Mobile Money
for the Unbanked

La prévention du risque de fraude dans l'argent mobile

Auteurs: Lara Gilman et Michael Joyce

Synthèse

La gestion des risques constitue un aspect essentiel de la réussite commerciale de toute entreprise. Une gestion efficace des risques est à la base de toute croissance commerciale durable, car elle protège deux atouts commerciaux essentiels : l'image de marque et le chiffre d'affaires.

Les opérateurs mobiles ont l'habitude de gérer les risques liés à leur activité GSM, et ceux qui ont lancé des services d'argent mobile sont conscients du fait que l'argent mobile comporte des risques spécifiques, dont notamment le risque de fraude. Cet article présente un cadre d'analyse pour la gestion des risques et de la fraude. Ce cadre d'analyse comporte quatre volets : (a) détermination du niveau de tolérance du risque ; (b) identification et évaluation des risques; (c) mise en place des mesures nécessaires à la réduction du niveau de risque; et (d) suivi et revue de la stratégie de gestion des risques.

Dans le cadre de ses recherches, le programme MMU a pu constater que les opérateurs sont conscients de la nécessité de mettre en place une solide stratégie de gestion des risques pour l'argent mobile. Cet article met en avant certaines pratiques efficaces utilisées par les opérateurs pour la gestion des risques et de la fraude afin d'aider les fournisseurs d'argent mobile dans la poursuite de l'examen et de l'amélioration de leurs stratégies de gestion des risques.

Introduction

La gestion des risques liés à l'argent mobile est une tâche complexe, notamment en ce qui concerne le risque de fraude. La fraude entraîne non seulement une perte financière pour les clients ou le fournisseur d'argent mobile, mais elle porte également atteinte à la réputation du service dans l'esprit des clients et met en danger la réputation du secteur dans son ensemble. Par conséquent, la prévention du risque de fraude constitue le principal objectif d'une solide stratégie de gestion des risques.

Dans la pratique, les opérateurs de réseau mobile, les banques et autres intervenants reconnaissent que la gestion des risques constitue un aspect essentiel de la réussite commerciale durable des services d'argent mobile. Comme expliqué dans d'autres publications du programme MMU, l'argent mobile est tout sauf un service à valeur ajoutée facile et rapide à mettre en place. Les opérateurs armés d'une bonne stratégie de gestion des risques ont conscience de la complexité intrinsèque de l'argent mobile et ont mis en place des ressources dédiées pour la gestion de la fraude et les activités de protection de leurs revenus.

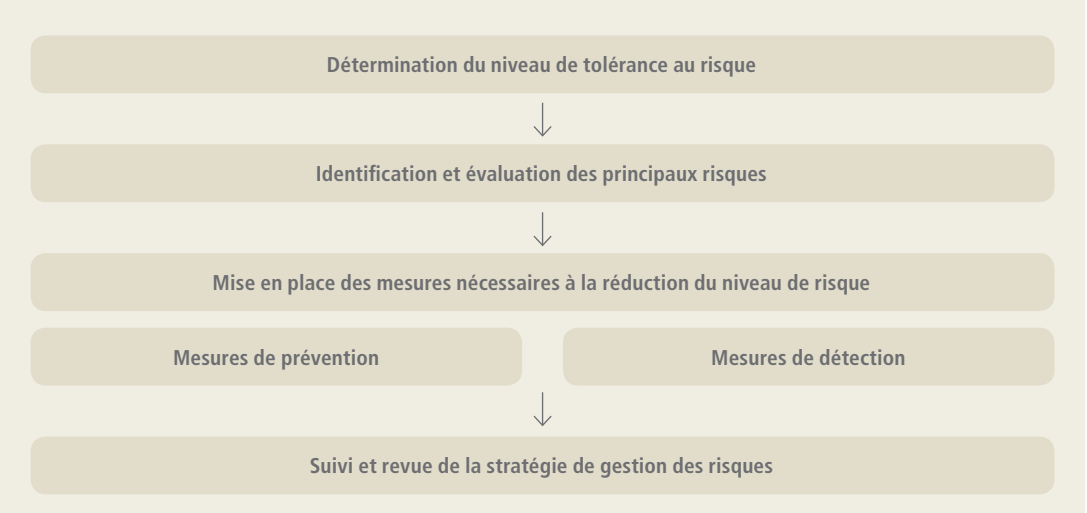
Toutefois, les stratégies de gestion des risques varient d'un opérateur à l'autre. Ces stratégies sont influencées par de nombreux facteurs, dont notamment le stade de développement du service, la structure organisationnelle, le nombre de fonctionnalités offertes, l'environnement réglementaire et le contexte local.

Même si les modes de lutte contre la fraude peuvent varier, il existe un cadre commun largement accepté comme constituant la base de toute stratégie de gestion des risques liés à l'argent mobile. Ce cadre se compose de quatre volets utilisés par les services d'argent mobile pour la gestion des risques : la détermination du niveau de tolérance du risque, l'identification des risques, la mise en place des mesures nécessaires à la réduction du niveau de risque et le suivi de leur efficacité. Le diagramme ci-dessous offre une représentation visuelle de ce cadre et constitue un guide des questions évoquées dans cet article.

Ce cadre de gestion des risques est proche des normes ISO 31000:2009[1] ou SOX[2] , qui constituent des références mondiales en matière de gestion des risques. En tant que tel, il pourrait s'appliquer à de nombreux secteurs d'activité, mais notre propos est son utilisation dans l'argent mobile afin de mettre en évidence les méthodes de prévention des risques utilisées par les opérateurs pour la gestion du risque de fraude lié à l'argent mobile. Les autres risques relatifs à la conformité réglementaire, à la continuité de l'exploitation, à la santé et à la sécurité et au vol physique sortent du cadre de cet article et n'y sont pas évoqués de manière spécifique.

La détermination du niveau de tolérance au risque : la base d'une bonne gestion des risques

Pour une gestion efficace de leur risque de fraude, les fournisseurs d'argent mobile doivent d'abord comprendre quel est leur niveau de tolérance de ce risque, ce qui est une manière d'exprimer les coûts qu'ils seraient prêts à assumer. Chaque risque a un



1 La norme ISO 31000:2009 (Gestion du risque – principes et lignes directrices) a été consultée pour préparation de cet article, mais le cadre d'analyse présenté ici diffère par plusieurs aspects. Les gestionnaires du risque chargés du développement de la documentation et des cadres d'analyse du risque pour leurs organisations doivent également tenir compte des éventuelles exigences réglementaires locales ainsi que des normes internationales comme par exemple ISO 31000.

2 Sarbanes-Oxley Act de 2002, une loi américaine sur la responsabilité financière.

coût, et chaque mesure de réduction du risque en a un aussi. Un service d'argent mobile averse au risque peut souhaiter éviter le risque en acceptant en contrepartie une croissance plus lente ou des coûts d'exploitation plus élevés. Inversement, un opérateur plus axé sur l'innovation et une croissance rapide peut être prêt à accepter un niveau de risque plus élevé. Le plus important est que les responsables de l'argent mobile et les personnes en charges du développement commercial soient informés des niveaux de risque acceptables lorsqu'ils mettent au point des stratégies commerciales ou étudient de nouvelles offres de services.

De la même manière que le niveau de tolérance du risque peut varier selon les services d'argent mobile, la méthodologie utilisée pour déterminer ce niveau de tolérance peut elle aussi varier. Certains opérateurs s'efforceront d'établir une mesure quantitative de leur niveau de tolérance (sous forme par exemple d'un pourcentage maximum de transactions frauduleuses ou faisant l'objet de réclamation), tandis que d'autres utiliseront une échelle qualitative, en définissant par exemple leur niveau de tolérance comme averse, minimal, prudent, ouvert, ou élevé.[3]

Un certain nombre d'intervenants sont susceptibles d'apporter leur soutien au processus de détermination du niveau de risque jugé acceptable. Nous avons vu certains opérateurs s'appuyer sur leur partenaire bancaire pour obtenir les conseils nécessaires à la définition de leur niveau de risque acceptable. D'autres utilisent le soutien disponible au niveau groupe tandis que certains opérateurs définissent leur niveau de tolérance par le biais de l'équipe de prévention des fraudes et de protection des revenus en charge de l'activité GSM de l'entreprise. Bien que cette étape du processus puisse s'avérer quelque peu conceptuelle, elle reste néanmoins importante pour pouvoir mettre en place des mesures de réduction du risque qui soient efficaces et appropriées.

Identification et évaluation des principaux risques : cerner le potentiel de fraude

Groupe Orange : les premiers pas de la gestion du risque lié à l'argent mobile

Préalablement au lancement d'Orange Money, le groupe Orange était conscient qu'il lui faudrait regarder ce nouveau service avec un œil neuf. Tandis que les équipes commerciales et marketing évaluaient les bénéfices potentiels directs et indirects du lancement de l'argent mobile, l'équipe centrale de lutte contre la fraude et de protection des revenus s'efforçait d'identifier et d'évaluer les risques liés à ce nouveau service complexe. Pour Orange, le principal objectif était de protéger les clients d'Orange Money contre la fraude, tout en veillant à ce que le service reste accessible et facile d'utilisation. Orange savait qu'une solide stratégie de gestion du risque était fondamentale pour établir une relation de confiance avec les clients.

La première démarche de l'équipe en vue de comprendre comment gérer les risques inhérents à l'argent mobile a été d'analyser la vulnérabilité du service. En complément de sa propre expérience issue de l'activité GSM, l'équipe de lutte contre la fraude a recherché le soutien de spécialistes extérieurs et de secteurs comparables, comme par exemple d'autres services financiers ou de paiement. Une fois établie la liste des fraudes potentielles, Orange était mieux armé pour mettre au point les seuils d'alerte et les processus visant à réduire les risques liés à l'argent mobile.

L'avantage de définir une stratégie en partant de zéro est que cela permet à l'opérateur de l'adapter aux besoins du service. L'argent mobile est complexe par nature, et nécessite des mesures et procédures de gestion des risques qui vont bien au-delà de ce qui existe dans l'activité GSM. Pour tout nouveau service, la perspective de devoir mettre au point une nouvelle stratégie en partant de zéro peut sembler chronophage, mais elle est indispensable. La première étape du développement de cette stratégie consiste à identifier et à analyser les sources de vulnérabilité du service.

Pour pouvoir mettre en place une stratégie de gestion des risques efficace, les opérateurs doivent identifier les sources de vulnérabilité dans le fonctionnement du service. Le processus d'identification est souvent effectué par les équipes en charge de la gestion des risques de l'entreprise dans son ensemble, comme par exemple l'équipe du contrôle de gestion. Nous avons ainsi vu quelques opérateurs de réseau mobile mettre en place un processus d'examen de tout nouveau produit de leur service d'argent mobile. Dans le cadre de cet examen, chaque nouveau produit ou mode de tarification doit être examiné par l'ensemble des services concernés de l'entreprise, dont notamment les ventes, le marketing, la distribution, les finances, la sécurité et le contrôle de gestion. L'équipe chargée de la sécurité et du contrôle de gestion identifie et évalue la probabilité des risques et en mesure l'impact. Bien qu'il ne s'agisse pas du seul modèle existant dans le secteur, il est important de noter que la responsabilité de l'identification des risques est clairement assignée à une équipe spécifique.

Quels sont donc les principaux risques de fraude dans l'argent mobile ?

Il existe des risques communs à l'ensemble des services d'argent mobile dans le monde, comme par exemple le risque de vol des informations relatives aux clients ou la manipulation des rapprochements comptables de l'argent électronique. Toutefois, sachant que les occurrences de fraude varient d'un opérateur à l'autre, il est plus approprié d'aborder l'identification des risques en fonction de l'environnement dans lequel s'effectuent les opérations. En d'autres termes, à quels moments dans le processus de l'argent mobile les acteurs ou participants sont-ils à risque ou en mesure de frauder ? Les principaux acteurs à considérer sont le client (risque transactionnel), l'agent (risque de distribution) et le collaborateur de l'entreprise (risque interne).

3 "Thinking about risk: managing your risk appetite: a practitioner's guide." HM Treasury, novembre 2006.

Les fraudes potentielles dans l'argent mobile		
Fraudes liées aux transactions	Fraudes liées à la distribution	Fraudes internes
■ **« Vishing/smishing »** termes anglais dérivés de « phishing » (fraude par « hameçonnage ») et désignant l'utilisation d'appels téléphoniques (« phishing » vocal) ou de SMS (« phishing » via SMS) trompeurs afin d'obtenir des renseignements personnels de la part de la victime, comme par exemple son numéro de compte, son code confidentiel ou d'autres informations concernant son identité. ■ **Fraude par avance de fonds :** les clients sont incités à envoyer de l'argent sous un faux prétexte ou en contrepartie d'une fausse promesse. ■ **Paies frauduleuses :** encaissement de sommes par des employés fictifs ou « fantômes ». ■ **Demandes d'annulation :** le client demande le remboursement d'opérations après avoir bénéficié de celles-ci. ■ **Fausses opérations :** envoi de SMS de confirmation d'opérations pour faire croire au client que celles-ci ont été effectuées. Souvent accompagnées de demandes d'annulation.	■ **Fractionnement des opérations :** les agents fractionnent les opérations de dépôt d'argent mobile afin d'accroître leurs commissions (ne s'applique qu'à une tarification dégressive en fonction du montant). ■ **Fausses opérations :** les agents transfèrent des sommes appartenant aux clients vers leur propre compte. ■ **Faux comptes :** ouverture de multiples comptes pour un seul client, ou de comptes au nom de clients fictifs pour percevoir les commissions d'enregistrement.	■ **Fraude interne :** connivence entre employés en vue d'un gain financier personnel injustifié. ■ **Vol d'identité :** accès aux renseignements personnels des clients et exploitation de ceux-ci par des salariés sans autorisation de l'entreprise.

En examinant chaque intervenant, les opérateurs peuvent identifier et évaluer les sources de vulnérabilité dans le système. Par exemple, les clients sont souvent victimes de fraude parce qu'ils ne protègent pas suffisamment leur code confidentiel. Au sein du circuit de distribution, les agents peuvent profiter du système en fractionnant certaines opérations pour encaisser des commissions indues. Bien que cela ne puisse pas être qualifié de fraude au sens juridique du terme, les opérateurs traitent souvent ce comportement comme une fraude, car il a le même effet sur les revenus de l'entreprise. Le risque interne, à savoir celui qu'un employé escroque la société, est important à cerner, car ses répercussions en termes financiers et d'image de marque peuvent être énormes même si la probabilité est faible. Les services d'argent mobile dotés d'une stratégie de gestion des risques efficace ont pris soin d'examiner toutes les sources de vulnérabilité possibles, et notamment le processus de rapprochement des transactions d'argent mobile, propice à des détournements de fonds par les employés de l'entreprise. L'identification du risque de fraude en provenance de l'ensemble des parties prenantes de l'argent mobile permet à l'opérateur d'obtenir une vision complète des risques à gérer.

Une fois ces risques identifiés, ils doivent être rapprochés des niveaux de risque jugés acceptables par l'entreprise. Tous les risques excédant le niveau de tolérance de l'entreprise doivent faire l'objet d'un examen supplémentaire, et des mesures de réduction du risque doivent être mises en place pour prévenir ou ramener ces risques à un niveau jugé acceptable par l'entreprise.

Les questions à se poser lors de l'identification et de l'évaluation des risques opérationnels liés à l'argent mobile

- Quelles sont les parties les plus complexes du processus ?
- Existe-t-il des transactions de montant élevé à haut risque se produisant de façon régulière ?
- Certains mécanismes d'authentification peuvent-ils être facilement contournés ou manipulés ?
- Est-il possible de profiter du système ?
- Est-il possible de perturber le fonctionnement du système ?
- Quelles sont les formes de fraude les plus courantes dans le pays en dehors de l'argent mobile ? Quelle est leur niveau de fréquence ?
- Quel est le niveau de criminalité et le pouvoir des forces de l'ordre dans le pays ?
- Quelle est la probabilité du risque ?
- Quelles sont les conséquences potentielles pour l'entreprise ? (au plan financier et de l'image de marque)

La mise en place de mesures de réduction du risque : prévenir le risque de fraude

Une fois les principaux risques identifiés, l'étape suivante consiste pour l'opérateur à mettre en place des mesures efficaces de réduction du risque, qui peuvent être des mesures peu coûteuses ou une politique spécifique de gestion de certains risques. Des mesures efficaces sont des mesures qui permettent un développement commercial durable sans le brider.

L'utilisation de mesures de contrôle pour réduire les risques liés à l'argent mobile

Les mesures de contrôle de l'argent mobile sont soit des mesures préventives, qui visent à réduire la probabilité d'apparition des fraudes, ou des mesures de détection, qui visent à surveiller et signaler des activités frauduleuse qui se sont déjà produites. Le tableau 1 présente les principales mesures de réduction des risques concernant les plupart des services d'argent mobile.

Tableau 1 : Exemples de mesures de réduction des risques liés à l'argent mobile

Mesures préventives	Mesures de détection
■ Contrôle des droits d'accès pour protéger les informations des clients	■ Surveillance et analyse des activités suspectes
■ Séparation des tâches concernant les procédures à haut risque (par exemple : rapprochements comptables de l'argent électronique) pour éviter les erreurs ou les fraudes	■ Surveillance des activités d'accès au système
■ Limites de montant pour réduire les risques liés au blanchiment des capitaux et au financement du terrorisme (AML/CFT)	■ Mise en place de solides procédures de recours des clients et de remontée des problèmes éventuels
■ Campagnes d'information auprès de la clientèle pour éduquer et protéger les clients	■ Surveillance de l'activité transactionnelle des agents
■ Formation des agents sur les pratiques acceptables et les termes et conditions de fonctionnement du service	■ SMS d'alerte aux clients
■ Formation des employés sur les rôles et responsabilités	■ Revue des opérations de montant élevé par la hiérarchie

Les mesures préventives sont généralement jugées plus efficaces que les mesures de détection, surtout lorsqu'elles sont intégrées dès le départ aux caractéristiques techniques du système de l'argent mobile. Lorsque des mesures telles que la séparation des tâches, le contrôle des droits d'accès ou le renforcement des réseaux sont mises en place, il est important que cette mise en place soit effectuée en bonne et due forme, avec une documentation appropriée, des revues et des tests. Si des mesures sont en place, mais peuvent être facilement contournées (par exemple s'il y a séparation des tâches, mais que les utilisateurs se prêtent régulièrement leurs mots de passe pour l'éviter), le risque de fraude persiste.

La taille du service et les ressources disponibles peuvent avoir une influence sur le poids relatif des mesures de prévention ou des mesures de détection au sein d'un réseau.

Sans pour autant constituer une liste exhaustive, chacune des mesures mentionnées concerne au moins l'un des risques spécifiques liés à l'argent mobile. Ainsi, le contrôle des droits d'accès permet de réduire le risque de vol des renseignements clients, tandis que le suivi et l'analyse des opérations suspectes accroît la visibilité des activités frauduleuses.

Easypaisa de Telenor Pakistan : l'utilisation de mesures de réduction des risques pour la gestion des arbitrages par les agents

Le commissionnement dégressif par tranches de montant d'opérations permet d'offrir aux agents une meilleure rémunération sur les opérations de faible montant, qui jouent un rôle essentiel dans le développement de l'argent mobile. Easypaisa a choisi de retenir cette tarification dégressive pour profiter des avantages commerciaux qui s'y rattachent. Mais ce mode de tarification est par nature plus risqué qu'une tarification proportionnelle, car il offre aux agents la possibilité de profiter du système en fractionnant les opérations pour augmenter leurs commissions.

Plutôt que d'abandonner les avantages liés au commissionnement dégressif par paliers, Easypaisa a mis en œuvre deux mesures, l'une préventive et l'autre a posteriori, pour réduire le risque. Ces deux mesures ont d'abord nécessité une analyse de l'activité des clients. Easypaisa a ainsi fait deux découvertes utiles pour la création de systèmes de contrôle adaptés aux besoins spécifiques de son service. En premier lieu, le comportement habituel des clients consiste à déposer un minimum de 50 roupies à la fois sur leur compte Easypaisa. L'équipe a ensuite déterminé que tout compte enregistrant plus de 45 dépôts d'espèces sur une période de 15 jours (soit une moyenne de trois dépôts par jour) était anormal et souvent lié à des activités suspectes.

Cette identification d'un comportement « normal » par opposition à un comportement dit « anormal » a permis aux équipes d'Easypaisa de mettre en place des mesures de réduction du risque qui soient efficaces sans pour autant être excessives. Sachant que le montant habituel de dépôt des clients était de 50 roupies, Easypaisa a pu mettre en place un montant minimum de dépôt non dissuasif pour les clients, mais qui rend plus difficile le fractionnement des opérations par les agents. De la même manière, la compréhension des caractéristiques d'un comportement « anormal » a permis à Easypaisa de mettre en point un système de détection qui s'appuie sur la production de rapports signalant tout compte enregistrant plus de 45 dépôts d'espèces en l'espace de 15 jours chez un même agent. Grâce à ces mesures de contrôle du risque, Easypaisa a pu profiter des avantages commerciaux d'un commissionnement dégressif par paliers tout en réduisant son niveau d'exposition au risque.

Les outils nécessaires à la réduction des risques : données, communication et procédures internes bien définies

Les services d'argent mobiles disposent de trois outils pour mettre en œuvre des mesures de contrôle efficaces :

1) Des informations statistiques et des tableaux de bord fiables et pertinents ;

2) De bons outils et canaux de communication avec les différents intervenants, y compris les clients ;

3) Des procédures internes qui définissent le mode de remontée des informations et les mesures à prendre en cas de détection d'activités suspectes.

Les informations statistiques représentent un atout important pour la prévention et la surveillance de la fraude dans l'argent mobile. La surveillance des transactions constitue un aspect essentiel de toute stratégie efficace, mais il n'existe pas de tableau de bord unique valable pour tous les services d'argent mobile. Pour obtenir des informations statistiques fiables, il faut travailler avec les équipes administratives et/ou les fournisseurs de plateformes. Si l'on examine de nouveau la manière dont Easypaisa contrôle les opérations d'arbitrage par les agents, on voit qu'il leur fallait découvrir des données pertinentes dans le contexte local pour pouvoir déterminer ce qui constituait un comportement normal et un comportement anormal.

Safaricom M-PESA: l'éducation des clients ou la communication en tant que mesure préventive

L'une des principales priorités du service M-PESA de Safaricom est de réduire le risque de fraude à l'encontre de ses clients. Plutôt que de se contenter de simples mesures de détection, Safaricom s'appuie largement sur des mesures de prévention pour réduire le risque de fraude à l'encontre de ses clients. La société a constaté que la mesure de prévention la plus efficace est d'informer les clients au moyen d'une communication claire. Pour toucher les clients de M-PESA, Safaricom utilise une approche à plusieurs volets. Envois en masse de SMS, messages radio dans les dialectes locaux, sketchs locaux et publicités dans les journaux sont autant de supports utilisés dans leurs campagnes d'information des clients. L'amélioration de l'information des clients au moyen d'une communication claire a joué un rôle essentiel dans la réussite de Safaricom en matière de prévention de la fraude à l'encontre des clients de M-PESA.

La communication, interne ou externe, est le deuxième outil que les services d'argent mobile doivent utiliser pour assurer le respect des mesures de contrôle des risques. En fonction du nombre et de la complexité des mesures de réduction du risque mises en place, il peut y avoir un nombre élevé de parties prenantes au processus. En interne, les responsables de l'argent mobile, les équipes d'assistance administrative, celles du service à la clientèle et celles des finances et du contrôle de gestion font partie des intervenants habituels devant être informés et incités à signaler toute anomalie ou activité suspecte aux services concernés.

La communication externe en direction des agents et des clients est tout aussi importante pour l'efficacité des mesures de prévention. L'éducation des clients sur les manières d'éviter le risque de fraude est une mesure de prévention essentielle pour réduire la fréquence des escroqueries visant les clients, comme en témoigne le cas de M-PESA.

Enfin, lorsqu'une fraude ou des activités suspectes sont détectées, **des procédures internes doivent être en place pour garantir que ces activités suspectes soient signalées de façon appropriées aux personnes responsables**. Ces procédures internes doivent être complètes pour que cette information soit communiquée et que des mesures appropriées soient prises. Si un client appelle pour se plaindre que de l'argent a disparu de son compte, le centre de service à la clientèle doit savoir comment faire remonter cette information.

De la même manière, si la réclamation concerne un agent en particulier, il doit également y avoir un processus en place prévoyant des mesures disciplinaires à l'égard de l'agent. Dans les cas les plus graves, lorsqu'un agent accède au compte d'un client en volant son code confidentiel, certains opérateurs mobiles bloquent souvent immédiatement le compte de l'agent dans l'attente d'une enquête plus poussée. Dans le cas d'infractions mineures par les agents, les opérateurs émettent généralement un avertissement avant de prendre d'autres mesures.

Lorsque les mesures de réduction du risque ne suffisent pas : transférer, tolérer ou supprimer les risques

Lorsqu'un risque ne peut être toléré par l'opérateur, celui-ci peut décider de le transférer. L'assurance constitue une forme de transfert des risques, mais la forme de transfert la plus adaptée à l'argent mobile est l'externalisation. L'utilisation de sous-traitants (tels que des agents, des sociétés de transports de fonds des sous-traitants de traitement des opérations) permet de réduire les risques pour l'opérateur. Toutefois, de nombreuses règlementations prévoient que la banque ou l'opérateur responsable ne peuvent pas transférer certaines responsabilités.

UBL Omni: quand tolérer et quand limiter les risques

Au Pakistan, UBL souhaitait trouver des manières d'encourager ses clients utilisateurs du service d'argent mobile Omni au guichet à passer au portemonnaie électronique. Grâce à un changement de réglementation, UBL a pu permettre aux nouveaux clients Omni d'effectuer deux opérations avant vérification de leur compte, en autorisant la réalisation de certaines transactions au moyen d'une authentification par SMS. UBL a décidé d'utiliser cette nouvelle possibilité comme une manière de réduire les barrières à l'essai par les clients du portemonnaie électronique.

L'équipe de gestion des risques et de la fraude avait conscience du risque supplémentaire d'activité frauduleuse généré par le fait d'autoriser des clients à effectuer des opérations sans code confidentiel dans certaines conditions. Mais il fut décidé que l'avantage commercial était plus important que le risque, lequel a été accepté au moment du lancement en autorisant certaines opérations de plus faible montant. L'activité fut surveillée par l'équipe, et au bout d'une semaine, elle se rendit compte de l'existence de quelques réclamations en provenance de clients, qui se plaignaient que des opérations avaient été effectuées sur leur compte sans leur autorisation.

En retour, l'équipe de gestion des risques et de la fraude décida de mettre en œuvre une mesure de contrôle supplémentaire. Une semaine plus tard, les transactions autorisées étaient limitées de sorte que des codes de décaissement étaient obligatoires à la place d'un code confidentiel.

UBL était en mesure d'accepter le risque au moment du lancement parce que l'entreprise avait la capacité, grâce à sa technologie, de réagir rapidement en cas d'augmentation du risque estimé. Il est également important de noter que même si UBL a choisi de tolérer ce risque, l'activité a néanmoins été surveillée de près pour s'assurer d'avoir une connaissance immédiate de tout dérapage.

Dans d'autres cas, l'opérateur peut décider de tolérer certains risques. La bonne solution consiste parfois à accepter un risque donné si l'analyse coût/bénéfice des mesures de contrôle de ce risque montre que le coût est trop élevé et/ou l'impact commercial limité. Dans le cas d'une telle décision, il convient de surveiller ce risque de près en cas de changement du rapport coût/bénéfice dans le temps.

La suppression d'un risque est une autre possibilité lorsqu'il n'existe pas de mesure pratique et efficace de réduction de ce risque. Lorsqu'un produit ou un service particulier présente de nombreuses possibilités de pertes ou de fraude, de réclamations clients ou d'autres problèmes, la meilleure solution est parfois d'arrêter ce produit. Il peut s'avérer nécessaire de le conserver pour certains comptes tout en gérant le changement pour d'autres.

Suivi et revue de la stratégie de gestion des risques : garantir l'efficacité sur le long terme

Le suivi des mesures de contrôle et l'examen régulier des risques au fil du temps sont indispensables au maintien de l'efficacité de toute stratégie de gestion des risques attachés à l'argent mobile.

Les questions clés du suivi

- Quelles sont les nouvelles activités frauduleuses qui apparaissent ? Est-ce qu'il existe une tendance ?
- Toutes les mesures de contrôle sont-elles correctement conçues et mises en place ?
- Les employés et la hiérarchie ont-ils une bonne connaissance et une bonne compréhension de leurs rôles et de leurs responsabilités ?

Les activités de suivi nécessitent un fort soutien hiérarchique et des ressources internes suffisantes

En premier lieu, il est important que le processus de gestion des risques bénéficie d'une participation active de la direction de l'entreprise. De nombreux opérateurs d'argent mobile ont un comité spécial dédié à la gestion des risques et composé de représentants des principales directions de l'entreprise. Les membres du conseil d'administration et les partenaires bancaires peuvent également être représentés. Ce comité doit avoir un ordre du jour fixe prévoyant l'examen du profil de risque actuel et de l'efficacité des mesures de contrôle en place et la surveillance de l'apparition de tout nouveau risque. Il peut également avoir son mot à dire pour l'approbation de nouveaux produits ou services, ou le changement de produits ou services existants. Tout au long du processus de gestion des risques, il est important que la direction de l'entreprise valide l'évaluation qui est faite des risques et toute décision d'acceptation de ceux-ci.

L'une des formes de suivi les plus courantes au sein des services d'argent mobile est la réalisation d'un audit interne annuel. Il s'agit d'un examen complet, qui a pour but de vérifier que l'ensemble des processus et mesures de contrôle en place est respecté, et qui est effectué par une équipe non impliquée directement dans le service d'argent mobile. L'équipe d'audit interne est souvent rattachée à la direction du groupe ou peut faire partie de l'équipe des finances et du contrôle de gestion. Les fournisseurs d'argent mobile peuvent s'appuyer sur les mêmes équipes d'audit interne que celles qui effectuent le suivi des risques de l'activité GSM de l'entreprise. Cette dernière option peut s'avérer la plus tentante pour les opérateurs de petite taille en raison des synergies de coût. Les opérateurs utilisant cette approche doivent néanmoins s'assurer que l'audit GSM est correctement adapté à l'activité de l'argent mobile.

Au-delà de l'examen habituel d'un audit interne, nous avons observé des manières plus créatives d'aborder le processus de suivi au sein des services d'argent mobile. Au Cambodge, WING effectue ainsi un examen par des pairs de son processus de rapprochement comptable. La manipulation des rapprochements comptables constitue certainement l'un des principaux risques de l'argent mobile, et nécessite un certain nombre de mesures de contrôle préventives et de détection, comprenant une claire séparation des tâches et une bonne surveillance des accès et de l'activité. Chez WING, des cadres non directement impliqués dans le processus effectuent ce rapprochement bancaire à titre de contrôle inopiné par sondage. Ce processus présente deux avantages : tout d'abord, ces cadres se familiarisent ainsi avec les étapes nécessaires à la réalisation de ces rapprochements comptables et gagnent ainsi une meilleure compréhension des anomalies pouvant se manifester. Ensuite, le responsable hiérarchique fait office de surveillant externe, réduisant le risque de connivence entre les personnes habituellement chargées de ces rapprochements comptables.

Ces activités de suivi sont essentielles à la réussite de la gestion des risques, car à mesure que les services d'argent mobile se développent et que de nouveaux produits ou simplement des clients s'ajoutent, les mesures de contrôle des risques en place doivent également être revues pour vérifier qu'elles conservent toute leur efficacité. Tout aussi important est le fait qu'à mesure que le service évolue, le niveau de sophistication des fraudeurs évolue lui-aussi. Les opérateurs doivent veiller à maintenir des ressources suffisantes pour un examen régulier non seulement de l'efficacité des mesures de contrôle en place, mais également du marché afin de détecter les nouvelles tendances en matière d'activités frauduleuses. Ces examens réguliers associés à une participation active de la direction sont indispensables au maintien de l'efficacité à long terme de la politique de gestion des risques de l'entreprise.

La fraude et les risques sont des aspects fondamentaux de l'argent mobile qui doivent être traités par tout opérateur du secteur. Ils concernent non seulement l'opérateur, mais également les clients, les agents, et les autorités réglementaires. Nos recherches ont montré qu'il existe de nombreuses manières d'identifier, de classer, de contrôler et de suivre le risque de fraude. En veillant à ce que le risque de fraude soit géré conformément au présent cadre d'analyse, les opérateurs peuvent se protéger, et protéger également leurs clients et leurs agents, tout en assurant la réussite de leur activité d'argent mobile.

Le programme MMU bénéficie du soutien de la Fondation Bill & Melinda Gates,
de la Fondation MasterCard et d'Omidyar Network

Pour plus d'informations, veuillez contacter
mmu@gsm.org
GSMA London Office
T +44 (0) 20 7356 0600
http://www.gsma.com/mmu