune 0,50 US$ à l'agent, soit 5 US$ au total. Sachant que les clients ne paient pas de frais sur leurs remises, cet arrangement n'a pas de conséquence pour eux.

Fraude des master-agents à l'encontre des agents

Oblong est un gestionnaire de réseau d'agents qui est autorisé à recruter de nouveaux agents. En théorie, la rémunération des agents est égale à 80 % du total des commissions. Dans la pratique, Oblong sous-estime de 20 % le montant total des commissions dues aux agents. Au lieu de leur verser 80 %, il leur verse 80 % de 80 %, ce qui est égal à 64 %. Les agents reçoivent par conséquent 16 % de commissions en moins. Ce type de fraude porte atteinte à la crédibilité du service d'argent mobile et dissuade les agents d'investir davantage dans cette activité.

3. FRAUDE LIÉE AUX PARTENAIRES COMMERCIAUX

La fraude liée aux partenaires commerciaux désigne les activités frauduleuses perpétrées à partir du réseau des partenaires commerciaux du service. Ceux-ci comprennent les organisations B2C (de l'anglais « *business to consumer* », qui font des versements en faveur des consommateurs), C2B (de l'anglais « *consumer to business* » : qui encaissent des paiements de consommateurs) et les détaillants. Les activités frauduleuses peuvent être perpétrées par des employés de ces partenaires commerciaux à l'encontre de l'organisation concernée ou des consommateurs ou par le partenaire commercial à l'encontre de l'opérateur d'argent mobile. Les fraudes liées aux partenaires commerciaux sont plus courantes pendant la phase de développement de la valeur ajoutée du service, principalement parce que c'est durant cette phase que les partenariats se développent. Ce type de fraude n'est pas encore très développé, car les transactions réalisées par des entreprises n'en sont qu'à leurs débuts.

Les formes de fraude les plus courantes dans cette catégorie sont les suivantes :

Fraude des employés à l'encontre des clients

Chakitu Bank a récemment commencé à offrir des services bancaires mobiles à ses clients. Ces services leur permettent de faire des opérations au moyen de leur téléphone portable. Les clients intéressés doivent d'abord s'abonner au service auprès des agences de Chakitu, qui associent leur numéro de portable à leur compte en banque.

Durant, un employé de la banque, connaît un certain nombre de clients qui font des opérations fréquentes et conservent des soldes importants sur leur compte, mais ne souhaitent pas utiliser les services bancaires mobiles. Il rattache frauduleusement ces comptes à son numéro de portable et fait des virements vers son numéro de portable. Lorsque les clients réalisent qu'ils ont été escroqués, des sommes substantielles ont déjà été débitées.

Fraude des employés à l'encontre de leur employeur

Nore Services est un établissement financier qui a intégré des services financiers mobiles aux comptes bancaires de ses clients, ce qui leur permet de transférer de l'argent vers leur compte d'argent mobile. Hatari travaille au service informatique de Nore et s'intéresse beaucoup à ces services. Beaucoup de collaborateurs de l'entreprise s'y intéressent très peu et Nore n'a pas mis en place de procédures ou de systèmes permettant de gérer les risques liés à cette intégration. En particulier, il n'y pas de rapprochement comptable régulier des opérations. Hatari a de multiples accès à l'interface qui fait le lien entre Nore et le service d'argent mobile. Il en profite pour transférer des fonds vers différents comptes d'argent mobile ouverts au fil du temps. Lorsque les auditeurs effectuent le rapprochement comptable deux semaines plus tard, ils découvrent un trou de plus de 100 000 US$.

4. FRAUDE LIÉE AUX PRESTATAIRES DE SERVICES FINANCIERS MOBILES

Cette catégorie couvre un large éventail d'activités frauduleuses commises par le personnel des prestataires de services financiers mobiles. Ces actes frauduleux seront perpétrés sans autorisation de l'entreprise. Les principaux types de fraude dans ce domaine concernent la fraude à l'encontre de l'opérateur d'argent et la fraude à l'encontre des agents, des entreprises et des consommateurs. Ce type de fraude est plus rare pendant la phase de mise en place des services et devient plus courant pendant les phases d'activation des clients et de développement de la valeur ajoutée. À ce stade, des montants substantiels de monnaie électronique ont été investis dans le système, qui devient par conséquent plus attrayant pour les fraudeurs.

Voici quelques exemples courants de ce type de fraude :

- ***Corruption au sein de l'activité d'argent mobile***

John est un enseignant qui cherche un moyen de compléter ses maigres ressources. Il entend dire que l'activité d'agent pour un important prestataire de services financiers mobiles est une activité lucrative. Il décide de postuler et soumet son dossier de candidature. Il reçoit un appel téléphonique qui lui indique que pour avoir le droit d'exploiter son point de vente, il doit verser une somme d'argent en tant que frais de dossier. S'il ne verse pas ce pot de vin, son point de vente ne sera pas autorisé.

- ***Détournement de fonds par les employés des opérateurs d'argent mobile***

Baku est un master-agent de grande taille qui exploite une trentaine de points de vente et traite des opérations pour les services financiers mobiles depuis plus de trois ans. Il est déclaré en faillite et le tribunal ordonne la liquidation judiciaire de l'entreprise. Le compte d'argent mobile de Baku est gelé dans l'attente de la fin de la procédure. L'accès au compte par les actionnaires d'origine de Baku est annulé et ils ne peuvent plus le consulter ou y faire des opérations.

La procédure de liquidation met cinq ans à se terminer, pendant lesquels le compte est en grande partie oublié. Un employé de l'opérateur d'argent mobile qui dispose de droits d'administrateur accède au compte et transfère les fonds qui s'y trouvent en sa faveur. À la fin de la procédure de liquidation, il ne reste plus d'argent sur le compte.

- ***Collusion entre les employés des opérateurs d'argent mobile et d'autres fraudeurs pour des échanges illégaux de cartes SIM.***

Jackie est assise dans son épicerie. Elle décide d'appeler son mari, qui travaille dans une autre ville. Elle essaie de lui téléphoner, mais n'arrive pas à se connecter. Encore un problème de réseau, marmonne-t-elle, et elle abandonne, convaincue qu'il s'agit d'une panne de réseau. Elle se remet au travail, mais sa voisine apparaît en lui tendant son téléphone : « c'est ton mari ! » lui dit-elle. Elle lui explique que son mari n'a pas réussi à la joindre pendant toute la matinée. Jackie réalise qu'il y a un problème avec sa ligne. Lorsqu'elle appelle le centre d'appel de l'opérateur avec le téléphone de son amie, on lui dit que sa ligne a été « permutée »… et elle se rend bientôt compte que son compte d'argent mobile a été vidé.

- ***Accès non autorisé aux renseignements financiers des clients pour en tirer un gain personnel.***

Paul et Michelle sont en train de divorcer. Paul soupçonne que Michelle a plus d'argent sur son compte d'argent mobile que ce qu'elle a déclaré. Il se met en quête d'un employé du service client qui accepte de lui fournir des renseignements. En échange d'un paiement, on lui communique le solde du compte.

- ***Transferts non autorisés au débit de comptes de clients***

John dépose de l'argent sur son compte et fait des opérations relativement fréquemment. Un jour, il consulte son solde et réalise que son dépôt de la veille n'apparaît pas. Il décide de vérifier au point de vente le plus proche de l'opérateur et constate que cet argent a disparu de son compte. Il demande un relevé et réalise qu'un retrait dont il n'a aucun souvenir a été effectué sur son compte.

Il dépose une réclamation auprès de l'opérateur d'argent mobile pour se plaindre que des fonds ont été débités de son compte sans son accord. L'opérateur fait une enquête et constate qu'un de ses employés a accédé au compte et transféré de l'argent vers son compte personnel. L'employé est incapable de fournir une explication pour son acte. Il est licencié.

5. FRAUDE LIÉE AUX SYSTÈMES

La fraude liée aux systèmes englobe toutes les activités frauduleuses qui exploitent les faiblesses et défaillances des systèmes et procédures du service d'argent mobile. Elle peut concerner l'ensemble des parties prenantes, et notamment les agents, les entreprises et les opérateurs d'argent mobile. Elle est plus fréquente lorsque les plateformes techniques n'ont pas de systèmes de contrôle adéquats pour surveiller le traitement des opérations. Elle se rencontre fréquemment pendant la phase d'activation des services et se développe pendant la phase de création de valeur supplémentaire.

Elle prend le plus souvent les formes suivantes :

Mots de passe/codes confidentiels communs

Chantal exploite un point de vente de l'argent mobile avec deux employés. Chacun d'entre eux est censé faire la demande d'un code confidentiel personnel (PIN) pour le traitement des opérations de l'argent mobile. Chantal les encourage néanmoins à utiliser le même code. Même lorsque ses employés quittent leur emploi, les remplaçants continuent d'utiliser le même code.
Un jour, Mark, un des employés, prend un jour de congé. Il s'arrête toutefois au magasin pour vérifier quelque chose et trouve le téléphone posé sur le guichet. Il en profite pour transférer de l'argent vers un numéro enregistré frauduleusement et retire cet argent à un distributeur automatique. Il est très difficile de prouver qu'il est coupable sachant qu'il n'était pas de service ce jour-là.

Faiblesse des mots de passe/codes confidentiels

Michi fait beaucoup d'opérations sur son compte mobile parce qu'il le trouve très pratique. Son fils Daudi est un joueur et a besoin d'argent pour satisfaire cette habitude. Il connaît l'année de naissance de son père, qui lui a demandé une fois de débloquer son téléphone en l'utilisant comme code confidentiel. Il finit par s'en servir pour se faire des virements en sa faveur qu'il retire ensuite en espèces.

Création de faux utilisateurs sur les plateformes de services financiers mobiles

John travaille pour un prestataire extérieur engagé par un établissement financier important. Il a reçu des droits d'administrateur pour participer à l'intégration entre la plateforme d'argent mobile et l'établissement financier. Il crée deux utilisateurs non autorisés qui ont le droit d'initier et de confirmer des opérations et transfère des fonds de l'organisation vers les portemonnaies mobiles de ses associés, détournant ainsi les fonds de l'établissement financier.

Utilisateurs dotés de droits multiples

Jim est le responsable des transferts d'argent chez un master-agent. Pour faire des économies, son employeur décide de ne pas recruter du personnel supplémentaire et met en place des autorisations uniquement pour lui et Jim sur son compte de gestion de l'argent mobile. Très occupé, il confie son mot de passe à Jim pour lui permettre d'initier et de contrôler les opérations sur le compte. Jim en profite pour transférer de l'argent sur les comptes de ses amis.

Fraude liée aux canaux multi-accès

À un moment donné, un master-agent important perd son ordinateur et effectue par conséquent des opérations sur un ordinateur situé dans un cybercafé. Il licencie par la suite deux de ses salariés, Navaro et Sadiki. Après avoir acheté un nouvel ordinateur, il oublie de désactiver le certificat sécurisé utilisé au cybercafé. Navaro et Sadiki, qui sont au courant, en profitent pour faire des opérations illégales à partir du cybercafé.

RÉPERCUSSIONS DE LA FRAUDE

La fraude n'est pas propre aux services financiers mobiles, elle se produit dans tous les services financiers. Sachant toutefois que les services financiers mobiles représentent l'un des principaux moyens d'élargir l'inclusion financière et de distribuer des services financiers destinés au grand public, la fraude dans ce domaine a des répercussions beaucoup plus importantes, qui affectent l'écosystème de l'argent mobile de différentes manières.

Crédibilité des services financiers mobile

En cas de fraude rampante et persistante, la crédibilité du service peut être dangereusement affaiblie. En cas de détournement de fonds dans le système ou de pots de vin exigés des agents pour accéder à des opportunités, le régulateur peut être amené à intervenir au titre de la protection des consommateurs. Les abonnés individuels peuvent être dissuadés d'utiliser le service de crainte de perdre leur argent suite à des fraudes. La crédibilité du service d'argent mobile d'un important opérateur de réseau mobile (ORM) d'Afrique de l'Est a ainsi été gravement entachée par des fraudes qui se sont produites au sein de l'entreprise.[56]

Impact sur l'image de marque

L'image de marque est capitale pour toute entreprise ou organisation. Elle représente les valeurs qui définissent la manière dont cette entreprise ou organisation est perçue par son environnement.

Si les produits de l'organisation sont touchés par de la fraude, les utilisateurs associeront la marque aux actes frauduleux, ce qui peut avoir des répercussions sur les autres produits ou services proposés par l'organisation.

Développement du nombre d'abonnés

Les abonnés souhaitent faire leurs opérations sur une plateforme de services financiers sécurisée, à laquelle ils peuvent se fier pour obtenir des services rapides et efficaces. Dans de nombreux pays, la peur de la fraude et la crainte de perdre de l'argent retarde l'adoption de l'argent mobile. De la même manière, l'adoption des cartes de crédit et de paiement a été négativement impactée par la crainte des fraudes. Par conséquent, si la fraude dans les services financiers mobiles n'est pas contenue, elle risque de freiner la croissance des opérations et de la clientèle.

Investissement des agents dans les services financiers mobiles

Les agents apportent des encours d'argent liquide et de monnaie électronique qui sont indispensables pour garantir la liquidité, et donc l'offre de services financiers mobiles. Un niveau élevé de fraude dans le système est susceptible de dissuader les agents d'investir dans leurs encours d'argent liquide et de monnaie électronique de peur de perdre leur capital. Les agents seront en outre peu disposés à engager des fonds si ceux-ci sont à risque d'être détournés par des fraudeurs et s'ils ne peuvent pas faire le rapprochement des commissions qu'ils gagnent avec ce qui est enregistré sur le système. Les opérateurs travaillent de plus en plus avec les agents pour lutter contre la fraude au sein de leurs points de vente, car cela affecte leur capacité à investir dans cette activité.

---

[5] Voir Mas & Ng'weno : *Why doesn't every Kenya business have a mobile money account?*

[6] Selon certaines indications, il semble toutefois que la confiance des clients n'a pas été trop ébranlée par les rapports de fraude interne (malgré l'importance de celle-ci) car les clients n'ont pas été touchés et l'ORM a été le seul à perdre de l'argent. Si beaucoup d'agents ou de clients avaient perdu de l'argent, les répercussions auraient probablement été beaucoup plus importantes.

Entreprises extérieures et autres prestataires

La troisième étape de l'évolution des paiements mobiles est l'introduction de services B2C (de l'anglais « *business to consumer* » : des entreprises vers les consommateurs) et C2B (de l'anglais « *consumer to business* » : des consommateurs vers les entreprises). Les entreprises concernées peuvent être des banques, des entreprises de services aux collectivités, des organisations qui versent des salaires, des supermarchés et toute autre organisation qui souhaite utiliser les paiements mobiles pour des versements ou des encaissements. En raison des volumes d'opérations et des sommes en jeu, elles éviteront les services qui ont un historique de fraudes entraînant la perte de fonds, ce qui peut entraver l'utilisation des services à une étape cruciale de leur développement.[7] Les discussions avec des opérateurs montrent que le processus de recrutement des banques en tant que clients C2B et B2C est onéreux, car elles ont l'obligation de garantir la sécurité des fonds de leurs clients.

Innovation et attitudes

L'innovation est un autre domaine dans lequel la fraude peut avoir des répercussions négatives. L'innovation comprend l'ouverture des plateformes à d'autre systèmes/réseaux pour élargir la gamme des services proposés. Les prestataires seront moins enclins à prendre des risques et à innover dans le domaine des paiements mobiles si l'écosystème dans son ensemble redoute les fraudes qui peuvent accompagner l'innovation. Pour promouvoir l'innovation, les organisations peuvent se trouver obligées d'essayer de limiter la fraude au sein des systèmes existants avant de pouvoir envisager d'introduire de nouveaux services.

Développement international

Le développement international des services financiers mobiles pourrait être entravé par l'idée que les paiements mobiles sont propices aux activités frauduleuses.

La perception est un aspect déterminant de l'adoption des services de paiement mobiles à l'échelon international. À mesure que les services deviennent populaires, il est donc important de limiter autant que possible la fraude. Les discussions avec un certain nombre de services potentiels montrent que la fraude est une préoccupation majeure, les opérateurs mentionnant les pertes importantes subies par un ORM d'Afrique de l'Est.

Coût de la fraude

La fraude et la gestion de fraude représentent une charge financière qui augmente le coût de traitement des opérations. Si les taux de fraude sont élevés, il peut être nécessaire d'augmenter les tarifs applicables aux clients pour générer des revenus suffisants qui permettent d'assurer la viabilité de toutes les parties prenantes. Lorsqu'une organisation perd de l'argent suite à des vols ou à des escroqueries par des tiers, elle est obligée d'augmenter ses tarifs pour rester rentable, ce qui peut rendre ses produits ou services inabordables pour une partie de la population. Si un agent perd de l'argent à cause d'actes frauduleux, il peut être amené à cesser son activité.

Blanchiment de capitaux

Dans certains cas, la fraude peut déboucher sur des activités de blanchiment de capitaux ou de financement du terrorisme. Ces activités peuvent prendre la forme de transactions liées au terrorisme suite à un manque de vigilance à l'égard des clients (KYC) au moment de l'enregistrement ou de l'introduction de fonds clandestins dans le système financier sous couvert de fausses identités. Bien que pour le moment, rien n'indique que cela se soit déjà produit, il est important que les prestataires de services financiers mobiles soient conscients de ces risques.

[7] Voir Mas & Ng'weno, *Why doesn't every Kenya business have a mobile money account?* pour une excellente présentation détaillée de ces aspects et d'autres questions connexes.

CONCLUSION

Il est évident que la fraude liée à l'argent mobile représente un souci croissant. Ces dernières années, plusieurs affaires graves ont été signalées, suscitant des inquiétudes au sein du secteur. À mesure que les paiements mobiles se développent dans de nombreux pays et que de nouveaux produits arrivent sur le marché, il est de plus en plus nécessaire de lutter efficacement contre la fraude. Les bailleurs de fonds et les consultants ont un rôle important à jouer dans ce domaine.

- **Recherche** : il existe très peu d'études sur la fraude dans les services financiers mobiles, notamment parce que ces services restent relativement nouveaux à l'échelon mondial avec un nombre limité d'entreprises performantes. Ces études impliqueraient de travailler en étroite collaboration avec ces entreprises pour mieux comprendre les risques de fraude. Dans la plupart des cas, ces entreprises seront très attentives au type d'organisation avec lequel travailler pour protéger leurs informations sensibles. Elles seront donc plus enclines à travailler avec des organisations extérieures réputées qui ne risquent pas de compromettre leurs informations. Les bailleurs de fonds et les consultants ont un rôle important à jouer pour identifier des intervenants extérieurs neutres capables de réaliser ces études, qui seront bénéfiques pour le secteur à long terme. Ces recherches permettront au marché de mieux cerner les causes profondes de la fraude, ses taux d'apparition, ses schémas les plus courants, les parties responsables et l'efficacité des différentes mesures de prévention mises en place.

- **Actions communes** : s'agissant d'un sujet hautement sensible, qui est susceptible de porter atteinte à leur image de marque et à leur niveau d'activité, beaucoup d'opérateurs préfèrent gérer les problèmes de fraude en interne, sans consulter d'autres intervenants. Il y a donc peu d'information qui circule entre les acteurs du secteur sur les expériences de fraude, et donc peu de transfert de connaissances. Un fraudeur qui a escroqué une organisation peut facilement passer à la suivante en sachant pertinemment que l'information a peu de chances de circuler entre les différents acteurs de l'argent mobile. Les bailleurs de fonds et les consultants pourraient remédier à cette situation en jouant le rôle de partie neutre pour l'organisation de sessions d'information, en y associant d'autres parties prenantes, comme par exemple les régulateurs, les organismes chargés de faire appliquer la loi, le monde universitaire, etc.

- **Développement d'outils et de processus intelligents** : il est indispensable de se doter d'outils et de processus intelligents pour lutter contre la fraude. La plupart des cas de fraude, et notamment ceux de grande taille/ampleur, peuvent être détectés et limités par des analyses de données appropriées. Beaucoup de services ne se sont pas encore dotés d'outils efficaces et fiables pour analyser leurs données en temps réel. Pour remédier à cette faiblesse, beaucoup d'entre eux risquent d'être obligés de mettre en place de nouvelles plateformes plus robustes ou de créer des interfaces capables de produire des données adaptées. Beaucoup de prestataires de services financiers mobiles ne comprennent pas l'importance de ces analyses ou n'ont pas les capitaux nécessaires pour investir dans cette activité. Ils sont complètement focalisés sur le développement de leur activité ou la mise au point de nouveaux produits pour leurs clients. Les bailleurs de fonds et les consultants peuvent combler cette lacune en investissant dans le développement d'outils et de processus intelligents pour le compte des prestataires. Ils peuvent collaborer avec des spécialistes de l'automatisation des services aux entreprises et identifier des ressources susceptibles de contribuer à l'analyse des données. Ils peuvent également concevoir, tester et mettre en œuvre des boîtes à outils.

Renforcement des capacités : beaucoup de services d'argent mobile ne possèdent pas les compétences requises pour comprendre la fraude dans leur entreprise et/ou dans le secteur en général. Le nombre de spécialistes est limité et son augmentation n'est pas encore en phase avec la demande des services. Des métiers dont le champ d'application était précédemment jugé limité sont en train de prendre une importance croissante. Des analystes commerciaux, des responsables de la lutte contre la fraude et le blanchiment de capitaux et des responsables de la conformité deviennent nécessaires. Mais le renforcement de ces capacités sort du métier de base des prestataires de services financiers mobiles. Même s'ils renforcent leurs compétences dans ce domaine, on observe une tendance à placer des spécialistes à l'intérieur des entreprises. Il n'existe pas de mécanisme permettant de surveiller les fraudes au niveau sectoriel et de renforcer la confiance de la population à l'égard de l'écosystème de l'argent mobile. Les bailleurs de fonds pourraient remédier à cette situation en apportant des financements pour développer des compétences dans ce domaine et créer des programmes et plateformes de formation consacrés à la lutte contre la fraude pour former les différentes parties prenantes de l'écosystème. Ce travail devra se poursuivre dans le temps pour permettre à tout un ensemble de spécialistes de développer une expertise dans ce domaine.

- **Education financière** : les agents comme les consommateurs ont besoin d'une meilleure éducation financière pour lutter contre le risque de fraude dans les services financiers mobiles. La réalisation d'opérations financières au moyen de la téléphonie mobile est un phénomène encore très récent. Même les classes moyennes et aisées, qui sont mieux formées et ont plus l'habitude de la technologie et de son utilisation, n'utilisent pas encore toutes les possibilités de ces services. La population à faible revenu, et plus particulièrement les personnes peu ou non bancarisées, ont besoin d'être formées à l'usage de ces services, à leurs avantages et à leurs risques, entre autres aspects, pour pouvoir s'en servir avec confiance. De la même manière, les agents ne seront pas en mesure de servir correctement les consommateurs s'ils ne connaissent pas les risques et les précautions à prendre en tant que prestataires de service. Cette éducation financière n'a pas besoin d'être formelle, mais elle implique de recourir à des outils de communication et de marketing pour sensibiliser les personnes concernées. Il existe un certain nombre d'aspects à prendre en compte :
  - Formation et certification des agents : il est largement admis que les agents forment la colonne vertébrale des services financiers mobiles. Une formation approfondie des agents constitue la première ligne de défense contre la fraude. Les prestataires de services financiers mobiles doivent donc avoir un programme complet de formation initiale et continue de leurs agents, comprenant une certification et des évaluations. Des agents bien formés seront conscients des risques et des mesures à prendre pour lutter contre la fraude et minimiser son impact.
  - Organisation de réunions de discussion avec les clients et/ou les agents : ces événements permettent de mieux faire connaître les services financiers mobiles et de recueillir les commentaires et suggestions des utilisateurs et des acteurs du secteur.
  - Organisation de « road shows » centrés sur des interactions expérientielles entre les prestataires de services financiers mobiles et les clients/agents. Ces sessions sont largement utilisées dans le secteur des biens de consommation courante pour mieux faire connaître les produits et services et répondre aux objections des consommateurs. Compte tenu des similarités qui existent entre ce secteur et celui des services financiers mobiles, ces « road shows » pourraient aider les prestataires à avoir un meilleur dialogue avec leurs clients.
  - Sensibilisation des consommateurs : des campagnes d'information dans la presse et les médias électroniques permettraient de sensibiliser le grand public à certains risques et à certaines formes de fraude.

- **Surveillance et supervision des agents** : le développement réussi des services financiers mobiles passe par l'identification, la mise en place et la gestion de réseaux de distribution. Il s'agit d'un processus coûteux, qui exige du personnel, des structures, des procédures et des activités de suivi pour garantir que ces réseaux et leurs agents apportent un service standardisé aux clients. Aussi robustes qu'ils soient, les systèmes et les processus ne sont efficaces que s'ils sont correctement mis en œuvre. Une surveillance régulière des agents est donc importante pour surveiller cet aspect. Les cas de laxisme délibéré ou de négligence des agents doivent donner lieu à des avertissements. En revanche, si les agents font des erreurs mais sont prêts à apprendre, ils peuvent être guidés tout au long du parcours.

Des audits doivent être réalisés périodiquement pour contrôler les registres et les pratiques des agents et reconnaître leur performance ou (le cas échéant) prendre des sanctions. Les prestataires de services financiers mobiles ont besoin des ressources et du soutien apportés par les bailleurs de fonds et les consultants pour mettre en place ces activités. Ils peuvent avoir besoin de recourir à des consultants pour les aider à renforcer leurs compétences internes au sein de l'organisation.

- **Visites mystère et autres mesures de surveillance de la conformité** : une manière de surveiller l'activité des agents et leur respect des procédures consiste à réaliser des visites mystère. Le contrôle et la supervision sont des méthodes formelles de gestion de la performance des agents et de leur respect des procédures en place pour lutter contre la fraude, mais compte tenu de leur caractère habituel, les agents reconnaissent souvent le personnel chargé des visites de contrôle/supervision. Les visites mystère effectuées par des personnes non connues des agents peuvent fournir des informations précieuses sur l'expérience réelle des consommateurs. Pour être fructueuses, ces visites doivent respecter les règles suivantes :

  - Elles doivent être planifiées dans le cadre de la stratégie de gestion des réseaux de distribution des prestataires de services financiers mobiles. Elles doivent avoir des objectifs précis avec des outils de suivi bien définis, pour garantir qu'elles ne seront pas épisodiques mais soigneusement organisées par l'équipe. Cette activité se déroule généralement de façon continue à différents niveaux couvrant tout le pays.

  - Les visites mystère doivent être effectuées à différents niveaux, y compris celui des régulateurs qui recueillent des informations pour leurs propres besoins. Les régulateurs auront une approche plus stratégique, recherchant une « impression générale » des services financiers mobiles pour mieux comprendre cette activité.

  - Les visites peuvent aussi être effectuées par des équipes d'encadrement internes ou des intervenants extérieurs engagés pour réaliser des évaluations indépendantes.

  - Les parties prenantes doivent être informées de l'existence de ces visites mystère en tant qu'outil de contrôle de la qualité. Cela permettra de s'assurer que les agents feront de leur mieux pour se conformer à leurs obligations, demanderont à être formés si nécessaires et feront part de leurs commentaires sur les outils utilisés pour évaluer la qualité de leur travail.

  - Les récompenses et les sanctions liées au respect des procédures doivent être définies et communiquées aux agents à l'avance. Ils seront ainsi au courant des conséquences, ce qui permettra d'éviter toute confusion ou crainte de victimisation.

- **Évaluations de la protection des clients** : les mesures de protection de client ont pour but de protéger les consommateurs et autres utilisateurs des services financiers, et donc le secteur en tant que tel, des pratiques déloyales. Une évaluation formelle de la capacité des organisations à optimiser la protection des clients, et donc à réduire son risque opérationnel, de fraude et de réputation, peut être réalisée dans le cadre d'une série d'entretiens avec des agents, des consommateurs, des employés et des cadres de l'entreprise (avec le soutien d'outils PRA).[8] Les bailleurs de fonds devraient encourager ces évaluations de la protection des client pour protéger le secteur naissant des services bancaires mobiles/en ligne des chocs récemment observés dans celui de la microfinance.

Les mesures de protection des clients comprennent les actions suivantes :

[8] *MSC* a adapté les sept principes de protection des clients définis par Smart Campaign pour les services financiers mobiles : (1) offre de produit et mode de distribution adaptés, (2) sécurité et fiabilité, (3) transparence des produits et des services, (4) tarification responsable, (5) traitement équitable et respectueux des clients, (6) mécanisme de traitement des réclamations et (7) protection et respect de la confidentialité des données clients.

- Mise en place de procédures efficaces au sein de l'entreprise pour offrir des garanties suffisantes aux utilisateurs des services financiers mobiles de l'organisation. Les procédures et processus mis en place par les prestataires ne doivent pas sacrifier la protection des clients à des considérations de maximisation des revenus ou de réduction des coûts de l'entreprise. Les entreprises s'efforcent souvent de maximiser leurs revenus en se concentrant sur les profits à court terme, ce qui peut avoir des conséquences négatives pour la protection des clients. Un bon exemple de cette approche consiste à s'assurer que l'entreprise dispose de procédures formelles de collecte et de surveillance des informations clients. Cette démarche est coûteuse, mais elle permet à l'entreprise de disposer en permanence d'informations fiables sur les utilisateurs de sa plateforme d'argent mobile. Lorsqu'elles sont correctement mises en œuvre, les mesures de protection des clients contribuent à assurer la viabilité à long terme des services.

- Participation aux groupes de pression du secteur, et notamment aux associations de prestataires de services d'argent mobile, pour définir des normes de protection des consommateurs. Les normes définies par les associations professionnelles permettent de s'assurer que les prestataires lancent tous des produits respectueux des consommateurs et prennent des mesures qui protègent la crédibilité des services du secteur.

Ces associations peuvent même travailler à une harmonisation des normes entre les différents réseaux et organiser des évaluations par les pairs pour vérifier le respect des normes fixées collectivement. Ces associations peuvent faire pression sur les gouvernements pour la mise en œuvre de certaines mesures de politique publique, comme par exemple des campagnes d'information sur la contrefaçon pour réduire la fraude.

- Les régulateurs jouent un rôle déterminant dans la protection des clients en définissant les politiques d'orientation du secteur, en fixant les normes applicables aux prestataires de services financiers mobiles et en assurant la surveillance régulière du secteur. Les régulateurs des services financiers mobiles comprennent, entre autres, les autorités réglementaires chargées des services financiers, des télécommunications et de la concurrence. Ces autorités doivent disposer des compétences et des outils nécessaires pour promulguer et faire appliquer des politiques qui améliorent réellement la protection des clients. Dans le cas contraire, elles risquent de mettre en place des politiques insuffisantes qui auront un impact négatif sur la protection des clients.

ANNEXES

ANNEXE 1 : FRAUDE LIÉE AUX CONSOMMATEURS

La fraude liée aux consommateurs est la fraude commise par des personnes qui se font passer pour des clients. Il s'agit du type de fraude le plus courant, qui vise de nombreuses parties prenantes : agents, autres consommateurs, entreprises et opérateurs d'argent mobile.

a) Fraude de consommateurs à l'encontre des agents

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
• **Fausse monnaie** : les fraudeurs mélangent de faux billets avec de vrais billets. Ils déposent cet argent sur leur compte d'argent mobile auprès d'un agent, puis le retirent ensuite auprès d'autres agents. La fréquence de ce type de fraude est plus élevée lorsque le service se trouve en phase d'activation des clients, et aussi lorsqu'un nouveau point de vente vient d'ouvrir et que le personnel n'a qu'une expérience limitée de la vérification des billets de banque.	Les agents de l'un des principaux services d'argent mobile d'Afrique de l'Est mentionnent le cas de fraudeurs qui jouent le rôle de deux clients pour faire distraction : • Le principal fraudeur prétend vouloir déposer de l'argent auprès d'un point de vente pour obtenir de la monnaie électronique. Une fois que ses billets ont été vérifiés, il fait semblant de changer d'avis et demande qu'on lui rende ses espèces. • Son complice engage une discussion polie avec l'employé de l'agent. Le fraudeur décide alors de terminer son opération de dépôt. • Distrait, l'employé de l'agent ne pense pas à vérifier de nouveau les billets, qui s'avèrent des faux.	• Les régulateurs devraient travailler avec les opérateurs pour sensibiliser les différents prestataires des réseaux de distribution (agents) aux caractéristiques de sécurité des billets de banque officiels. • Campagnes d'information des consommateurs sur les caractéristiques des billets de banque officiels, comprenant des supports destinés aux points de vente, comme par exemple des affiches. • Les agents devraient être encouragés à investir dans des outils de détection des faux billets, comme par exemple des appareils UV ou des compteuses de billets. • Mise en place de lignes d'appel ou de points de contact pour signaler l'apparition de faux billets. • Visites mystère par les opérateurs pour vérifier le respect des procédures de dépôt et de retrait d'espèces. Les principaux points à surveiller sont les suivants : o Les espèces reçues des consommateurs doivent être contrôlées, authentifiées et validées ; o Avant de s'en aller, les clients doivent confirmer que les espèces reçues des agents ne sont pas douteuses, de façon à éviter des réclamations ultérieures concernant leur authenticité.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
• **Accès non autorisé aux appareils des agents** : les fraudeurs accèdent aux équipements utilisés par les agents (téléphone/ TPV) et enregistrent leur numéro comme étant celui du prestataire d'argent mobile ou du propriétaire du point de vente. • Dans le premier cas, ils envoient de faux SMS de retrait à des agents, qui traitent l'opération en pensant qu'elle est légitime. • Dans le second cas, ils se servent du numéro pour se faire envoyer de l'argent en dupant l'agent. • Fraude dans les circuits de distribution qui permettent aux agents de traiter des opérations à la fois par téléphone et en ligne.	Les cas signalés correspondent à des situations dans lesquelles les fraudeurs (souvent connus du personnel) ont pu accéder aux appareils de traitement des opérations. Certains agents ont observé des cas de collusion entre fraudeurs et employés, notamment lorsque les appareils sont utilisés par plusieurs personnes au sein du point de vente. Ce type de fraude est mentionné par de nombreux opérateurs de services financiers mobiles de toute l'Afrique. Les agents signalent des cas dans lesquels le propriétaire du point de vente demande qu'on lui envoie de l'argent. L'employé effectue alors le virement vers un numéro de téléphone préenregistré, sans le vérifier, et le numéro s'avère erroné. Un leader du marché a rencontré ce type de fraude en Afrique centrale. Des employés qui avaient eu accès au mot de passe et au code confidentiel du point de vente arrivent à transférer de l'argent en ligne en débitant le compte d'argent mobile de l'agent.	• Les agents du réseau de distribution doivent limiter l'accès aux appareils de traitement des opérations. Ces appareils doivent être conservés sous clé et protégés par un code lorsqu'ils ne sont pas utilisés. • Les opérateurs d'argent mobile doivent empêcher les cartes SIM qui servent aux opérations de recevoir des SMS autres que ceux du prestataire d'argent mobile. Cela passe par l'installation de filtres de blocage des transactions générées par ordinateur. • Les appels à destination des appareils de traitement des opérations doivent être limités à quelques numéros préenregistrés par l'opérateur d'argent mobile. Ces numéros préenregistrés sont uniquement communiqués aux prestataires du réseau de distribution. • Réunions d'information avec les prestataires du réseau de distribution pour parler de la fraude et de ses manifestations. • Limiter les opérations en ligne à des terminaux sécurisés dotés de certificats de sécurité. • Pour permettre les transactions en ligne, utiliser un système de mot de passe qui exige une autorisation via le téléphone ou le terminal du point de vente. • Les opérations effectuées en ligne devraient générer une notification envoyée sur le téléphone de l'agent pour confirmation. • Les employés des agents ne devraient pas partager leurs mots de passe ou utiliser des mots de passe qui sont faciles à deviner. • Les mots de passe des employés devraient être désactivés lorsqu'ils quittent leur emploi. • Processus précis d'autorisation avec documentation écrite pour tout changement dans le compte des agents ou tout échange de carte SIM.

b) Fraude à l'encontre des consommateurs

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
• **Hameçonnage (*phishing*), usurpation d'identité via SMS (*spoofing*), faux SMS (divers) :** • Les fraudeurs envoient des SMS aux consommateurs pour annoncer une fausse promotion pour laquelle ils doivent envoyer de l'argent sur des numéros de compte d'argent mobile frauduleux. • Les fraudeurs appellent un consommateur en se faisant passer pour un agent d'un centre d'appel. La victime est conduite à exécuter différentes actions qui l'amènent à transférer de l'argent de son compte vers celui du fraudeur. • **Extorsion** : les fraudeurs extorquent de l'argent à leurs victimes (consommateurs ou agents) sous des menaces de mort ou de kidnapping. • **Fausse erreur d'opération** : les fraudeurs font un virement prétendument erroné en faveur d'un consommateur. Ils appellent ensuite le bénéficiaire pour dire qu'ils se sont trompés et demander qu'on leur renvoie l'argent. Si le consommateur se laisse faire, il finit par transférer son propre argent en faveur du fraudeur.	La majorité des services d'Asie et d'Afrique ont été confrontés à ce type de fraude. Le *phishing* part du principe que parmi le grand nombre d'abonnés visés, certains enverront de l'argent aux fraudeurs. Ce type de fraude se produit le plus souvent lorsqu'il y a une panne technique du système qui affecte les opérations des clients. Il a été signalé dans de nombreux services d'argent mobile en Afrique. Ce type de fraude a été signalé dans les services matures d'Afrique de l'Est. Le fraudeur commence généralement par rassembler autant d'informations que possible sur sa victime pour donner l'impression qu'il la connaît personnellement. Cette forme de *phishing* a été signalée sur plusieurs marchés matures d'Afrique de l'Est. Les fraudeurs envoient une série de faux SMS suivis d'appels téléphoniques. Certaines des victimes ciblées finissent par transférer de l'argent aux fraudeurs.	• Le prestataire de services financiers mobiles devrait limiter la quantité d'information figurant sur les rapports d'opération des points de vente. Cette information peut en effet être utilisée à mauvais escient par les fraudeurs qui y ont accès. • Les consommateurs doivent déclarer toutes les menaces et cas de fraude aux forces de l'ordre. • Pour les opérations réalisées pour des clients, il est préférable que ces opérations soient limitées à un téléphone portable ou terminal de point de vente et non en ligne. • Développer un processus d'autorisation des échanges de cartes SIM et limiter le nombre de personnes autorisées à faire de tels échanges. • Campagnes d'informations à destination des agents et des consommateurs sur : – les différents types de fraude – leurs manifestations – les personnes à risque – les mesures de prévention • Mettre en place des procédures et directives précises pour la détection, la déclaration et la gestion de la fraude, comprenant des outils de déclaration périodique selon une fréquence à préciser. • Définir et mettre en place des directives destinées aux agents et distributeurs sur la distance entre les consommateurs et le respect de la vie privée, et configurer les équipements pour empêcher l'accès non autorisé aux opérations des clients.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Accès non autorisé aux codes confidentiels (PIN) : les fraudeurs amènent les clients à communiquer leur code confidentiel. Ils s'en servent ensuite leur voler de l'argent en mettant la main sur leur téléphone portable.	Les principaux opérateurs ont mené d'importantes campagnes d'information au Kenya, au Rwanda et en Tanzanie pour convaincre les clients de ne pas divulguer leurs codes confidentiels. Les victimes sont souvent illettrées et liées aux fraudeurs.	
Fraude aux bons de retrait : les bons de retrait et codes d'opération servent à réaliser des transferts en faveur d'utilisateurs non enregistrés, des retraits à des guichets automatiques ou des paiements en ligne ou en magasin. Les bons de retrait sont aussi utilisés pour des services de paiement traditionnels, comme Western Union ou Moneygram.	Ce type de fraude a été signalé par les opérateurs dans les premiers temps des services. Les consommateurs se volent les bons de retrait entre eux et s'en servent pour retirer de l'argent.	• Mettre en place des procédures précises d'émission des bons de retrait qui prévoient une date d'expiration et une notification de celle-ci. • Les bons de retrait ne doivent pas être accessibles à d'autres personnes que le bénéficiaire et en cas de perte, celui-ci doit pouvoir notifier l'entreprise et obtenir un bon de remplacement. • Dans le cas des clients non enregistrés, il est préférable de leur demander de s'enregistrer avant de pouvoir accéder aux fonds.
Annulations non justifiées : après avoir reçu des services et payé pour ceux-ci, les fraudeurs contactent l'opérateur mobile et demandent l'annulation de l'opération pour se faire rembourser.	Cette forme de fraude a été signalée en Afrique de l'Est.[9] Dans leur rapport, Mas & N'gweno y font référence en indiquant qu'il s'agit de la principale raison pour laquelle les entreprises n'utilisent pas M-PESA.	Une procédure précise de gestion des demandes d'annulation d'opérations qui garantit que les intérêts de toutes les parties prenantes sont pris en compte. Ce sujet est évoqué plus en détail dans le tableau de la page suivante.

[9]Voir Mas and Ng'weno : *Why doesn't every Kenya business have a mobile money account?*

Annulation d'opérations

Dans les services financiers mobiles, l'annulation d'opérations effectuées entre des parties (personnes physiques et/ou morales) est un sujet controversé, car elle peut conduire à des fraudes intentionnelles.

L'annulation d'opérations peut concerner les parties suivantes :

- Agent qui dépose de l'argent sur un mauvais compte
- Client qui retire de l'argent auprès d'un agent en utilisant un mauvais numéro d'agent
- Client qui envoie de l'argent à un mauvais numéro
- Client qui envoie de l'argent à une mauvaise entreprise (C2B)
- Entreprise qui envoie de l'argent à un mauvais client (B2C)

Annulation de transferts C2B ou de virements en faveur d'agents

L'annulation de ces opérations est le cas de figure le plus simple, parce que les prestataires de services financiers mobiles disposent de contrats signés avec les entreprises et les agents concernés, qui ont fait l'objet de vérifications préalables approfondies.

- En règle générale, lorsqu'un virement en faveur d'un agent doit être annulé, l'opérateur mobile appelle l'agent concerné pour vérifier qu'il s'agit bien d'un virement erroné. Il est extrêmement rare que l'agent refuse le débit dans le cas d'un virement effectué par erreur.
- Dans le cas de fonds envoyés par erreur à une entreprise, l'émetteur peut contacter directement l'entreprise, ou informer le prestataire d'argent mobile qui notifie l'entreprise. Là encore, il est hautement improbable que l'entreprise refuse le débit si les fonds lui ont été adressés par erreur.

Annulation d'opérations B2C

Si les fonds proviennent d'un agent ou d'une entreprise cliente, ils peuvent être bloqués en urgence par l'opérateur et reversés immédiatement à l'émetteur dès qu'il en est avisé. Les clients concernés peuvent alors être informés de l'annulation de l'opération.

Annulation d'opérations entre particuliers (P2P)

Ce cas de figure concerne les opérations effectuées entre abonnés individuels. Il représente la majeure partie des annulations d'opérations, mais aussi celles qui sont les plus controversées.

Il existe un certain nombre de scénarios pour procéder à ces annulations.

Scénario 1 : pas d'annulation

L'opérateur choisit de ne pas interférer avec les opérations des clients, qui sont invités à se mettre en rapport avec le bénéficiaire de l'opération pour résoudre directement le problème entre eux ou de procéder par voie judiciaire.

Avantages

- Les ressources de l'opérateur ne sont pas mobilisées pour traiter les demandes d'annulation.
- Ce scénario réduit le risque de fraudes dans lesquelles les clients obtiennent des services pour ensuite chercher à escroquer la personne qui les fournit en demandant l'annulation du paiement en leur faveur.

Inconvénients

- La majorité des demandes d'annulation d'opérations sont légitimes et les clients concernés risquent de perdre leur agent.
- Les clients dépendront de la bonne volonté des destinataires pour obtenir un remboursement.
- Les destinataires feront souvent payer au client le coût du transfert pour leur rembourser l'argent, alors que les annulations d'opération sont généralement gratuites.
- Les clients risquent de perdre confiance dans le service, surtout s'ils ont une mauvaise expérience et perdent de l'argent.

La plupart des services ont choisi de ne pas adopter cette approche, car elle donne une image impersonnelle de l'opérateur.

Scénario 2 : Annulation immédiate des opérations par le centre d'appel

Le centre d'appel a le pouvoir d'annuler les opérations sur la seule foi de la demande de l'émetteur, sans consulter le bénéficiaire.

Avantages

- L'annulation de l'opération est immédiate et se traduit par conséquent par des opérations supplémentaires sur la plateforme.
- L'annulation est moins coûteuse, car elle ne nécessite pas de contacts supplémentaires avec des tiers, qui consomment du temps et des ressources.
- Les fonds de l'émetteur sont protégés avant de pouvoir être détournés. Il y a eu des cas dans lesquels des consommateurs ont reçu des virements par erreur et ont immédiatement retiré l'argent.

Inconvénients

- Il y a un risque élevé d'annulations frauduleuses.
- Cette approche peut susciter de la méfiance à l'égard du système si n'importe quel client peut demander l'annulation d'opérations et obtenir un remboursement.
- Cette option prive le bénéficiaire de la possibilité d'expliquer sa situation/son point de vue.

Scénario 3 : Blocage des fonds avant annulation de l'opération

Dans ce scénario, le client appelle le centre d'appel et demande l'annulation d'une opération. Le centre d'appel bloque immédiatement la somme concernée pour qu'elle ne puisse pas être retirée, puis contacte le bénéficiaire. Si celui-ci soutient que le transfert est légitime, le centre d'appel débloque l'argent en sa faveur. Mais si le bénéficiaire reconnaît que l'argent appartient à l'émetteur, les fonds sont reversés à celui-ci.

Avantages

- Processus inclusif, qui permet aux deux parties concernées de faire valoir leur point de vue. Si le destinataire des fonds a fourni des produits ou des services à l'émetteur, cela sera mentionné dans l'appel.
- Même lorsque les fonds ne sont pas reversés, l'émetteur aura le sentiment que l'opérateur a fait tout ce qui était en son pouvoir pour les récupérer. Des messages générés par le système à l'attention de l'émetteur peuvent être utiles. L'image de marque du service d'argent mobile n'est pas ternie.
- Le bénéficiaire se sent obligé de rendre l'argent s'il ne lui appartient pas, car l'appel provient de l'opérateur.
- Le processus est moins coûteux pour les deux parties à l'opération, car il n'y a pas de frais supplémentaires pour le remboursement des fonds.

Inconvénients

- Le bénéficiaire peut malgré tout refuser de rendre l'argent.
- Le processus prend du temps, car il est nécessaire de joindre les deux parties.
- Il est coûteux pour l'entreprise, car celle-ci doit affecter des ressources pour assurer la gestion des annulations d'opération.
- Cette approche est préférable pour protéger l'image de marque de l'entreprise, mais des mesures supplémentaires seront nécessaires pour réduire la fréquence des annulations d'opérations et donc le risque de fraude. Ces mesures peuvent notamment prendre les formes suivantes :
    - Donner la possibilité aux clients de télécharger directement dans le menu des services financiers mobiles les numéros de téléphone provenant de leurs contacts ou de leur carte SIM vers lesquels ils souhaitent transférer de l'argent.
    - Encourager les entreprises à s'enregistrer pour des services qui leur sont destinés au lieu d'utiliser des services destinés aux particuliers.
    - Ajouter une clé de vérification aux numéros de compte des entreprises et, si possible, des particuliers.
    - Informer les clients de la politique d'annulation d'opérations.

c) Fraude à l'encontre des partenaires commerciaux (entreprises)

TYPE DE FRAUDE	EXEMPLE	MESURES DE PRÉVENTION
Usurpation de l'identité d'entreprises : les fraudeurs se font passer pour des agents d'une entreprise et encaissent des paiements au nom de celle-ci. Ils contactent les consommateurs en communiquant les coordonnées de leur compte personnel d'argent mobile qu'ils font passer pour celui d'une entreprise.	Un fraudeur met en place des équipements de point de vente (avec affiches et signalétique) dans un quartier défavorisé d'une grande agglomération en se faisant passer pour un représentant de l'une des principales compagnies d'assurance d'Afrique de l'Est. Il encaisse ainsi à titre personnel des primes d'assurance. Ce type de fraude est plus répandu sur les marchés arrivés à maturité, où le taux d'adoption des paiements mobiles chez les entreprises est élevé.	• Définir et publier une procédure précise de recrutement des entreprises, avec des règles précises de vigilance à l'égard des clients (KYC). • Les organisations doivent se doter d'une procédure précise de décaissement pour éviter toute erreur dans les versements. • Processus complet couvrant la détection, la surveillance, la communication et la gestion de la fraude. • Application de sanctions pour les agents qui ne respectent pas les règles d'enregistrement des entreprises en tant que clients de l'argent mobile.
Décaissements erronés conservés par les destinataires : il arrive que des organisations B2C fassent des virements erronés en faveur de personnes qui décident de retirer cet argent. Bien qu'il s'agisse d'une erreur d'opération à l'origine, il y a fraude lorsque les destinataires décident de retirer l'argent et de clôturer leur compte d'argent mobile.	Une organisation a viré par erreur des sommes plus importantes que prévu sur les comptes de participants à une enquête, les versements ayant été multipliés par dix. Par chance, elle a été en mesure d'annuler les versements avant que les destinataires puissent retirer les fonds.	• Il doit y avoir un processus précis de remontée d'informations pour signaler les cas de fraude et sensibiliser le marché à la fraude. • Les entreprises doivent effectuer un rapprochement comptable quotidien de leurs débits/crédits par rapport à leurs systèmes internes.

ANNEXE 2 : FRAUDE LIÉE AUX AGENTS

a) Fraude des agents à l'encontre des consommateurs

Les agents entretiennent les contacts les plus étroits avec les abonnés. Ils jouent un rôle crucial pour enregistrer les clients et traiter leurs opérations de dépôt et de retrait d'espèces. Aux débuts du développement des services financiers mobiles, ils sont en première ligne pour informer les consommateurs, leur montrer comment utiliser les services et leur vendre la proposition de valeur du produit. Par la suite, ils forment les clients aux nouveaux produits et services. Les fraudes commises par les agents peuvent prendre les formes suivantes :

FRAUDE	EXEMPLE	MESURES DE PRÉVENTION
Accès non autorisé au code confidentiel (PIN) des clients pour ensuite retirer des fonds sur leur compte	Une grande banque d'Afrique de l'Est a noté une augmentation des réclamations relatives à des doubles retraits chez les agents. L'enquête a montré que les agents obligeaient les clients à répéter des opérations sous le prétexte que leur opération initiale n'avait pas été enregistrée. Ils le faisaient en désactivant l'impression des reçus sur leur terminal de point de vente.	• Mettre au point des procédures détaillées de vérification des antécédents des agents afin d'éviter de recruter des agents qui ont mauvaise réputation ou sont susceptibles de commettre des fraudes (par exemple ceux qui ont un casier judiciaire). • Documenter tous les tarifs applicables aux clients et les communiquer par le biais de supports marketing obligatoires. Les agents doivent avoir l'obligation d'afficher les tarifs dans leur point de vente. • Mener des campagnes périodiques et planifiées d'information des consommateurs sur la protection de leur code confidentiel, afin de les dissuader de le divulguer à des tiers. Veiller à ce que la documentation correspondante soit également disponible dans tous les points de vente. • Organiser des visites mystère et des visites de contrôle (audits) des agents. • Faire appliquer des sanctions légales pour les agents qui participent à des fraudes, prévoyant notamment la résiliation de leur contrat. • Impliquer les autorités d'application de la loi dans la gestion et la détection de la fraude. Les agents impliqués dans des cas de fraude devraient faire l'objet de poursuites judiciaires avec publication de leurs agissements pour attester de la volonté de l'entreprise de lutter contre la fraude.
Utilisation non autorisée du code confidentiel des clients pour retirer de l'argent sur leur compte, un cas de fraude fréquent avec des clients récents et illettrés qui confient leur code à l'agent.	Un opérateur récent d'Afrique de l'Est a découvert des cas de fraude commise par les agents à l'encontre de clients non enregistrés. Les agents affirmaient que le code confidentiel communiqué par ces clients analphabètes ne marchait pas et s'en servaient pour retirer de l'argent à un autre endroit.	
Retraits fractionnés : les agents obligent les clients à fractionner leurs retraits en leur faisant croire qu'ils n'ont pas assez d'argent liquide pour traiter l'opération.	Ce type de fraude a été signalé en Asie et en Afrique. Les agents dont les commissions dépendent d'un barème par tranches de montant prétendent ne pas avoir assez d'espèces et demandent aux clients de faire des opérations de plus faible montant. L'agent encaisse ainsi davantage de commissions, tandis que les clients paient davantage de frais.	
Facturation de surcharges non autorisées : les agents facturent parfois des frais supplémentaires en plus des tarifs officiels, ce qui renchérit le coût du service pour les clients.	La facturation de surcharges a été signalée en Asie du Sud. Certains agents facturent des frais de transport, de « traitement accéléré », etc. Dans certains cas, le client est au courant de ces frais supplémentaires mais n'a pas le choix. Dans d'autres, il n'est pas au courant.	

FRAUDE	EXEMPLE	MESURES DE PRÉVENTION
		• Définir et faire appliquer des exigences de monnaie électronique et d'espèces pour les agents. • Mettre au point des outils de gestion de la liquidité des agents pour surveiller leurs besoins en monnaie électronique et en espèces. Ces outils pourraient être utilisés par l'agent et par l'opérateur d'argent mobile pour anticiper les besoins journaliers, hebdomadaires et mensuels. Ils pourraient également fixer des seuils en fonction de la saisonnalité, des activités ou de certains événements susceptibles d'influer sur leurs besoins. • Automatisation des commissions facturées aux clients et de celles versées aux agents, que ce soit sur la plateforme de l'argent mobile ou sur celle de l'organisation cliente.

b) Fraude des agents à l'encontre des opérateurs d'argent mobile

La relation entre les agents et les opérateurs d'argent mobile est mutuellement avantageuse. Les agents sont rémunérés pour les opérations qu'ils traitent tandis que les opérateurs étendent leur service à un public plus large, de façon plus rapide et plus pratique. Les agents peuvent profiter de certaines failles de la plateforme et des processus de l'argent mobile pour se procurer des revenus supplémentaires. Les fraudes de cette nature peuvent prendre les formes suivantes :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Dépôts fractionnés[10] : les agents incitent les clients à faire plusieurs remises de montant moins élevé pour permettre à l'agent de toucher davantage de commissions. Les dépôts fractionnés sont plus courants lorsque les commissions des agents varient par palier ou prennent la forme d'un montant fixe par opération (commission forfaitaire). Il n'y a pas d'incitation à fractionner les opérations lorsque les commissions sont basées sur un pourcentage du montant de l'opération.	Plusieurs opérateurs importants d'Afrique de l'Est ont connu des volumes importants de dépôts fractionnés qui ont alourdit leurs structure de coût. Les agents encaissaient davantage de commissions, ce qui avait un impact négatif sur la rentabilité du service pour les opérateurs. Les opérateurs ont lutté contre ce phénomène en produisant des rapports de surveillance des dépôts fractionnés, ce qui a considérablement amélioré leur rentabilité.	• Documenter les obligations contractuelles des agents en ce qui concerne les dépôts fractionnés et imposer des sanctions appropriées à ceux qui recourent à cette pratique. • Mener des campagnes d'information pour sensibiliser les consommateurs à ce type de fraude, au moyen notamment de brochures commerciales, d'affiches et de prospectus. • Analyser et passer en revue la structure des commissions versées aux agents pour détecter les éventuelles anomalies et les corriger. Il est conseillé de réaliser cet examen deux fois par an.
Dépôts directs : les services mis en place par les ORM obligent les clients[v] à déposer de l'argent sur leur compte d'argent mobile (opération gratuite) pour faire des virements (qui sont une opération payante). Les agents peuvent inciter les clients à éviter cette facturation en déposant l'argent directement sur le compte du bénéficiaire.	Un opérateur d'Afrique australe se heurte à des difficultés concernant les dépôts directs, car les clients préfèrent déposer directement l'argent sur le compte des bénéficiaires pour ne pas payer de frais de transfert. La facturation de l'opérateur comprend les frais de transfert et les frais de retrait.	• Organiser des visites mystère chez les agents pour détecter l'existence de dépôts fractionnés ou de dépôts directs et vérifier le respect des obligations de vigilance à l'égard des clients (KYC). • Mettre au point des systèmes intelligents capables de repérer les dépôts directs au moyen du réseau GSM. Les donnés GSM permettent de repérer les dépôts effectués chez un agent et crédités sur un compte situé à un autre endroit.
Virements parallèles entre agents : les agents peuvent faciliter des virements officieux dans le cadre de transferts inter-agents qui sont généralement gratuits pour les agents.	Certains agents d'Afrique australe et d'Asie du Sud ont mis au point un système parallèle de transfert d'argent : ils envoient les fonds à un autre agent dont ils donnent les coordonnées au client pour le retrait. Le système est avantageux pour l'agent et le client, mais prive l'opérateur de revenus.	• Les régulateurs doivent fixer des règles concernant les obligations de conformité et de déclaration. Les opérateurs d'argent mobile doivent faire des déclarations périodiques sur des indicateurs clés de conformité.

10 Voir la « Focus Note » nº 71 de *MSC India* intitulée *Sustainability of BC Network Managers (BCNMs) in India - How are BCNMs Paid?*

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Enregistrement de clients sur la base de fausses pièces d'identité ou sans vérification de leur identité : ces pratiques peuvent être le fait d'agents malhonnêtes dans le but d'accroître leurs revenus ou de faciliter des fraudes perpétrées par des clients enregistrés. **Enregistrement de faux clients** en enregistrant des numéros de téléphone qui ne sont pas encore affectés à des abonnés, dans le but de générer des commissions supplémentaires. **Enregistrement de personnes au nom d'entreprises** dans le but d'encaisser des paiements provenant du public.	Beaucoup d'opérateurs d'Afrique de l'Ouest et d'Afrique de l'Est ont entrepris des opérations de nettoyage de leurs fichiers clients après avoir déterminé que certains enregistrements étaient inexacts. Des contrats d'agent ont été résiliés par des opérateurs d'Afrique de l'Est suite à l'enregistrement frauduleux de clients. En Asie, il y a eu des cas d'enregistrement de consommateurs qui n'étaient pas intéressés par le service dans le seul but de partager la commission avec l'agent. Cette pratique a conduit à des taux importants de comptes inactifs. En Afrique de l'Est, des opérateurs mobiles ont rencontré le cas d'agents qui enregistraient des clients particuliers comme des entreprises. Il y a souvent dans ce cas collusion entre l'agent et les fraudeurs. Des agents négligents peuvent être amenés à enregistrer involontairement des fraudeurs comme des entreprises en infraction de leurs obligations de vigilance à l'égard des clients (KYC).	• Les régulateurs doivent user de leur autorité pour faire respecter des normes chez les opérateurs d'argent mobile. Ils peuvent suspendre ou annuler l'agrément de l'opérateur et l'obliger à agir de manière plus proactive. • Les régulateurs doivent rester à l'écoute du public et faire des suggestions aux opérateurs en réponse aux problèmes rencontrés dans l'enregistrement des clients. • Les régulateurs et les opérateurs d'argent mobile devraient mettre en place un enregistrement des abonnés sur les réseaux mobiles et le rattacher à celui de l'argent mobile. • Les opérateurs d'argent mobile devraient travailler en étroite collaboration avec les autorités nationales chargées de l'émission des pièces d'identité pour la vérification des documents d'identification. • Procédure approuvée d'enregistrement des clients couvrant les documents exigés des clients et préparation de manuels de formation destinés à l'ensemble des prestataires de distribution. • Diviser la commission d'enregistrement des clients entre enregistrement et activation du compte (opération). • Facturer aux agents les commissions illégalement encaissées.
Blanchiment de capitaux : abus de la fonction de représentant d'un opérateur d'argent mobile pour servir d'intermédiaire à des activités de blanchiment de capitaux ou d'autres activités criminelles.	Ce type de fraude n'a pas été signalé jusqu'à présent, mais il est peu probable que des agents tirent parti de leur relation avec des opérateurs d'argent mobile pour blanchir des capitaux ou servir de façade à des activités illicites.	

c) Fraude du personnel à l'encontre des agents

Les agents sont en première ligne des services financiers mobiles. Ils sont motivés par les revenus tirés de l'enregistrement des clients et du traitement de leurs opérations de dépôt et de retrait d'espèces et embauchent des salariés pour s'occuper de ces opérations. Cela crée un nouvel ensemble de possibilités de fraude qu'ils doivent gérer dans le cadre de leur exploitation courante. Un niveau élevé de fraude par le personnel peut compromettre la viabilité de l'activité de l'agent et par conséquent sa volonté et/ou sa capacité à investir dans cette activité.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Détournement des fonds de l'agent par ses employés, qui « se servent dans la caisse » pour ensuite démissionner, disparaître ou continuer de travailler jusqu'à être démasqués par leur employeur. **Sous-évaluation des encaisses** : les employés de l'agent sous-estiment systématiquement les encours d'espèces du point de vente et investissent la différence dans leur propre entreprise ou activité. Dans certains cas, les employés s'entendent avec ceux d'autres agents et se font des avances entre eux pour couvrir les écarts de caisse en cas de contrôle par leur employeur respectif. **Fraude par imitation** : les employés peuvent profiter de la recrudescence d'un certain type de fraude pour prétendre en être les victimes et détourner l'argent soi-disant « perdu » vers leur propre compte.	Un agent d'Afrique centrale a dû fermer définitivement un point de vente parce que son employé avait disparu avec la totalité de la caisse et de son encours en monnaie électronique. Il hésite à ouvrir d'autres points de vente tant qu'il n'est pas en mesure de gérer ce risque. Un agent d'un opérateur important d'Afrique de l'Est déclare avoir noté que l'encours de monnaie électronique de l'un de ses points de vente fluctuait en moyenne 50 % en dessous de son investissement d'origine. Interrogée, l'employée du point de vente a nié tout écart. Le chef d'entreprise a organisé une visite de contrôle surprise en se rendant sur place avant l'ouverture. Après rapprochement des comptes, la moitié de l'investissement était manquant, sans que l'employée puisse fournir d'explication. Elle avait en fait détourné l'argent vers des activités personnelles. Elle a rapidement été arrêtée et a remboursé l'argent.[vi] Un certain nombre d'agents sont persuadés que lorsque certaines fraudes augmentent, certains de leurs employés y participent et prétendent être les victimes des fraudeurs. Ce n'est pas à exclure, car ce type de fraude se produit également dans d'autres services financiers et dans le commerce de détail.	• Les prestataires de distribution devraient contrôler les antécédents de leurs employés avant leur embauche pour vérifier qu'ils sont dignes de confiance et n'ont pas d'antécédents criminels non déclarés. • Les prestataires de distribution doivent mettre en place des procédures de double autorisation pour toutes les opérations en ligne afin de responsabiliser leur personnel : un employé initie l'opération et un second la contrôle. • Les prestataires de distribution devraient procéder à des contrôles fréquents et non planifiés de leurs points de vente afin de vérifier les encaisses en liquide et en monnaie électronique. • Les prestataires de distribution doivent s'assurer que tous les points de vente procèdent à un arrêté de caisse journalier à la fermeture (pour les espèces et pour l'encours de monnaie électronique) et signalent toute différence. • Les opérateurs d'argent mobile devraient diffuser des rapports produits par leur plateforme pour aider leurs prestataires de distribution à gérer leur activité. • Les opérateurs d'argent mobile devraient créer des forums permettant aux prestataires de distribution d'échanger des idées sur les différents problèmes de fraude et les meilleures pratiques de lutte contre la fraude.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Fraude sur les commissions immédiates : dans les modèles où les commissions sont versées immédiatement aux agents, ceux-ci ont du mal à faire leur rapprochement comptable des commissions encaissées, car celles-ci sont mélangées aux autres opérations d'argent. Les employés en profitent pour duper leurs employeurs.	En Afrique de l'Ouest, les agents d'un important service d'argent mobile sont confrontés à des difficultés de rapprochement des commissions gagnées sur les opérations qu'ils réalisent, car celles-ci sont immédiatement créditées sur leur compte d'argent mobile. Le service envisage de les regrouper pour faire un versement unique en fin de mois.	• Les prestataires de services financiers mobiles devraient coopérer avec leurs agents de distribution pour trouver des contrats d'assurance contre la fraude à des prix abordables qui leur permettent de se protéger du risque de détournement de fonds par des salariés ou du risque de cambriolage. • Création d'une liste noire des salariés d'agents qui se sont rendus coupables d'activités frauduleuses. • Implication des forces de l'ordre dans les enquêtes sur les cas de fraude. • Versement groupé des commissions dues aux agents à l'issue d'une période donnée, dans l'idéal une fois par mois. Ce versement doit être accompagné d'un rapport détaillant les commissions gagnées, le mode de paiement et les références de celui-ci.

d) Fraude perpétrée par les master-agents

Les master-agents sont nommés par les prestataires de services financiers mobiles pour gérer les points de vente qui forment leur réseau de distribution. Ils jouent un rôle déterminant pour aider les agents sur le terrain et faciliter leur mise en place pour le compte de l'opérateur d'argent mobile. Les master-agents doivent faire preuve d'une grande intégrité, faute de quoi leur comportement peut avoir un impact négatif sur la confiance des parties prenantes à l'égard du système. Les fraudes les plus couramment commises par des master-agents sont les suivantes :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Prélèvements non autorisés sur les comptes des agents : les master-agents peuvent faire des prélèvements non justifiés sur les comptes des agents dont ils ont la responsabilité, ce qui prive ces agents de leur argent et des revenus qu'ils sont censés percevoir sur les opérations qu'ils traitent.	Pendant la phase de démarrage d'un service d'Afrique de l'Est, un certain nombre d'agents d'un service d'Afrique de l'Est se sont plaints de master-agents qui prélevaient de l'argent sur leur compte d'argent mobile sans leur autorisation. L'opérateur a mis en place des restrictions d'accès aux comptes des agents, ce qui a permis d'éliminer ce type de fraude.	• Définition précise des fonctions d'agent et de master-agent pour le processus de recrutement des prestataires de distribution. • Contrats et règlements détaillés pour le fonctionnement des master-agents en termes d'obligations, de personnel et d'exigences pour le recrutement des agents. • Directives opérationnelles approuvées définissant clairement les conséquences d'une mauvaise gestion des agents par les master-agents et le processus à suivre pour remédier aux défaillances le cas échéant. • Mise en place de directives relatives au partage des commissions entre agents et master-agents et communication de celles-ci au sein de la plateforme d'argent mobile pour garantir une application uniforme au sein des réseaux de distribution. • Permettre aux agents de réaliser des opérations indépendamment des master-agents. Limiter la fonction de master-agent à la gestion de la relation et à la diffusion de rapports. • Permettre le crédit direct de la part des commissions revenant aux agents sans que les master-agents aient à recevoir puis reverser cet argent. • Audit indépendant des agents pour documenter la performance des master-agents. • Mettre des canaux de communication adéquats à la disposition des agents (lignes d'appel, adresses e-mail, forums d'agents) pour qu'ils puissent donner leur feedback.
Déductions injustifiées sur les commissions gagnées par les agents : les master-agents peuvent surévaluer les taxes applicables ou sous-évaluer les commissions dues aux agents pour réduire les sommes qui leur sont versées.	Ce type de fraude a été signalé en Afrique et en Asie. Les agents sont censés recevoir un certain pourcentage du total des commissions sur opérations. Certains master-agents ne leur reversent qu'une partie de ce pourcentage, se gardant la différence pour eux, ce qui réduit d'autant les commissions reversées aux agents. Ce type de fraude porte atteinte à la crédibilité de l'opérateur d'argent mobile et décourage les agents d'investir davantage dans cette activité.	
Revente non autorisée des outils nécessaires à l'activité d'agent[vii] : les master-agents reçoivent des outils destinés au fonctionnement des points de vente qu'ils revendent aux agents au lieu de simplement les activer.	Ce type de fraude a été signalé dans plusieurs services d'Afrique de l'Est. Les opérateurs d'argent mobile y mettent fin en résiliant les contrats des entreprises concernées.	

ANNEXE 3 : FRAUDE LIÉE AUX PARTENAIRES COMMERCIAUX

a) Fraude perpétrée par le personnel des organisation C2B et B2C

À mesure que l'argent mobile se développe, les opérateurs élargissent leurs services pour répondre à l'évolution des besoins des clients. Les nouveaux services s'accompagnent de nouvelles formes de fraude. Les employés des entreprises partenaires peuvent tirer parti des failles du système dans les procédures, les plateformes ou les contrôles internes pour commettre des fraudes à l'encontre des entreprises. En raison de la sensibilité de ce sujet chez les entreprises, les cas de fraude sont rarement, voire jamais signalés. Les formes de fraude habituelles sont les suivantes :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Les employés et les fraudeurs associent des numéros de téléphone frauduleux aux comptes bancaires : des employés complices associent le numéro de téléphone de fraudeurs aux comptes bancaires de client pour leur permettre de retirer de l'argent sur ces comptes.	Dans le cadre de la mise en place de retraits bancaires au moyen de l'argent mobile, un employé d'une grande banque d'Afrique de l'Est avait frauduleusement associé le numéro de compte d'un client à son numéro de téléphone portable. Il pouvait ainsi retirer de l'argent sur le compte du client en utilisant son propre code confidentiel. Il a rapidement été démasqué et licencié.	• Les entreprises clientes devraient procéder à un rapprochement comptable quotidien de toutes leurs opérations d'argent mobile pour détecter tout écart éventuel. • Les entreprises devraient conserver des comptes distincts pour leurs paiements et leurs encaissements afin de limiter leur exposition à la fraude. • Tous les paiements effectués à partir du compte d'argent mobile d'une entreprise devraient faire l'objet d'une double autorisation par deux personnes distinctes.
Annulation injustifiée de paiements de clients en faveur de l'entreprise : des employés de l'entreprise annulent des opérations sur le compte d'argent mobile de l'entreprise, alors qu'il s'agit du paiement légitime de services, pour se partager le produit de l'annulation avec l'émetteur du paiement.	Ce type de fraude n'a pas encore été signalé ou rendu public. Il peut toutefois se produire si l'entreprise n'a pas des systèmes de contrôle suffisamment solide pour la surveillance des paiements et des annulations d'opérations.	• Pour les clients qui associent leur compte bancaire à un compte d'argent mobile, l'établissement bancaire doit veiller à ce que : ○ Le client remplisse une demande dûment signée auprès de la banque pour demander le rattachement des comptes ; ○ Un responsable de la banque confirme la demande après du client par un autre moyen (visite ou appel téléphonique). • La banque doit envoyer une notification au titulaire du compte bancaire concerné par la demande rattachement à un compte d'argent mobile.
Transferts illégaux à partir du compte d'argent mobile de l'entreprise par les employés en charge des paiements. Cela peut inclure des virements en faveur de bénéficiaires qui n'y ont pas droit, des faux paiements, etc.	Ce type de fraude n'a pas encore été signalé ou rendu public. Il pourrait se produire en cas d'entente entre les employés et les fraudeurs pour créer des faux utilisateurs et émettre des paiements en leur faveur.	• Les banques doivent mettre en place un plafond journalier sur les opérations que les clients peuvent réaliser avec leur compte d'argent mobile. • Les établissements devraient limiter le nombre de personnes ayant le pouvoir de rattacher un compte bancaire à un compte d'argent mobile. • Les établissements doivent conserver un registre des personnes qui effectuent des changements quelconques sur la plateforme de services bancaires mobiles.

b) Fraude à l'encontre des opérateurs mobiles par les organisations B2C et C2B

Les partenaires commerciaux peuvent détourner des revenus qui appartiennent aux opérateurs d'argent mobile. La source de fraude la plus probable est la collusion entre employés et fraudeurs, comme détaillé ci-dessous :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Collusion d'employés de l'opérateur d'argent mobile avec des clients, des partenaires commerciaux et/ou des agents pour l'application frauduleuse de tarifs plus bas.	La probabilité de ce type de fraude est plus grande pour les opérations qui concernent des entreprises, car les employés de l'opérateur ont dans ce cas davantage de flexibilité pour appliquer des tarifs différents selon les organisations.[ix]	• Documentation des tarifs et commissions applicables et mise en place de procédures précises en matière de politique tarifaire, de parties concernées, de règles commerciales et de période d'application. • Documentation d'un processus précis de mise en œuvre technique et de vérification des tarifs et commissions convenus, indépendamment du processus d'autorisation. • Séparation des rôles entre les personnes qui définissent les règles commerciales, les tarifs applicables au client et les commissions des agents et celles qui sont chargées de leur mise en œuvre au sein de la plateforme. • Contrôles réguliers et ponctuels des tarifs et commissions appliqués et des paramètres techniques • Automatisation de la facturation des frais applicables aux clients C2B avant retrait ou décaissement des fonds. Lorsqu'une entreprise cliente retire des fonds provenant d'encaissements sur le système, les frais doivent être débités automatiquement avec mise à disposition d'un relevé d'opérations sur le système.
Fraude sur le règlement des frais[viii] : les partenaires C2B des opérateurs sont censés régler les frais d'opération sur leurs encaissements avant de pouvoir les retirer. Si la plateforme le permet, ils peuvent retirer la totalité des fonds sans régler les frais qu'ils doivent au prestataire de services financiers mobiles.	Des opérateurs mobiles d'Afrique de l'Est ont signalé des cas d'entreprises partenaires qui avaient omis par négligence de régler leurs frais lors du retrait de leurs encaissements. Ce risque augmente avec le recrutement d'un nombre croissant d'organisations qui utilisent l'argent mobile pour faire des encaissements ou des décaissements.	

ANNEXE 4 : ADMINISTRATION ET GESTION DES SYSTÈMES

La crédibilité des services financiers mobiles repose sur l'exactitude et la rapidité du traitement des opérations. Le fait que ces services soient fondés sur la technologie génère tout un ensemble de risques spécifiques. Ces risques sont liés à l'administration des systèmes, à la gestion des mots de passe et à l'usage abusif des droits d'accès. Le tableau ci-dessous présente les types de fraude les plus courants dans ce domaine et les mesures de prévention correspondantes.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION[x]
Utilisation malhonnête des mots de passe permettant d'accéder à la plateforme d'argent mobile par différents utilisateurs, comprenant les super-administrateurs, super-utilisateurs, administrateurs et autres utilisateurs du système. **Création de faux utilisateurs** sur la plateforme d'argent mobile en ligne. Ces utilisateurs servent à initier et approuver des opérations sur la plateforme ou les téléphones pour détourner de l'argent sur les comptes d'argent mobile d'agents ou d'entreprises clientes, ce qui réduit la capacité de l'opérateur à remonter à la source de la fraude. **Utilisateurs dotés de droits multiples** : les utilisateurs qui ont le droit d'initier et de valider des opérations ont le pouvoir d'escroquer l'organisation qui leur a attribué ces droits.	Ce type de fraude n'a pas encore été reconnu publiquement.[xii] Il est susceptible de se produire au moment de la création d'utilisateurs par l'administrateur du système. Celui-ci peut consulter le mot de passe de l'utilisateur, mais celui-ci n'est pas invité à le changer. L'administrateur peut alors profiter de cet accès pour faire des changements sur les comptes de clients. Ce type de fraude n'a pas encore été signalé. Il pourrait toutefois se produire lorsque les systèmes de contrôle d'accès à la plateforme technique de l'argent mobile ne sont pas adéquats. Ce type de fraude a été signalé par un master-agent dans un service d'Afrique de l'Est. Il se produit lorsque les chefs d'entreprise n'ont de contrôles internes suffisants. Les employés en profitent pour détourner de l'argent et produire de rapprochements comptables pour leur employeur.	**Droits des super-administrateurs** • Séparation claire des rôles dans le système entre super-administrateurs, administrateurs, super-utilisateurs et utilisateurs. Le rôle des super-administrateurs doit se limiter à la création/suppression des administrateurs et super-utilisateurs, et celui des administrateurs à la création/suppression des utilisateurs. Le rôle des utilisateurs doit quant à lui être limité au traitement des opérations. • Les super-administrateurs doivent être approuvés et mis en place avec l'accord du plus haut niveau hiérarchique du prestataire de services financiers mobiles. Toute la documentation correspondante doit être conservée. • La création ou la suppression des administrateurs doit s'effectuer en deux étapes : ✓ Demande documentée d'une personne autorisée pour le compte de l'organisation selon une procédure approuvée ✓ Mise en œuvre du changement demandé sur la plateforme par le super-administrateur. • Automatisation de la création de mots de passe sur le système de l'argent mobile pour qu'ils ne soient pas visibles par des tiers. Tous les utilisateurs doivent avoir l'obligation de changer leur mot de passe lorsqu'ils se connectent au système pour la première fois. • La création ou la suppression des utilisateurs doit s'effectuer sur un terminal (ordinateur) sécurisé équipé de certificats de sécurité, cette procédure devant faire l'objet de contrôles fréquents.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION[x]
Fraude sur les canaux multi-accès (web et téléphone) : les systèmes accessibles à distance, à partir par exemple d'un cybercafé, peuvent être pénétrés par des fraudeurs possédant les coordonnées d'accès aux comptes. Il est également bien connu que des fraudeurs peuvent installer des logiciels sur des ordinateurs publics pour enregistrer les mots de passe utilisés. Dans certains cas, les fraudeurs peuvent accéder aux informations des cartes SIM pour créer des cartes clones, comme cela est courant dans le secteur des cartes de paiement.	Un opérateur important d'Afrique centrale a détecté un cas de fraude dans lequel les fraudeurs utilisaient l'Internet pour transférer de l'argent à partir des comptes d'argent mobile des agents.	**Administrateurs** • Les administrateurs doivent être créés et supprimés par le super-administrateur sur la base d'une lettre d'autorisation provenant du département/service de l'utilisateur. • Les administrateurs doivent être limités à la création/suppression d'autres utilisateurs, sans autres fonctions opérationnelles. • Une liste générée par le système des utilisateurs créés par les administrateurs doit être transmise au niveau hiérarchique le plus élevé de l'organisation pour notification. • Idéalement, les nouveaux utilisateurs ne devraient être opérationnels sur le système qu'à l'issue d'une période de 24 heures après leur création et après validation par le niveau hiérarchique le plus élevé de l'organisation/département concerné.
Mots de passe/codes confidentiels faciles à deviner[xi] : Les mots de passe et codes confidentiels peu robustes peuvent être découverts par les fraudeurs à force d'essayer. Les codes confidentiels à 4 chiffres sont particulièrement exposés à ce risque, car beaucoup de clients utilisent leur date de naissance.	Chez les prestataires d'argent mobile d'Afrique, il existe de nombreux cas de clients escroqués par des proches qui arrivent facilement à deviner leur code confidentiel.	**Utilisateurs** • Établir des procédures précises pour chaque type d'opération. • Fixer des plafonds d'opération pour les différents types d'utilisateurs. Pour les opérations simples de service à la clientèle, comme les dépôts ou les retraits d'espèces, les utilisateurs peuvent effectuer les opérations sans avoir besoin d'un accord. • Pour les opérations plus complexes ou les opérations réalisées en ligne, il doit y avoir un processus en deux étapes : ✓ Un utilisateur initie l'opération ✓ Un deuxième utilisateur la valide. • Les utilisateurs ne doivent jamais être en en mesure d'initier et de valider la même opération. • Un registre des opérations doit être conservé avec le détail de toutes les demandes traitées sur la plateforme et la personne qui s'en est occupé.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION[x]
		Gestion des mots de passe et codes confidentiels (PIN) • Les mots de passe et codes confidentiels ne doivent jamais être partagés entre utilisateurs, super-utilisateurs, administrateurs et super-administrateurs. • Il est préférable que les mots de passe et codes confidentiels ne puissent pas être consultés par une autre partie que l'utilisateur concerné. Dans le cas contraire, les utilisateurs doivent avoir l'obligation de changer de mot de passe la première fois qu'ils se connectent. • Complexité des mots de passe et codes confidentiels : veiller à ce que les codes confidentiels aient plus de 4 chiffres pour éviter que les utilisateurs n'utilisent leur date de naissance. • Tous les terminaux (appareils) qui permettent de faire des opérations en ligne doivent être couverts par un certificat de sécurité et faire l'objet de contrôles réguliers. • Tous les certificats de sécurité doivent expirer automatiquement à l'issue d'un certain délai (n'excédant pas un an) et de nouveaux certificats doivent être émis à l'issue de ce délai. • Lorsque le nom d'un employé est supprimé de la liste, le certificat qu'il/elle utilisait doit être supprimé et un nouveau doit être émis au nom du remplaçant. • Le système d'argent mobile doit garder la trace de tous les certificats émis aux différentes équipes avec, de préférence, communication périodique à l'organisation. • Chaque organisation doit se doter d'une équipe de lutte contre la fraude, chargée notamment de mener des actions de sensibilisation auprès de l'ensemble des utilisateurs : agents, partenaires commerciaux et personnel des prestataires d'argent mobile.

=

ANNEXE 5 : FRAUDE LIÉE AUX PRESTATAIRES DE SERVICES FINANCIERS MOBILES

Ce type de fraude pourrait être qualifiée de « fraude familiale ». Elle est commise par les employés du prestataire de services financiers mobiles au détriment de l'entreprise, de ses partenaires et d'autres parties prenantes. Cette fraude interne porte atteinte à la crédibilité des services et provient généralement d'une défaillance des processus.

a) Fraude liée à la gestion financière

Le processus de création de l'argent mobile commence par le dépôt de fonds auprès d'un compte bancaire qui jour le rôle de compte « miroir » des encours d'argent mobile. Le montant des fonds déposés en banque doit être égal au total des fonds en circulation dans l'écosystème d'argent mobile. Cet écosystème se compose des consommateurs, des agents, des entreprises clientes et des différents comptes de recettes de l'opérateur. Ces fonds sont exposés à différents risques susceptibles de porter atteinte à la crédibilité du produit, dont notamment :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Accès non autorisé du personnel financier au compte d'argent mobile des agents ou des clients C2B et B2C en vue de transférer des encours d'argent mobile vers d'autres titulaires de compte.	Ce type de fraude n'a pas encore été signalé. Il pourrait néanmoins se produire dans des services dépourvus de procédures solides pour le dépôt et le transfert des encours de monnaie électronique.	• Le rapprochement comptable des encours bancaires et des encours de monnaie électronique doit être effectué quotidiennement et toute différence éventuelle doit être approuvée par un responsable de l'entreprise. • Les comptes d'argent mobile des entreprises et des agents ne doivent être ouverts qu'après autorisation de l'organisation, dans le cadre d'une relation contractuelle valable. • Les entreprises (agents/clients) doivent communiquer et certifier les coordonnées précises des contacts au sein de leur organisation ainsi que leurs coordonnées bancaires. • Tout changement dans la dénomination ou les coordonnées des titulaires de comptes d'agents ou d'entreprises clientes doit être dûment autorisé par un représentant officiel de l'organisation concernée. • Tous les postes de recette et comptes de crédit téléphonique doivent faire l'objet d'un rapprochement comptable quotidien pour en vérifier les soldes et les opérations au débit et au crédit. • Les comptes d'attente devraient être vérifiés et soldés quotidiennement, leur solde n'excédant pas 24 heures. • Mettre en place des procédures précises pour les tiers concernant les dépôts bancaires, la vérification des remises et la résolution des litiges sur les dépôts avec des normes claires de niveau de service.
Détournement de fonds appartenant au prestataire d'argent mobile : des employés escroquent l'opérateur d'argent mobile en visant la vente de crédit téléphonique, les frais facturés aux clients, des fonds non réclamés, des comptes inactifs ou d'autres sources de revenus. Les fonds peuvent être détournés vers des comptes fictifs pour être ensuite retirés du système d'argent mobile.	Un service d'Afrique de l'Est a failli perdre de l'argent à cause d'un employé qui avait essayé de retirer des fonds sur le compte de l'entreprise. Sa tentative a échoué grâce à des systèmes de contrôle efficaces. MTN Ouganda, qui fait partie d'un grand groupe international de télécommunications, a évoqué dans les médias une perte de plus de 9 milliards USHS (4 millions US$) en raison d'une fraude perpétrée par son personnel. D'après l'entreprise, cette fraude a été commise par des salariés qui avaient pu accéder aux fonds de l'entreprise après une mise à niveau du système.[xiii]	
Émission d'argent mobile en faveur d'organisations en contrepartie de fonds non compensés : le personnel chargé de l'émission de monnaie électronique peut être amené à émettre de l'argent mobile en contrepartie de fonds non compensés, comme par exemple des chèques, des virements	Cette fraude se produirait si une organisation déposait un chèque sur un compte en fiducie. Le montant du chèque ne serait crédité qu'après encaissement du chèque par la banque (compensation). En cas de collusion entre les employés et les remettants, les fonds pourraient	

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
télégraphiques ou d'autres méthodes de transfert, sans attendre que les fonds soient effectivement crédités au compte de l'organisation partenaire.	être crédités de manière anticipée. Ce type de fraude n'a pas encore été signalé dans les services financiers mobiles.	• Il est préférable que toutes les demandes de retrait provenant des partenaires commerciaux soient automatisées et traitées par des personnes autorisées, et non manuellement : l'employé se connecte à l'interface internet et fait l'opération au lieu d'adresser une demande écrite à l'opérateur.
Accès non autorisé aux comptes suspendus d'entreprises ou de prestataires de distribution : en cas de suspension prolongée, ces comptes sont exposés au risque de débits frauduleux.	Ce type de fraude n'a pas encore été signalé. Cependant, à mesure que les services se développent, il existe un risque accru d'opérations frauduleuses sur des comptes inactifs si les entreprises ne se sont pas dotées de systèmes de contrôle adéquats.	• En l'absence d'accès internet, toutes les demandes de retrait doivent être formulées sur du papier à entête et signés par une personne autorisée au sein de l'organisation. • L'équipe financière ne doit procéder au retrait qu'après avoir vérifié que la demande est légitime et provient de la bonne personne. • Le retrait des fonds doit être autorisé par au moins trois personnes différentes au sein du service d'argent mobile, dont deux personnes qui vérifient la validité de la demande dans le système et autorisent le débit des fonds sur le compte en banque. • Avant tout versement sur le compte d'un partenaire commercial, la personne autorisée de l'organisation concernée devrait être contacté pour valider le retrait avec un responsable de l'équipe du prestataire de services financiers mobiles. • Toute la documentation correspondante, comprenant les registres d'opération du retrait, doit être conservée et contrôlée périodiquement. • L'organisation doit définir les conditions et la durée d'inactivité[xiv] des comptes de particuliers et d'entreprises. Aucun compte sur lequel existe un solde significatif ne doit rester inactif pendant une période plus longue que celle fixée. Les comptes inactifs doivent être signalés et gelés et leurs titulaires doivent être contactés. • Les sommes correspondant aux bons de retrait en circulation doivent être contrôlées et vérifiées périodiquement, même si les bons restent inutilisés.

b) Équipes des centres d'appel

Les employés des centres d'appel sont le premier point de contact des consommateurs et autres parties prenantes qui contactent l'entreprise. Pour faciliter leur travail, ils ont accès à des sites dédiés qui leur permettent d'effectuer certaines opérations, comme par exemple des modifications sur les comptes des clients. Cette fonction présente des risques de fraude qui doivent être gérés par l'entreprise.

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION
Accès non autorisé[xv] aux registres d'appel à des fins personnelles : les équipes d'assistance à la clientèle ont accès aux données des clients et peuvent en profiter pour vendre des informations à caractère personnel à des tiers ou les communiquer à des fraudeurs.	Ce type de fraude n'a pas encore été signalé. Il pourrait typiquement se produire si un employé malhonnête fournissait des renseignements à des fraudeurs pour faciliter des activités de *phishing* ou d'extorsion de fonds.	• Le prestataire d'argent mobile doit être équipé d'un système CRM pour la gestion des réclamations des consommateurs. Ce système doit inclure les informations suivantes : o Nature du problème o Délai prévisionnel de résolution • L'entreprise doit avoir une procédure de remontée des réclamations de façon à traiter toutes les réclamations de clients et y apporter une solution.
Transfert non autorisé de fonds appartenant à des clients vers d'autres comptes au moyen des outils mis à la disposition des employés.	Ce type de fraude n'a pas encore été publiquement signalé par des prestataires. Il peut toutefois se produire si des comptes clients restent inactifs pendant une longue période.	• Les employés des centres d'appels doivent faire l'objet d'une vérification de leurs antécédents avant d'être embauchés.
Échanges non autorisés de carte SIM[xvi] lorsque la carte SIM d'un client est remplacée par une nouvelle sans son accord. Le titulaire de la nouvelle carte SIM peut accéder au compte d'argent mobile du client et y faire des opérations. Ces échanges peuvent être effectués délibérément par le personnel du prestataire de services financiers mobiles ou à la demande de fraudeurs qui parviennent à passer au travers des procédures de vérification.	Un opérateur d'Afrique centrale a licencié des employés qui s'étaient rendu coupables de cette fraude, tandis qu'un autre opérateur d'Afrique de l'Est a poursuivi un employé en justice.	• L'entreprise doit conserver un journal des opérations effectuées sur la plateforme, en gardant trace de tous les accès au système et aux comptes avec horodatage et numéros de référence. • Les fonctions d'assistance à la clientèle devraient être limitées à l'annulation d'opérations et ne pas inclure la possibilité de transférer des fonds entre des comptes. Les transferts de fonds devraient être remontés à une autre équipe, au sein du service d'assistance à la clientèle ou en dehors de celui-ci. • Documenter une procédure précise pour les changements de carte SIM, qui limite les personnes/organisations autorisées à procéder à des échanges et prévoit un délai entre le moment où l'échange a lieu et celui où il est activé.
Utilisation non autorisée des droits d'accès de collègues : les fraudeurs parviennent à se procurer leurs renseignements d'accès et s'en servent pour commettre des fraudes sur la plateforme d'argent mobile.	Certains employés des services financiers mobiles peuvent utiliser des mots de passe faciles à deviner ou être amenés à communiquer leur mot de passe, lequel est ensuite utilisé par des fraudeurs. Ce type de fraude n'a pas encore été publiquement signalé, mais se rencontre dans le secteur financier. Il est donc susceptible de se produire également dans les services financiers mobiles.	• Garder la trace des échanges effectués au moyen de rapports produits par le système.

c) Fraude par corruption des équipes commerciales

Il est largement reconnu que la clé de la réussite des services financiers mobiles est la gestion des structures de distribution. Les équipes commerciales sont chargées de la rechercher, du recrutement et de la gestion des agents. Cette fonction particulière peut donner lieu à des pratiques malhonnêtes de la part de ces équipes dans un but d'enrichissement personnel. Ce type de fraude prend les formes suivantes :

TYPE DE FRAUDE	EXEMPLES	MESURES DE PRÉVENTION

Sollicitation de pots de vin[xvii] **:** les employés peuvent solliciter de l'argent pour accorder des services en retour, comme par exemple l'agrément d'une candidature d'agent, l'ouverture de comptes commerciaux, etc.
 	
Fausses notes de frais : la gestion des prestataires de distribution exige de nombreux déplacements sur le terrain. Certains membres de l'équipe peuvent soumettre de fausses notes de frais au titre de leurs déplacements.
 	
Accès non autorisé aux renseignements personnels des agents : les employés peuvent demander à consulter les outils et registres des agents pour faire des changements sur leur compte en complicité avec des fraudeurs.
 	
Des employés complices peuvent collecter des dépôts auprès des agents sous le prétexte de les déposer pour leur compte.
	Les pratiques de corruption sont plus fréquentes sur les marchés arrivés à maturité. En Afrique de l'Est, un certain nombre de salariés ont été licenciés suite à des activités frauduleuses de cette nature.
	
	Les fausses notes de frais ne concernent pas seulement le secteur des services financiers mobiles, mais aussi beaucoup d'autres secteurs d'activité. En l'absence de systèmes de contrôle adéquats, elles peuvent entraîner des pertes substantielles pour l'entreprise.
	
	Bien qu'on ne connaisse pas de cas précis, les agents se plaignent parfois de personnes qui se font passer pour des employés de l'opérateur mobile pour accéder à leurs registres et associent cela à des fraudes qui se produisent ultérieurement.
	
	Une grande banque d'Afrique de l'Est a licencié un salarié qui avait encaissé les dépôts d'un agent au lieu de les déposer sur son compte.
	
	.
		• Définir et documenter un processus précis de recrutement et de gestion des agents. Ce processus doit couvrir les aspects suivants :
		  ○ Critères de sélection
		  ○ Délais et étapes d'agrément
		  ○ Traitement des litiges
		• Automatiser le processus de recrutement et le rendre public au moyen de canaux d'information appropriés.
		• Mettre en place de canaux de communication à la disposition des candidats pour signaler et faire connaître les failles et les cas de corruption dans le processus d'agrément.
		• Automatiser la totalité du processus de traitement des candidatures pour avoir la garantie que les problèmes soient signalés lorsqu'ils se produisent.
		• Définir et documenter précisément la relation entre la performance des prestataires de distribution et la mise à disposition de points de vente ou d'outils commerciaux supplémentaires.
		• Tous les recrutements d'agents doivent être autorisés sur la base d'une liste de contrôle et d'accords formalisés.
		• Conserver une base de données ou liste de suivi des outils commerciaux, comprenant les cartes SIM mises à la disposition des points de vente, récupérées, suspendues et soldées sur le marché. Ces outils doivent également être contrôlés par des audits réguliers.
		• Conserver une autorisation signée pour tous les outils mis à disposition des prestataires de distribution et installés sur le système d'argent mobile.
		• Examiner les rapports de tous les points de vente agréés comme agents pour vérifier qu'ils respectent les critères et normes de candidature/performance.

ANNEXE 6 : DÉFINITIONS

Administrateurs : sur une plateforme d'argent mobile, les administrateurs sont créés par des super-administrateurs (voir définition). Leur rôle consiste à gérer les fonctionnalités du système à différents niveaux, comprenant la création d'utilisateurs, les processus de fin de journée ou de sauvegarde, et l'entretien général du système.

Agents : les agents sont des points de vente, des commerces, des locaux ou des points de distribution où des opérations d'argent mobile sont réalisées pour le compte des prestataires d'argent mobile. Les agents servent de point d'enregistrement et de dépôt ou retrait d'espèces pour les clients. Ils reçoivent des commissions sur les opérations qu'ils traitent pour le compte de l'opérateur de services financiers mobiles.

Commission forfaitaire : dans un modèle de commissions forfaitaires, l'agent ou son organisation reçoit un montant fixe quel que soit le montant des opérations traitées. Ce type de commission est courant dans le secteur bancaire. Souvent, il ne rémunère pas adéquatement les opérations de montant élevé et peut donc inciter les agents à fractionner les opérations des clients.

Commission par palier (ou échelonnée) : commission versée aux agents en fonction de fourchettes de montant. La commission est fixe au sein de chaque fourchette, mais varie lorsque le montant de l'opération du client sort des limites de chaque fourchette. Ce type de commission a pour principal avantage de garantir une rémunération minimale à l'agent pour le traitement d'opérations de faible montant.

Commission proportionnelle (au pourcentage) : les commissions proportionnelles sont des commissions calculées comme un pourcentage du montant des opérations traités par les agents. Elles découragent les opérations de faible montant qui génèrent une rémunération négligeable et incitent les agents à réaliser des opérations de montant plus élevé.

Master-agents : également appelés super-agents, gestionnaire de réseau d'agents ou agrégateurs, les master-agents sont des organisations qui contrôlent ou gèrent un certain nombre de points de vente d'agents. Les master-agents sont généralement sélectionnés par le prestataire de services financiers mobiles.

Obligations de vigilance à l'égard des clients, ou KYC (de l'anglais « Know Your Customer ») : cette expression fait référence à un ensemble d'obligations imposées par les régulateurs et les opérateurs pour l'utilisation des services financiers mobiles. Ces obligations ont pour but de garantir que dans toute la mesure du possible, l'identité des personnes physiques ou morales clientes est dûment vérifiée avant qu'elles soient autorisées à faire des opérations au sein de l'écosystème. Ces obligations de vigilance sont généralement définies par les régulateurs, mais certains opérateurs peuvent choisir d'imposer des obligations supplémentaires. Les obligations de vigilance à l'égard des clients comprennent la vérification de leur identité avant de faire des opérations et la signature d'un bordereau d'opération pour confirmer la bonne fin des opérations.

Opérations B2B : de l'anglais « *business to business* » (entreprise à entreprise), ce terme désigne les opérations inter-entreprises, comme par exemple un transfert d'argent entre deux entreprises. Ces opérations ne sont pas très courantes dans les services financiers mobiles. Avec l'introduction de services marchands, ces opérations devraient se développer.

Opérations B2C : de l'anglais « *business to customer* » (entreprise à client) ou « *business to consumer* » (entreprise à consommateur), ce terme désigne les transferts émis par des entreprises en faveur d'abonnés. Il peut s'agir de prestations sociales, de versements de salaires, de décaissements de prêt ou de tout autre versement d'une organisation en faveur de particuliers.

Opérations C2C : de l'anglais « *customer to customer* » (client à client) ou « *consumer to consumer* » (consommateur à consommateur), ce terme désigne les transferts d'argent effectués entre deux abonnés de l'argent mobile qui sont des particuliers.

Opérations C2B : de l'anglais « *customer to business* » (client à entreprise) ou « *consumer to business* » (consommateur à entreprise), ce terme désigne les virements de particuliers en faveur d'organisations commerciales. Il peut s'agir de paiements marchands, de paiements de services collectifs, de primes d'assurance, de dépôts bancaires ou de tout autre transfert initié par une personne physique en faveur d'une personne morale.

Super-administrateurs : les super- administrateurs sont les personnes qui détiennent l'accès principal à la plateforme (y compris le mot de passe principal). En l'absence de super-administrateurs, la plateforme ne pourrait pas fonctionner.

Super-utilisateurs : la fonction de super-utilisateur est une fonction opérationnelle dotée de droits supérieurs pour le traitement des opérations sur la plateforme de services financiers mobiles. Les super-utilisateurs ont accès à tous les modules de la plateforme, à l'exception des modules d'administration et de mise en place. En générale, les super-utilisateurs approuvent différents droits accordés aux autres utilisateurs.

Tarifs forfaitaires : les tarifs forfaitaires sont des tarifs qui ne changent pas selon le montant de l'opération. Ce mode de tarification est courant dans le secteur bancaire qui l'étend parfois aux services bancaires sans agence. Dans les services financiers mobiles, ils sont courants dans les opérations entre pairs qui ne génèrent pas de coût supplémentaire pour les opérateurs.

Tarifs par palier (ou échelonnés) : les tarifs échelonnés sont des frais forfaitaires sur les opérations qui varient par palier en fonction de fourchettes de montant. Ce mode de tarification est courant dans les services financiers mobiles et s'inspire largement du modèle Western Union. On le rencontre fréquemment en Afrique de l'Est et en Afrique centrale.

Tarifs proportionnels (en pourcentage) : les tarifs calculés en pourcentage du montant des opérations sont largement inspirés du modèle de fonctionnement des cartes bancaires, dans lequel un certain pourcentage du montant des transactions est facturé aux commerçants. Les frais proportionnels sont courants en Afrique de l'Ouest, en Afrique australe et en Asie pour les opérations entre pairs. En Afrique de l'Est, ils s'appliquent aux paiements de services collectifs et aux paiements marchands.

Utilisateurs : sur une plateforme d'argent mobile, les utilisateurs sont créés par les administrateurs. Leur fonction consiste à traiter des opérations sur le système au sein de certains modules. Les utilisateurs sont généralement approuvés par des super-utilisateurs et leurs droits sont subordonnés à l'accord de ces super-utilisateurs.

Visites mystère : les visites mystère sont une méthode d'observation discrète par les parties prenantes, qui permettent de vérifier que les organisations ou les agents respectent les procédures obligatoires.

NOTES DE FIN DE RAPPORT

[i] Dans le cadre de ce document, les consommateurs sont des personnes physiques qui peuvent être clientes ou non du service considéré. Les actes frauduleux commis par des consommateurs sont les mêmes que le consommateur soit enregistré ou non. Dans de nombreux cas, un consommateur qui a l'intention de commettre une fraude peut s'enregistrer dans le seul but d'escroquer d'autres acteurs de l'écosystème de l'argent mobile. Dans d'autres cas, un consommateur peut être incité par un fraudeur à s'inscrire au service d'argent mobile pour pouvoir transférer de l'argent en faveur de ce dernier.

[ii] Les régulateurs protègent les informations des clients au moyen des lois relatives au respect de la vie privée. Celles-ci font de l'accès non autorisé aux données des clients un délit punissable par la loi. L'accès aux données personnelles des clients par des employés peut être motivé par l'appât du gain alors même s'il est passible de sanctions pénales.

[iii] Dans le cadre des barèmes de commissions par paliers, les commissions des agents exprimées en pourcentage du montant des opérations des clients sont plus élevées sur les opérations de faible montant que sur les opérations de montant plus élevé. Les agents peuvent donc encaisser davantage de commissions s'ils fractionnent un retrait en plusieurs opérations au lieu de le traiter comme une seule opération.

[iv] Au moment du lancement des services financiers mobiles d'un grand opérateur international de télécommunications en Afrique, les frais applicables aux clients n'étaient pas intégrés à la plateforme. Les clients devaient donc régler directement les agents en espèces. Ce système a entraîné de multiples surfacturations sur le marché en l'absence de pièces de monnaie et de change. Dans la pratique, les agents encaissaient davantage de commissions que ce qui était préconisé par le prestataire, ce qui a porté atteinte à la confiance des clients à l'égard du service, et l'opérateur a été obligé de changer de méthode. Par la suite, tous les frais d'opération et commissions des agents ont été intégrés au système.

[v] Beaucoup de services ne facturent pas les remises d'espèces pour encourager l'entrée de fonds dans le système des services financiers mobiles. Une fois que l'argent est entré dans le système, les opérateurs encaissent des revenus sur les opérations à venir, comme par exemple les virements, les retraits ou les achats de crédit téléphonique.

[vi] On observe également qu'en Afrique de l'Est, les agents préfèrent embaucher des femmes plutôt que des hommes, ayant le sentiment que ces derniers sont plus enclins à commettre des fraudes.

[vii] Les agents ont besoin de cartes SIM et de terminaux de point de vente pour traiter les opérations des clients. L'obtention de ces outils revient en pratique à obtenir le droit d'offrir des services financiers mobiles. Certains master-agents peuvent se procurer ces outils pour les revendre à des tiers.

[viii] Dans le cadre des encaissements C2B, les opérateurs n'autorisent les entreprises à déduire les frais du service de leurs recettes que lorsqu'elles souhaitent accéder à leurs fonds. Les employés de ces organisation doivent donc déterminer périodiquement ce qui est dû à l'opérateur sur le montant total des encaissements, pour déduire ces frais de leurs recettes. Beaucoup de plateformes ne déduisent pas automatiquement ces frais, ce qui fait que les organisations pourraient encaisser leurs fonds sans déduire les frais dus au prestataire de services financiers mobiles.

[ix] Dans la plupart des opérations impliquant des entreprises, les prestataires de services financiers mobiles appliquent des tarifs différents selon les entreprises. Dans certains cas, chaque entreprise client a son propre tarif. Cela se produit généralement lorsque l'opérateur a encore peu de partenaires commerciaux en place. Dans un certain nombre de services, les opérateurs fixent des tarifs différents par catégorie d'entreprises. Certaines entreprises bénéficieront de tarifs plus bas en raison de volumes prévisionnels élevés ou d'une relation privilégiée avec l'opérateur. Dans les deux cas, le service aura une procédure de mise en œuvre des tarifs convenus pour ces entreprises. Il est alors possible que les processus en place puissent faire l'objet d'abus par des employés s'ils ne sont pas assez solides.

[x] *The Observer : How **MTN lost mobile** billlions* par Jezz Mbanga (24 mai 2012). La nature exacte de cette fraude n'est pas précisée. Les reportages font état d'un accès non autorisé aux comptes des clients par des employés. L'opérateur affirme que les employés ont volé de l'argent directement à l'entreprise et que les comptes des clients n'ont pas été touchés. Quelle que soit la vérité, cette fraude montre qu'il existait des points de faiblesse dans les systèmes de contrôle de l'entreprise, qui ont conduit à la perte de plusieurs millions de dollars.

[xi] Le risque lié aux comptes inactifs est relativement important, surtout lorsque les services se développent. Dans le secteur bancaire, il existe une définition précise des comptes inactifs, qui font l'objet d'une surveillance particulière. Dans les services financiers mobiles, la notion d'inactivité des abonnés dépend de la réglementation applicable aux opérateurs de télécommunications concernant le recyclage des cartes SIM inactives. Dans de nombreux cas, le délai d'inactivité est de 6 mois. Beaucoup d'opérateurs n'ont pas encore de définition de l'inactivité pour les partenaires commerciaux ou les agents dont les comptes d'argent mobile ne sont pas soumis aux procédures de recyclage des cartes SIM. Il est clair que cela constitue un risque pour les opérateurs, qui devraient définir l'inactivité des comptes d'entreprises et mettre en place des procédures précises pour la gestion de ces comptes.

[xii] Les régulateurs protègent les informations des clients au moyen des lois relatives au respect de la vie privée. Celles-ci font de l'accès non autorisé à des informations un délit punissable par la loi. L'accès aux données personnelles des clients par des employés peut être motivé par l'appât du gain alors même s'il est passible de sanctions pénales.

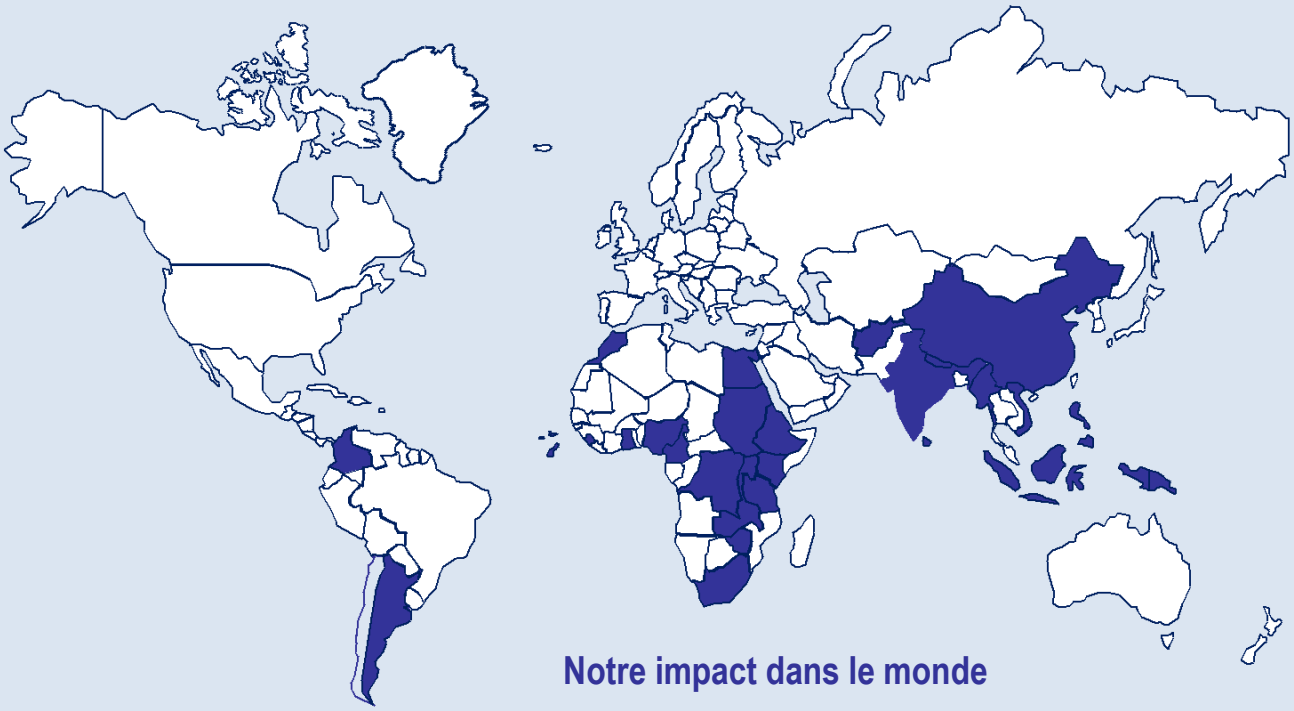
[xiii] *MTN Moves To Prevent Sim Card Swap Fraud* cet échange de carte SIM s'était produit par erreur, mais il a entraîné une perte financière pour un organisme caritatif d'Afrique du Sud.

[xiv] http ://www.itwebafrica.com/telecommunications/ Dans cet article paru le 11 septembre 2012, le directeur général de Safaricom reconnaît avoir licencié 16 salariés qui s'étaient rendus coupables de corruption. La corruption a tendance à se répandre lorsque les services financiers mobiles sont considérés comme une activité lucrative avec peu de barrières à l'entrée pour les investisseurs potentiels.

[xv] Certaines plateformes de paiements mobiles sont très flexibles, ce qui permet aux prestataire de services financiers mobiles de définir les structures de gestion du risque sur la plateforme en fonction des besoins. Cela peut s'avérer contre-productif, car l'opérateur peut volontairement mettre en place des processus peu robustes qui entraîneront des fraudes. En cas de fraude, c'est son image de marque qui sera également ternie. Il est important que les fournisseurs de plateforme prévoient une structure minimale de gestion des risques pour aider les opérateurs. Par exemple, toutes les plateformes devraient avoir un processus de double contrôle (initiateur/vérificateur) pour toute opération réalisée en ligne.

[xvi] http ://finance.yahoo.com/blogs/the-exchange/cracking-pin-code-easy-1-2-3-4-130143629.html. Dans cet article de blog, Nick Berry, fondateur de Data Genetics, une société de conseil en technologie de Seattle, explique que beaucoup de personnes utilisent des combinaison très simples de chiffres et de lettres pour leurs mots de passe et codes confidentiels, comme par exemple leur année de naissance, 1234, 1111 ou des répétitions comme 1313. Ce constat montre qu'il existe une forte probabilité que des fraudeurs puissent facilement deviner des codes confidentiels.

[xvii] Il est très difficile pour les opérateurs et leurs partenaires commerciaux de reconnaître publiquement des cas de fraude dans la gestion des mots de passe dans un cadre financier quelconque. Cela reviendrait à reconnaître que leurs processus ne sont pas suffisamment robustes.



Notre impact dans le monde

Bureaux de *MicroSave Consulting (MSC)* dans le monde

INDE
Siège : Lucknow
Tél. : +91-522-2335734
Fax : +91-522-4063773
Bureau de New Delhi :
Tél. : +91-011-45108373
Bureau de Hyderabad :
Tél. : +91- 40-23386140
info@*MicroSave*.net

ARGENTINE
Saavedra 1086 Apt C.
Ciudad Autónoma de
Buenos Aires, (1229)
Argentine
Tél. : +54-9-11-6965-778

INDONÉSIE
Jl. Penjernihan I No. 10,
Komplek Keuangan -
Pejompongan,
Jakarta Pusat 10210,
Indonésie
Tél. : +62 82122 565594

KENYA
Shelter Afrique House,
Mamlaka Road,
P.O. Box 76436, Yaya 00508,
Nairobi, Kenya
Tél. : +254-20-2724801/ 2724806
Fax : +254-20-2720133
Mobile : +254-0733-713380

PAPOUASIE-NOUVELLE-GUINÉE
First Floor,
Town Post Office,
Port Moresby
Papouasie-Nouvelle-Guinée
Tél. : +675-3434789

PHILIPPINES
Unit 402, Manila Luxury
Condominiums,
Pearl Drive corner Gold Loop,
Ortigas Center, Pasig City,
Metro Manila, Philippines
Tél. : +(632) 477-5740
Mobile : +63-917-597-7789

OUGANDA
Regency Apartments
30 Lugogo By-Pass
P.O. Box 25803
Kampala, Ouganda
Tél. : +256 312 260 225
Mobile : +256 776 36 5536

MicroSave
Market-led solutions for financial services