Mobile Money for the Unbanked

L'argent mobile au service des personnes non bancarisées

Juin 2009

Les auteurs
Marina Solin
Andrew Zerzan

L'Association GSM (GSMA) représente les intérêts de l'industrie mondiale de la téléphonie mobile. Couvrant 219 pays, GSMA rassemble presque 800 opérateurs mobiles du monde entier ainsi que plus de 200 entreprises appartenant plus généralement au secteur de la téléphonie mobile. Pour plus d'information, nous vous invitons à visiter www.gsmworld.com. GSMA produit et organise également des évènements de premier rang, comme par exemple le MobileWorld Congress de Barcelone et le Mobile Asia Congress. Pour en savoir plus sur ces deux congrès, vous pouvez consulter les sites internet www.mobileworldcongress.com et www.mobileasiacongress.com.

Nous formulons nos remerciements à Thaer Sabri thaer@flawlessmoney.com de Flawless Money pour avoir contribué à ce document (www.flawlessmoney.com).

Table des Matières

Présentation générale

Les services d'argent mobile sont actuellement en cours de déploiement au sein de nombreux marchés dans le monde. Des preuves tangibles indiquent que ces services améliorent l'accès aux services financiers formels dans les pays en voie de développement.

Le développement de ces services suscite néanmoins la crainte qu'ils puissent être utilisés à des fins de blanchiment de capitaux et de financement du terrorisme (BC/FT). Bien qu'il n'y ait eu jusqu'à présent aucune preuve de BC/FT, les systèmes d'argent mobile restent susceptibles d'être utilisés à ces fins dans le futur (de la même manière d'autres services financiers formels sont actuellement visés).

Nous pensons qu'il est opportun de discuter aujourd'hui de comment évaluer ces risques et de les réduire de manière efficace. Les opérateurs mobiles offrant ces nouveaux services ne possèdent pas forcément une bonne connaissance des risques de blanchiment d'argent et de financement du terrorisme. Les autorités réglementaires concernées (comme les Banques Centrales et les entités de renseignement financier) ne sont généralement pas familiarisés avec les services d'argent mobile et des risques de blanchiment de capitaux (BC) et de financement du terrorisme (FT) posés par ceux-ci.

L'objectif de ce document de travail est de présenter une méthodologie d'évaluation des risques reposant sur le cadre général des recommandations du Groupe d'Action Financière (GAFI).[1] Cette méthodologie à pour vocation d'apporter à l'industrie, ainsi qu'aux autorités réglementaires, des méthodes souples et cohérentes d'évaluation et de réduction des risques de BC/FT en matière de services d'argent mobile.

La méthodologie d'évaluation des risques présentée dans ce document de travail a été développée sur la base des hypothèses suivantes:

- La réglementation doit être basée sur les risques et rester neutre vis-à-vis de la technologie : « À risque identique, réglementation identique » pour tous les intervenants (banques, opérateurs mobiles et autres prestataires de paiements). Bien qu'il soit question de services d'argent mobile dans ce document, nous pensons que cette même méthodologie doit pouvoir être appliquée à d'autres services ou acteurs.
- Pour toute évaluation et mesure de réduction des risques, il est essentiel de permettre à « l'effet domino » caractéristique des services d'argent mobile d'améliorer le niveau d'inclusion financière. Le développement du secteur financier formel et la réduction de l'économie informelle contribuent directement à la réduction des risques de BC/FT.
- Le caractère traçable et numérique de l'argent mobile minimise les risques de BC/FT par rapport à l'argent liquide.
- L'inclusion financière et LAB/CFT sont complémentaires et se renforcent mutuellement.
- Les services d'argent mobile doivent constituer une activité réglementée placée sous la supervision du régulateur financier ou d'une autre autorité de surveillance financière.
- Une réglementation adaptée en matière de LAB/CFT doit provenir d'une collaboration étroite entre l'industrie et le régulateur financier. Bien qu'utilisant le cadre général fourni par le GAFI, les mesures adaptées de LAB/CFT doivent résulter d'une collaboration basée sur l'expérience.

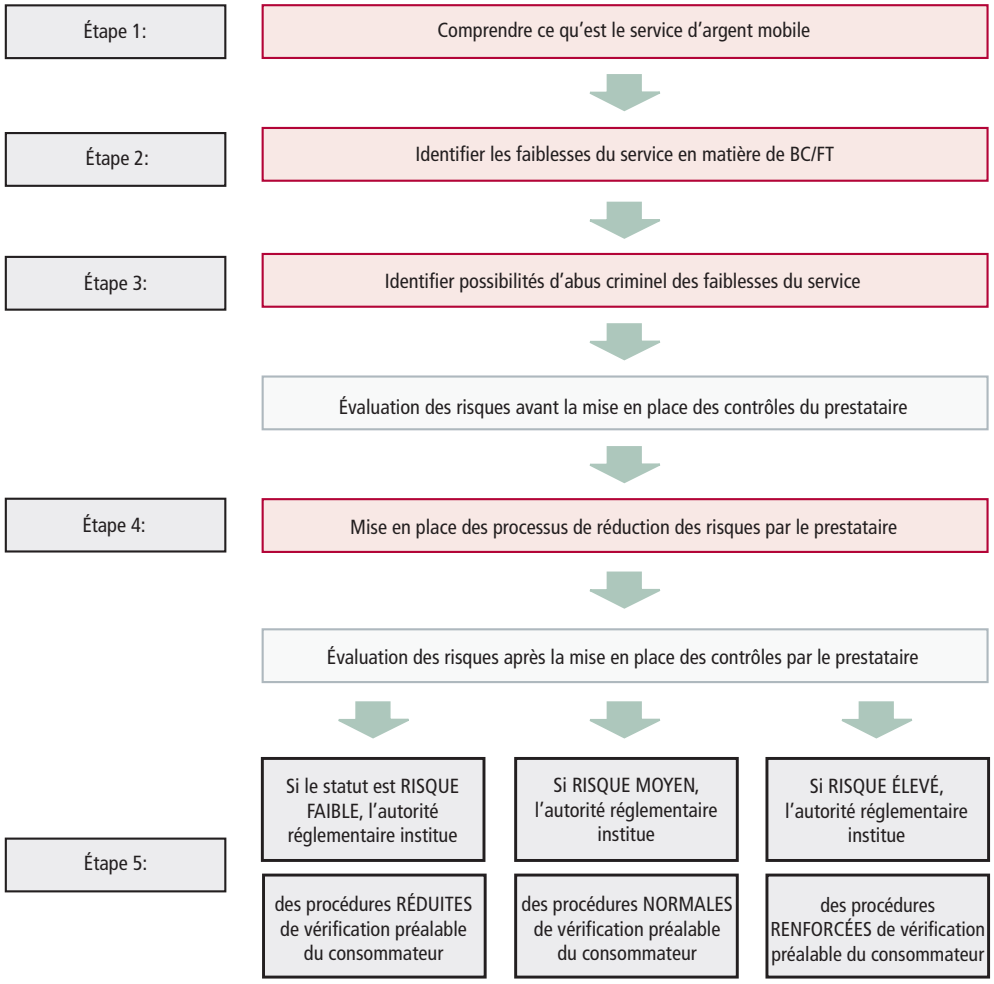
La méthodologie présentée comporte 5 étapes. Nous estimons que cette approche permet, aux opérateurs mobiles et aux régulateurs financiers en charge de LAB/CFT d'assurer une prévention efficace et adaptée du blanchiment des capitaux et du financement du terrorisme.
La première étape consiste à comprendre les services fournis, leur usage et leur environnement. La deuxième étape consiste à analyser les points faibles de ces services en matière de BC/FT. La troisième étape permet ensuite aux opérateurs et aux autorités réglementaires de mieux comprendre comment les criminels et les terroristes sont susceptibles de tirer parti de ceux-ci. Ce processus permet de définir le profil de risque de départ avant la mise en place de systèmes de contrôle.

[1] Par exemple, la recommandation 5 du GAFI concernant les procédures de vérification préalable concernant le client préconise d'effectuer des actions de contrôle en fonction du niveau de risque : contrôles accrus pour les risques élevés, contrôles réduits pour risques moindres. Ce document explique comment appliquer cette recommandation aux services d'argent mobile.

L'étape 4 correspond à l'introduction de mesures de contrôle basées sur les systèmes. Il est alors possible d'évaluer le risque total du service et d'identifier les mesures supplémentaires (Connaissance du client ou *Know Your Customer* - KYC) nécessitées par la réglementation.

L'objectif de notre démarche est d'encourager l'utilisation de l'éventail complet des outils de réduction des risques tout en considérant les risques de BC/FT sous-jacents.

Schéma général de la méthodologie d'évaluation des risques



Il existe beaucoup d'avantages à faciliter l'usage des services d'argent mobile pour les clients les plus pauvres dans les pays en développement, tout en prévenant en même temps les risques de BC/FT. Bien que nous ne suggérions pas un modèle de solution unique, nous espérons que ce document de travail fournira un cadre méthodologique utile tant pour le régulateur que pour les prestataires de services.

1.Introduction

Les services d'argent mobile (voir définition en annexe 1) sont actuellement en cours de déploiement au sein de nombreux marchés dans le monde entier. Des preuves tangibles indiquent que ces services améliorent l'accès aux services financiers formels dans les pays en développement.

Son potentiel d'amélioration de l'accès aux services financiers, a amené la Fondation Bill & Melinda Gates à financer le programme *Mobile Money for the Unbanked* (l'argent mobile au service des personnes non bancarisées) du GSMA. Le projet a pour objectif de fournir d'ici 2011 un accès financier par téléphone mobile à 20 millions de personnes non bancarisées vivant avec moins de 2 dollars par jour. Dans de nombreux pays en développement, les opérateurs mobiles ont mieux réussi à atteindre les consommateurs non bancarisés que les banques. Les services d'argent mobile fournissent une occasion unique de faire passer les clients disposant d'un téléphone mobile mais pas d'un compte bancaire, d'un système de paiement en argent liquide à un système financier formel qui leur donne accès à une variété de services financiers,

Des études conduites dans plusieurs pays, notamment au Brésil, en Afrique du Sud, au Kenya, en Malaisie et aux Philippines [2] indiquent que le coût réduit des services d'argent mobile constitue l'un des facteurs déterminants de leur adoption. La vitesse d'exécution, leur facilité d'utilisation, ainsi que le sentiment de sécurité du client pour son argent et pour les transactions qu'il effectue, sont également des facteurs importants,

Le niveau élevé d'utilisation du service dans les pays offrant un produit facile d'utilisation, comme au Kenya et aux Philippines, témoigne de l'existence d'un besoin pour de tels services. En outre, on constate un fort taux de pénétration parmi les consommateurs non bancarisés (en moyenne, un tiers des utilisateurs d'argent mobile sont non bancarisés). Ces services sont typiquement utilisés pour effectuer des transactions de faible montant et sont déployés en milieu urbain et rural. Ce document examine les risques de blanchiment de capitaux (BC) et de financement du terrorisme (FT) liés aux services d'argent mobile dans les pays en voie de développement.[3]

L'objectif de ce document de travail est de présenter une méthodologie d'évaluation des risques reposant sur le cadre général des recommandations du Groupe d'Action Financière (GAFI).[4] Notre méthodologie a pour vocation d'apporter à l'industrie ainsi qu'au régulateur des méthodes souples et consistantes d'évaluation et de réduction des risques de BC/FT pour les services d'argent mobile. L'adoption d'une telle méthodologie permet de produire une analyse des risques proportionnée et cohérente produisant des résultats identiques pour des risques identiques, quelle que soit la situation à laquelle elle est appliquée.

Ce document de travail a été rédigé en réponse à de nombreuses questions récurrentes portant sur les risques de BC/FT en matière de services d'argent mobile. Certaines de ces questions sont traitées dans le cadre de la méthodologie d'évaluation des risques; d'autres sont récapitulées dans l'annexe 2 « Questions/réponses ». Nous espérons que ce document ainsi que la méthodologie présentée s'intègreront aux débats en cours quant aux meilleures solutions de gestion des risques de BC/FT en matière de services d'argent mobile.

[2] Informations fournies par la Banque Mondiale dans *Mobile Phone Financial Services* (2008), page 8, encadré 1 et les études à venir. Voir également la présentation de Caroline Pulver (2009): *The Performance and Impact of M-PESA: Preliminary Evidence from a Household Survey* (Performance et impact de M-PESA : résultats préliminaires d'une étude des ménages), diapositif 9.

[3] Les pays développés présentent également une population non bancarisée. On estime par exemple qu'il existe entre 3 à 8 millions d'adultes exclus des services financiers au Royaume-Uni. Bien que les avantages d'une approche réglementaire adaptée en matière de risques BC/FT soient plus importants pour les pays en voie de développement, la méthodologie présentée dans ce document peut également s'appliquer aux pays développés.

[4] Par exemple, la recommandation 5 du GAFI concernant les procédures de vérification préalable concernant la clientèle. Cette recommandation préconise d'effectuer des actions de contrôle en fonction du niveau de risque : contrôles accrus pour les risques élevés, contrôles réduits pour risques moindres. Le présent document décrit comment appliquer cette recommandation aux services d'argent mobile.

1.1 L'argent mobile dans le cadre de LAB/CFT

Certaines tendances générales se dégagent au sein du secteur de l'argent mobile (et plus généralement du secteur des nouvelles technologies de paiement). Parce qu'il est important de tenir compte de ces tendances lors de l'élaboration des réglementations de LAB/CFT, nous avons tiré de chaque tendance un principe réglementaire qui permette d'aider le régulateur à forger une réglementation efficace en matière de LAB/CFT.

- *Tendance : De nouveaux types de prestataires de service apparaissent afin de répondre aux besoins des consommateurs. Ce changement technologique intervient rapidement alors que la réglementation peine à s'adapter.*

Alors qu'une ère d'innovation s'ouvre ; où les banques et une multitudes d'autres institutions non bancaires offrent de nouveaux services de paiement, la réglementation devrait s'adapter aux différents types de services et non de prestataires. De même, en matière de criminalité financière, les règles de LAB/CFT doivent être les mêmes pour toutes les organisations offrant le même service, variant uniquement en fonction du niveau de risque : « À risque identique, réglementation identique ». La méthodologie d'évaluation des risques présentée dans ce document doit donc s'appliquer à toutes les entités (banques, opérateurs mobiles ou autres prestataires) offrant des services d'argent mobile (ainsi que pour tout autre service de paiement).

L'innovation technologique arrivant rapidement, la réglementation se doit de rester appropriée malgré ces changements. Pour que la réglementation reste efficace dans le futur, elle doit être conçue de façon à prendre en compte différents risques (technologiques, systémiques et opérationnels), sans se limiter à certaines technologies. Si la réglementation porte sur les risques effectifs posés par un service spécifique, elle a plus de chances de rester applicable même en cas de changement de prestataire ou de technologie. L'identification et la réduction des risques liés à un service donné doivent être au centre des activités de LAB/CFT.

Principe : La réglementation doit être définie en fonction du niveau de risque et doit être indépendante de la technologie: « À risque identique, réglementation identique », pour tous.

- *Tendance : les services d'argent mobile possèdent un « effet domino » caractéristique faisant passer les personnes non bancarisées dans le système financier formel.*

La recherche montre [5] que les services d'argent mobile permettent de faire passer la clientèle d'une économie basée sur l'argent liquide au secteur financier formel. Lorsque la confiance est établie, les clients autrefois non bancarisés sont enclins à contracter des services financiers traditionnels, tels que des comptes d'épargne (par exemple, les clients précédemment non bancarisés formulent une demande de compte d'épargne après être devenus des utilisateurs habiles de services d'argent mobile, Les banques peuvent ensuite prendre le relai et prendre en charge ces nouveaux clients). L'argent mobile a donc une fonction importante d'introduction des clients non bancarisés au système financier formel. À grande échelle, cela se traduira par une formalisation du système financier et une diminution globale du risque de BC/FT.

Principe : Lors de l'évaluation des risques et de la meilleure manière de les réduire, il est essentiel de laisser ce fameux « effet domino » agir comme multiplicateur et augmenter ainsi le niveau d'inclusion financière. Le développement du système financier formel et la réduction de l'économie informelle contribuent directement à la réduction des risques de BC/FT.[6]

[5] '*Understanding the Unbanked Customer and Sizing the Mobile Money Opportunity*' (Comprendre la clientèle non-bancarisée et saisir la chance de l'argent mobile) par Paul Leishman (2009) dans le rapport annuel 2009 de *Mobile Money for the Unbanked.*
[6] Discours de Paul Vlaanderen, président du GAFI, lors de la 9ème réunion du conseil des ministres ESAAMLG à Maseru (Lesotho) le 21août 2009

- *Tendance : l'argent mobile a une meilleure traçabilité que l'argent liquide.*

Les risques de BC/FT en matière d'argent mobile sont généralement comparés aux risques liés aux services bancaires traditionnels. Cependant, l'argent mobile intéresse surtout une clientèle évoluant au sein d'une économie basée sur l'argent en liquide. Par conséquent, les risques de BC/FT liés aux services d'argent mobile doivent également être comparés aux risques de BC/FT liés à l'économie basée sur l'argent en liquide. Les services d'argent mobile viennent remplacer au fil du temps les paiements en espèces, leur apportant visibilité et traçabilité. Ils doivent donc être considérés comme un service ayant le potentiel de réduire les risques par comparaison aux paiements en liquide. Ils constituent une étape intermédiaire vers des comptes bancaires classiques et devraient être encouragés par les autorités réglementaires.

Principe : la nature numérique et la traçabilité de l'argent mobile réduisent les risques de BC/FT par rapport à l'utilisation d'argent liquide.

- *Tendance : l'inclusion financière et par conséquent le développement du système financier formel ont été reconnus comme des outils essentiels en matière de LAB/CFT.*

Les services d'argent mobile dans les pays en développement favorisent l'accès aux services financiers. L'accès aux services financiers et la prévention du BC/FT « sont complémentaires: ils ne constituent en aucune manière des objectifs politiques contradictoires pour le secteur financier. Sans un degré d'inclusion financière suffisamment important, le système LAB/CFT d'un pays donné ne protège l'intégrité que d'une portion de son système financier – celle ayant été déclarée comme formelle - , laissant la partie informelle et non déclarée vulnérable aux abus. Les mesures permettant à un plus grand nombre de clients de faire usage de services financiers formels étendent par conséquent la portion légitime du secteur financier. »[7]

Principe : inclusion financière et LAB/CFT sont complémentaire et se renforcent mutuellement.

- *Tendance : il est de plus en plus reconnu que les services d'argent mobile doivent être réglementés et supervisés par le régulateur financiers de chaque marché.*

Les prestataires doivent être réglementés sur la base des services qu'ils fournissent, conformément à la définition fonctionnelle d'une « institution financière » par le GAFI. Il existe déjà un large éventail d'outils réglementaires concernant les services d'argent mobile. À une extrémité se trouvent les réglementations bancaires traditionnelles, au titre desquelles les opérateurs doivent s'associer avec des banques pour pouvoir offrir des services d'argent mobile. Au sein de ce partenariat, la banque a la responsabilité des activités réglementées de LAB/CFT. À l'autre extrémité de cet éventail réglementaire, les opérateurs mobiles de certains pays ont également la possibilité de postuler auprès des autorités réglementaires pour une licence de paiement ou d'argent électronique, se transformant ainsi en prestataires de services réglementés devant se conformer par eux-mêmes aux obligations de LAB/CFT. Ceci démontre que les services d'argent mobile font partie intégrante du système financier formel et doivent systématiquement se conformer aux obligations de LAB/CFT. Tant que le service lui-même est de nature financière, il est de plus en plus reconnu que celui-ci soit réglementé par les autorités financières, quelle que soit la nature du prestataire.

Principe : les services d'argent mobile decraient être une activité réglementée placée sous la tutelle de régulateur financier ou de toute autre autorité financière compétente.

[7] Discours de Paul Vlaanderen, président du GAFI, lors de la 9ème réunion du conseil des ministres ESAAMLG à Maseru (Lesotho) le 21 août 2009, citant Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, et R. Walker. 2008 dans *Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines.* (La mise en œuvre des normes du GAFI dans les pays en voie de développement et l'inclusion financière : conclusions et recommandations) Initiative FIRST Initiative. Washington, D.C.: Banque Mondiale page vi

- *Tendance : Jusqu'à présent seulement très peu de cas d'activité criminelle par le biais des services d'argent mobile ont été prouvés.*

Empiriquement, il n'y a eu que très peu de cas de blanchiment d'argent[9] par l'intermédiaire des services d'argent mobile dans les pays où ces services ont connu une croissance importante. Qui plus est, il n'y a eu aucun signalement de financement terroriste[10]. Bien que tout système de paiement soit voué à faire l'objet d'abus à un moment donné, les études de la Banque Mondiale et les rapports du groupe de travail du GSMA sur la fraude indiquent que l'argent mobile n'a jusqu'à présent pas été l'objet d'activité criminelle ou terroriste par comparaison aux autres systèmes de paiement comme par internet ou en argent liquide.

Bien qu'aucun système de paiement ne puisse complètement échapper à la fraude, il est important de mesurer le pouvoir d'attraction d'un système pour les activités criminelles au travers des données statistiques.

Bien que cela constitue une bonne nouvelle pour le moment, la vigilance reste nécessaire pour détecter les nouveaux risques en voie d'apparition et les activités de BC/FT. Cela ne peut s'effectuer que par une étroite surveillance à la fois par les prestataires de services d'argent mobile et par les autorités réglementaires financières (et/ou unités de renseignement financier). Nous espérons que la présente méthodologie d'évaluation des risques combinée à une étroite collaboration entre les autorités réglementaires et les prestataires d'argent mobile se traduira par la production de réglementations efficaces.

Nous préconisons par conséquent une approche empirique[11]: suivi attentif et apprentissage par le biais des expériences d'argent mobile pour une évaluation préliminaire des risques sur la base de la présente méthodologie d'évaluation des risques de BC/FT tant par l'industrie que par le régulateur afin de déterminer des règles adéquates de réduction des risques.

Principe : une réglementation adéquate en matière de LAB/CFT doit provenir d'une étroite collaboration entre l'industrie et le régulateur financier. Sur la base d'une collaboration basée sur l'expérience lors de l'expérimentation de nouveaux services, les risques liés aux nouveaux services sont systématiquement évalués avant de déterminer les mesures appropriées permettant de réduire ces risques.

[9] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik et Andrew Zerzan: *Integrity in Mobile Phone Financial Services* (Intégrité des services financiers par téléphone mobile), Banque Mondiale (2008); De Koker, Louis. 2009: *The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines* (Les risques de blanchiment d'argent soulevés par les produits financiers à faible risque en Afrique du Sud: conclusions et recommandations), Journal of Money Laundering Control, Vol. 12 No. 4. 323-339

[10] Zerzan, Andrew: *New Technologies, New Risks? Innovation and Countering the Financing of Terrorism* (Nouvelles technologies, nouveaux risques? Innovation et lutte contre le financement du terrorisme), Banque Mondiale(2009)

[11] Cette approche empirique se caractérise par un apprentissage commun de l'industrie et des autorités réglementaires dans le cadre d'expérimentations à petite échelle leur permettant, par un suivi particulièrement attentif de celles-ci, de bien appréhender les différents aspects de l'argent mobile, les risques correspondants, et les moyens d'atténuer ces risques de manière satisfaisante. Cette approche permet aux autorités réglementaires d'élaborer des outils de prévention des risques efficaces et adaptés pendant la phase pilote. Nous pensons que cette approche est plus efficace qu'une application à l'aveugle de règles existantes, susceptibles de n'être ni adéquates ni efficaces. Le choix final et le lancement des instruments réglementaires de prévention des risques interviennent à l'issue de la phase d'expérimentation du projet et avant le déploiement à grande échelle des services concernés. En soumettant l'autorité réglementaire et l'opérateur de téléphonie à ce processus, cette approche les force à acquérir une connaissance approfondie des risques et des outils de prévention de ces risques pour un service donné par un processus d'apprentissage commun et partagé.

Principes réglementaires pour une réglementation LAB/CFT efficace :

- La réglementation doit être fonction du niveau de risque et indépendante de la technologie: « À risque identique, réglementation identique », pour tous.
- Lors de l'évaluation des risques et de leur réduction, il est essentiel de laisser « l'effet domino » caractéristique de l'argent mobile augmenter le degré d'inclusion financière. Le développement du système financier formel et la réduction de l'économie informelle contribuent directement à la réduction des risques de BC/FT.
- La nature numérique et la traçabilité de l'argent mobile réduisent les risques de BC/FT par rapport à l'utilisation de l'argent liquide.
- Inclusion financière et LAB/CFT sont complémentaires et se renforcent mutuellement.
- Les services d'argent mobile doivent constituer une activité réglementée placée sous la tutelle du régulateur financier ou de toute autre autorité financière compétente.
- Une réglementation adéquate en matière de LAB/CFT doit provenir d'une étroite collaboration entre l'industrie et le régulateur financier. Sur la base d'une approche collaborative empirique **lors de l'expérimentation de nouveaux services**, les risques liés aux nouveaux services sont systématiquement évalués avant de déterminer les mesures appropriées permettant de réduire ces risques.

1.2 Pourquoi utiliser une méthodologie d'évaluation des risques?

De nouveaux services d'argent mobile font leur apparition dans le monde alors que les régulateurs financiers n'ont qu'une connaissance limitée des risques de BC/FT liés à ces nouveaux services émergents. Les règles actuelles de LAB/CFT sont souvent appliquées de manière disproportionnée par rapport aux risques encourus, handicapant ainsi l'adoption des services d'argent mobile par la clientèle. Il est par exemple disproportionné d'exercer des procédures de vérification préalable approfondies auprès de clients à faibles revenus effectuant des opérations de très petit montant[12] Des règles excessivement strictes en matière de connaissance des clients (ou *Know Your Customer* c'est-à-dire de procédures de vérification d'identité) peuvent être impossibles à satisfaire pour les clients les plus pauvres, les obligeant ainsi à rester dans une économie informelle.

Le moment est donc opportun pour engager un débat au niveau mondial sur la manière d'harmoniser et d'ajuster les règles de prévention de BC/FT s'agissant de services d'argent mobile, afin d'en garantir l'efficacité et de s'assurer que les services d'argent mobile bénéficient à une portion important de la population non bancarisée.

[12] Nous nous référons ici à la population cible du projet *Mobile Money for the Unbanked*: les clients vivant avec moins de 2 dollars par jour et effectuant des opérations en conséquence. Nous estimons qu'exercer des procédures de vérification préalable approfondies sur cette clientèle est disproportionné

2. Caractéristiques des services d'argent mobile

Dans ce chapitre, nous examinons les caractéristiques principales des services d'argent mobile[13]. Celles-ci peuvent se classer en trois parties: 1) les types de services, 2) leur utilisation et 3) une description des conditions dans lesquelles ils sont utilisés. La description de ces caractéristiques nous permettra de déterminer les risques de BC/FT liés à chacune d'entre elles.

Les services de paiement communément appelés services d'argent mobile recouvrent un éventail de services: certains ne constituent qu'une nouvelle façon d'accéder à un compte bancaire, d'autres permettent d'effectuer des paiements à partir d'une carte de crédit ou d'autres produits financiers, et d'autres permettent d'effectuer des paiements à partir de comptes ouverts auprès des opérateurs de téléphonie mobile.

Les services de paiement étudiés dans ce document impliquent l'ouverture d'un compte prépayé, généralement détenu par l'opérateur de téléphonie mobile (ou dans certains cas d'un compte spécifique auprès d'une banque partenaire), et utilisé comme un moyen de paiement indépendant. Ils représentent par conséquent plus qu'un simple moyen d'accéder à un compte bancaire et soulèvent des problèmes spécifiques en matière de réglementation LAB/CFT.

2.1 Quels sont les services en cause?

Les fonctionnalités de paiement les plus courantes sont les suivantes:

Virements nationaux: transferts d'argent entre deux personnes résidant dans le même pays (aussi appelés P2P).

Virements internationaux: transferts d'argent généralement effectués entre les travailleurs émigrés à l'étranger et les membres de leur famille dans leur pays d'origine.

Stockage d'argent: dans certains systèmes, le compte sert à stocker de l'argent en sécurité, que ce soit par le biais d'un compte ouvert dans une banque ou, plus couramment, d'un compte ouvert au niveau de l'opérateur mobile.

Paiements de détail: paiements auprès de commerçants participants. Ces commerçants peuvent être des supermarchés, des distributeurs de biens de consommation ou l'opérateur mobile lui-même (pour l'achat de crédit de temps d'appel ou d'autres services par les utilisateurs).

Paiements de factures: pour le paiement des factures des services de première nécessité comme l'eau et l'électricité, apportant commodité et efficacité.

Paiements en provenance de l'État: versement des salaires, pensions et autres versements, appelés à se développer dans les quelques années à venir.

2.2 Comment ces services sont-ils utilisés en pratique?

Les éléments d'information suivants donnent une image de l'utilisation de ces services en Afrique de l'Est (Kenya, Tanzanie, Ouganda) et Asie du Sud-Est (Philippines, Malaisie) où ils sont les plus répandus:

Montant des paiements: généralement très bas, en moyenne de 20 à 50 dollars. L'utilisateur typique effectue un montant total d'opérations de 500 à 1000 dollars par an seulement (selon le PIB du pays).

Fréquence d'utilisation: par exemple, les études menées au Kenya indiquent que plus de 65% des clients utilisent le service au moins une fois par mois, mais seulement 1% l'utilisent plus fréquemment qu'une fois par semaine.

Chargement et retrait d'argent: l'ajout et le retrait d'argent sur un compte s'effectuent auprès d'une variété de commerces de détail tels que les agences de l'opérateur de téléphonie mobile, les pharmacies ou les supermarchés/supérettes. Dans les marchés où il existe une plus grande présence des institutions financières classiques, ces opérations peuvent s'effectuer auprès d'une agence bancaire ou d'un agent de transfert de fonds.

[13] Voir les définitions de l'argent mobile, des paiements mobiles et des services bancaires mobiles en annexe 1, ainsi que la comparaison entre services d'argent mobile et services bancaires en annexe 4.

2.3 Quel est l'environnement d'utilisation de ces services?

L'environnement actuel des services d'argent mobile peut être décrit sur la base de l'exemple du Kenya [14] :

Géographie: l'argent circule généralement des zones urbaines vers les zones rurales. La plupart des services ne fonctionnent actuellement qu'à l'intérieur de chaque pays. Il existe néanmoins une forte demande pour les paiements transfrontaliers à cause du besoin de transférer de l'argent de façon économique vers les familles restées au pays.

Profil démographique de la clientèle: les utilisateurs urbains ont tendance jusqu'à présent à être des clients bancarisés envoyant de l'argent aux membres de leur famille non-bancarisés. L'expéditeur travaille généralement en ville et envoie de l'argent à sa famille comme une aide régulière. Ce phénomène suscite une demande pour des services d'argent mobile plus rapides, plus sûrs et plus pratiques et attire les clients non-bancarisés vers le système financier formel.

Infrastructures en place de paiement et services financiers: la plupart des personnes ne disposent pas de compte bancaire ou d'accès à une institution financière. En l'absence de services d'argent mobile, les transferts d'argent s'effectuent fréquemment sous forme d'espèces via des canaux informels, comme l'utilisation de convoyeurs d'argent ou de systèmes alternatifs de transferts.

Infrastructures d'identification de la population: bien que dans le cas du Kenya, il existe un système obligatoire de carte d'identité, dans beaucoup d'autres pays où les services d'argent mobile sont en plein essor il est pratiquement impossible d'effectuer des vérifications d'identité formelles. L'absence d'infrastructures nationales d'identification et de documentation affecte la majorité de la population dans la plupart des marchés et l'empêche d'accéder au système financier formel (voir les informations supplémentaires en annexe 3).

Cadre réglementaire: l'application de la réglementation LAB/CFT en matière de services d'argent mobile est inégale selon les pays dans lesquels ces services se sont développés. Selon la Banque Mondiale, il y a parfois eu une application disproportionnée des normes LAB/CFT à cause d'une peur actuellement non-fondée des services d'argent mobile.[15] Certains pays ne disposent pas d'un cadre réglementaire approprié ou n'appliquent pas ces réglementations dans les faits.

Les facteurs évoqués ci-dessus sont utilisés dans l'analyse des risques qui suit. Nous les évaluons pour déterminer leur contribution au profil de risque global des produits de paiement. Les profils de risque de deux services de paiement incluant un service d'argent mobile typique et un service bancaire traditionnel sont comparés en annexe 4 à titre d'exemple.

[14] Il est difficile de définir un environnement à l'échelle mondiale sachant que la clientèle non-bancarisée se trouve dans le monde entier et dans tous les pays en voie de développement. Nous utilisons le Kenya comme un exemple car il s'agit du pays où les services d'argent mobile ont jusqu'à présent remporté le plus de succès. Le Kenya compte à l'heure actuelle 8 millions d'utilisateurs des services d'argent mobile.
[15] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik et Andrew Zerzan: *Integrity in Mobile Phone Financial Services* (Intégrité des services financiers par téléphone mobile), Banque Mondiale (2008).

3. Méthodologie d'évaluation des risques

Il existe déjà une documentation utile en provenance de la Banque Mondiale et du CGAP donnant un aperçu général des questions de LAB/CFT liées aux services d'argent mobile[16].

L'objectif de la méthodologie d'évaluation des risques présentée dans ce document est de proposer une méthode d'analyse systématique des risques de BC/FT, apportant ainsi à l'industrie et aux autorités réglementaires un outil pratique d'évaluation des risques, et par conséquent la capacité de choisir des réponses de prévention des risques adéquates.

Pour pouvoir mettre en œuvre cette méthodologie, nous devons analyser :
- Les vulnérabilités de l'argent mobile en matière de BC/FT
- Comment ces vulnérabilités peuvent être exploitées par les acteurs de BC/FT
- Quels sont les outils appropriés pour la prévention des risques connus.

3.1 Quelles sont les vulnérabilités des services d'argent mobile en matière de BC/FT?

Après avoir identifié les caractéristiques des services d'argent mobile présentant des risques de blanchiment d'argent, l'analyse de risque commence par une analyse de la vulnérabilité de ces services vis-à-vis des risques de BC/FT.

Tout système de paiement présente des vulnérabilités susceptibles d'ouvrir la porte au BC/FT. Dans les marchés où la demande pour les services d'argent mobile est la plus forte (ainsi que leur succès) les transactions en espèces constituent la forme de paiement prédominante.

Par conséquent, nous comparons d'abord la vulnérabilité générique des transactions en espèces et par téléphone mobile sur la base des facteurs de risque de la Banque Mondiale: anonymat, insaisissabilité, rapidité et absence de surveillance[17].

Comparaison des niveaux de risque entre opérations en espèces et opérations d'argent mobile en l'absence de contrôles LAB/CFT

Facteurs généraux de risque	Espèces	Argent mobile
Anonymat	***	**
Insaisissabilité (absence de traçabilité des opérations)	***	**
Rapidité	*	***
Absence de surveillance	***	*[18]

*** Indique un niveau de risque élevé
** Indique un niveau de risque moyen
* Indique un niveau de risque faible

Anonymat: même dans le pire des cas, en l'absence d'enregistrement des clients mobiles, les transactions sont moins anonymes que les paiements en espèces car elles peuvent toujours être rattachées à un numéro de téléphone portable spécifique et le détail de ces transactions (numéro de téléphone portable de l'expéditeur, numéro de téléphone portable du bénéficiaire, montant et date) reste enregistré et traçables. Elles diffèrent en cela des paiements en espèces pour lesquels il n'y a ni identification des parties, ni trace du paiement. En outre, les pays exigent de plus en plus un enregistrement en face-à-face avec présentation d'un justificatif de domicile pour tout achat d'une carte SIM.

Insaisissabilité: alors que les transactions en espèces sont insaisissables, les transactions d'argent mobile sont facilement traçables dans le système des opérateurs mobiles dans le cadre de leurs pratiques commerciales habituelles. Les numéros de téléphone (d'envoi et de réception), l'heure et le montant de la transaction sont connus de l'opérateur mobile.

[16] Voir par exemple Isern J. et de Koker L., Normes LAB/CFT: Améliorer l'inclusion et l'intégrité financières, Focus Note n° 56, Washington, D.C. : CGAP, 2009.
[17] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik et Andrew Zerzan: *Integrity in Mobile Phone Financial Services* (Intégrité des services financiers par téléphone mobile), Banque Mondiale (2008).
[18] Les opérateurs de téléphonie mobile offrant des paiements mobiles doivent être agréés par les autorités financières parce qu'il s'agit d'une activité réglementée. Dans certains cas, les opérateurs de réseaux mobiles s'engagent dans des partenariats avec des banques ayant l'autorisation réglementaire d'offrir des services de paiement mobile. Dans d'autres cas, les opérateurs mobiles sont agréés par la banque centrale en tant que prestataire de services financiers indépendant par le biais d'une licence spécifique de paiement ou d'argent électronique. Nous faisons néanmoins l'hypothèse que les paiements mobiles sont systématiquement placés sous la tutelle des autorités financières ou ne sont sinon pas autorisés.

Rapidité: pour les transactions à distance[20], le caractère électronique de la technologie mobile rend les transactions plus rapides et faciles que les transactions en espèces. La rapidité constitue par conséquent un facteur de risque plus important pour les services d'argent mobile que pour les espèces. En l'absence de contrôles internes automatisés, cela peut fournir un moyen efficace de blanchiment de l'argent ou de financement d'activités terroristes.

Absence de surveillance: alors qu'une économie d'espèces échappe à toute surveillance, les opérateurs mobiles offrant des services monétaires mobiles sont généralement réglementés, que ce soit indirectement par le biais d'un partenariat avec une banque (les autorités réglementaires assurent de ce fait une surveillance des activités d'argent mobile de la banque dans le cadre de ce partenariat) ou directement par le biais de l'obtention d'une autorisation de paiements ou d'argent électronique.

Pour résumer, nous estimons dès le départ qu'à l'exception de la rapidité, les risques de BC/FT sont plus élevés pour les opérations en espèces que pour les services d'argent mobile. Sachant que les services d'argent mobile sont principalement déployés dans les pays en voie de développement et les économies d'argent comptant, ils constituent a priori une amélioration en terme de LAB/CFT par rapport aux espèces.

Il existe néanmoins des vulnérabilités que les criminels sont susceptibles d'exploiter si elles ne sont pas contrôlées.

3.2 Comment les criminels et terroristes peuvent-ils exploiter ces vulnérabilités?

Après avoir identifié les vulnérabilités globales des systèmes d'argent mobile, nous pouvons appliquer les typologies connues d'activités de BC/FT pour mesurer l'attractivité de ces systèmes à des fins criminelles. Ces typologies représentent des schémas criminels habituels associés à certains services financiers. Elles permettent aux praticiens de repérer les abus et aux autorités réglementaires d'évaluer la solidité des systèmes des prestataires. Dans le cadre de la présente méthodologie, elles constituent un moyen efficace de mesure le niveau de risque d'un service de paiement et de repérer les situations où des mesures de préventions s'avèrent nécessaires.

Comme il n'existe jusqu'à présent que très peu de cas de blanchiment de capitaux et aucun de financement du terrorisme par argent mobile, nous utiliserons des typologies rencontrées dans les paiements de détail et les autres nouvelles méthodes de paiement.[21] Elles apportent quantité d'informations pouvant être utilisées dans notre analyse.

Les typologies sont tout d'abord organisées selon trois étapes: 1) chargement des fonds sur le compte, 2) transfert des fonds et 3) retrait des fonds. Elles sont ensuite classées en fonction des opportunités pour des activités de BC/FT se présentant pour les différents intervenants dans le système: les consommateurs, les commerçants, et les agents partenaires. Une analyse de ceux-ci est présentée dans le tableau de l'annexe 5.

Sur la base des quatre facteurs de vulnérabilité identifiés au chapitre précédent, nous pouvons illustrer la manière dont ils peuvent faciliter des stratégies criminelles visant à exploiter le système pour des activités de BC ou de FT. Bien qu'il ne s'agisse que d'exemples, et que la liste complète se trouve en annexe 5, ils seront évoqués ici pour illustrer le lien entre les typologies de BC/FT et les vulnérabilités d'un système donné.

Chargement. La typologie la plus notable à ce niveau est probablement l'introduction de fonds illicites dans le système (également connue comme la phase de « placement » en matière de blanchiment de capitaux). Elle peut avoir plusieurs buts, l'un d'entre eux étant de continuer le processus de *smurfing* (fraude financière) par lequel les criminels dissimulent le montant réel des sommes en jeu en le fractionnant en petits montants pouvant passer inaperçus.

Transfert. Les services de paiement peuvent être utilisés pour faire « écran », stratégie permettant aux criminels de compliquer le circuit de l'argent et d'empêcher d'en suivre la trace.

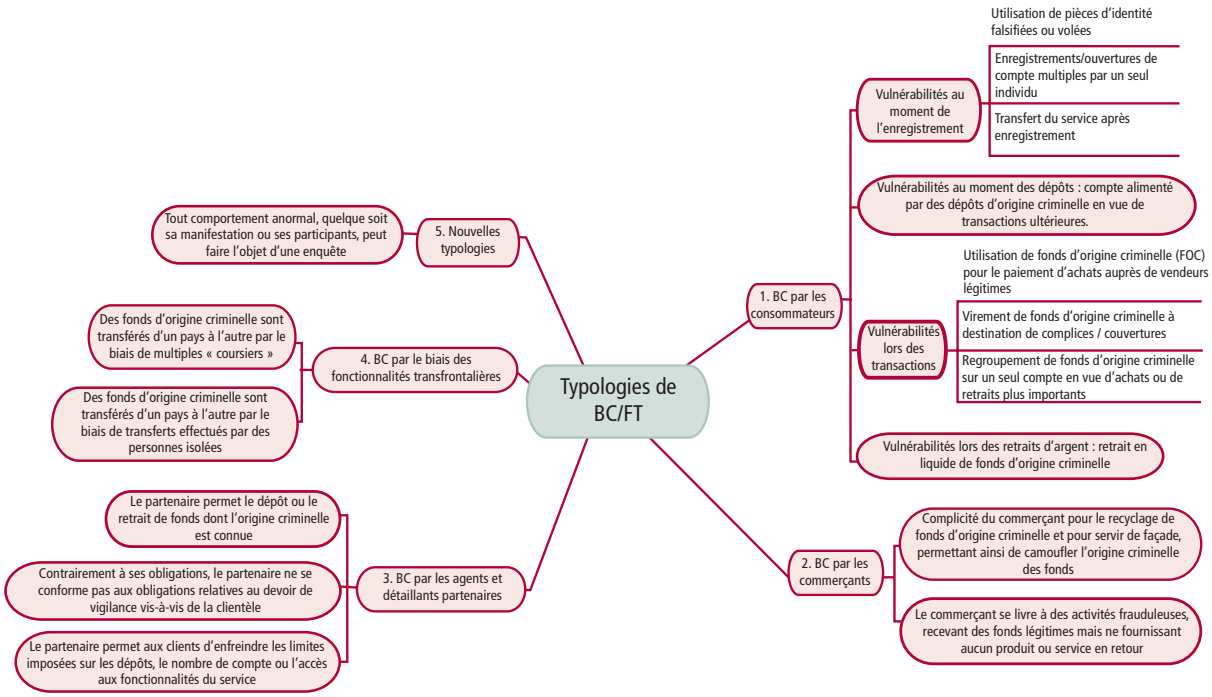
Retrait. Qu'il s'agisse de la suite de la stratégie précédente ou d'un moyen de recycler des fonds d'origine illicite, les criminels peuvent trouver un intérêt à cette opération. Un mouvement rapide de fonds, effectué de manière anonyme, entre le chargement initial et leur retrait pourrait servir à des activités de BC ou FT.

[20] Pour les transactions face à face, la remise d'espèces reste encore aussi rapide et efficace que tout paiement électronique (et moins traçable).
[21] Les aspects communs entre ces services sont détaillés dans: *"Report on New Payment Methods"* (rapport sur les nouvelles méthodes de paiement) du GAFI, 13 octobre 2006; *"Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems"* (Blanchiment de capitaux et financement du terrorisme: vulnérabilités des sites de commerce en ligne et des systèmes de paiement via internet) du GAFI, 18 juin 2008.

Facteurs généraux de risque	Exemples d'exploitation de ces vulnérabilités à chaque étape		
	Chargement	Transfert	Retrait
Anonymat	Les criminels peuvent ouvrir plusieurs comptes pour dissimuler le montant réel des dépôts	Les noms des suspects ne peuvent être repérés par le système, ce qui en fait une zone sûre pour les terroristes et les criminels connus	Permet de retirer des fonds illicites ou liés à des activités terroristes
Insaisissabilité	Les criminels peuvent dissimuler le fruit de leurs activités criminelles dans différents comptes	Les criminels peuvent effectuer des opérations multiples pour camoufler le circuit de l'argent et l'origine réelle des fonds.	Les fonds camouflés en provenance de différents comptes peuvent être retirés en même temps.
Rapidité	Des fonds illégaux peuvent être déposés rapidement puis transférés sur un autre compte.	Les opérations s'effectuent en temps réel, laissant peu de temps pour les bloquer en cas de suspicion de BC/FT.	Les fonds illégaux peuvent circuler rapidement dans le système pour être retirés sur un autre compte.
Absence de surveillance	Sans surveillance adéquate, les services peuvent présenter un risque systémique.		

L'examen des différentes manières dont les criminels peuvent utiliser le système ne doit cependant pas limiter aux seules étapes des opérations de paiement. Il est également nécessaire d'identifier les typologies liées aux différentes parties prenantes concernées.

Ces typologies sont résumées dans le diagramme ci-dessous et détaillées dans le texte qui suit. La numérotation des paragraphes dans le texte correspond aux chiffres figurant dans le diagramme, lequel fournit une présentation visuelle des différentes typologies.



BC/FT par la clientèle: peut se produire sous la forme d'un virement classique ayant une origine ou une destination criminelle (par exemple, financement du terrorisme)[22]. Bien que des justificatifs réels puissent être utilisés lors de la souscription, de fausses informations peuvent également être présentées. L'étape de dépôt en compte peut également servir à recycler des fonds d'origine frauduleuse via l'utilisation de cartes bancaires ou cartes de crédit volées (ce qui peut être considéré comme un processus de « placement »). Les opérations peuvent également servir à transférer des fonds entre complices, ou à les transférer vers d'autres pays dont les juridictions ont des réglementations en matière de LAB/CFT moins lourdes, où les fonds peuvent être utilisés pour financer d'autres activités criminelles. Cela s'accompagne alors par le retrait de ces sommes sous forme d'espèces pour leur utilisation ou pour leur transfert par le biais d'autres moyens.

BC/FT par les commerçants: ces personnes sont susceptibles de présenter un risque plus élevé, car elles peuvent recevoir des montants substantiels de paiements et les faire apparaître comme le produit légitime de leur activité (cela pouvant comprendre l'intégration de fonds). Les commerçants peuvent être des criminels eux-mêmes, escroquant leur clientèle, ou servant de façade pour le blanchiment du produit des activités de leurs complices, se faisant passer eux-mêmes pour des clients.

BC/FT par les agents, intermédiaires et partenaires de détail: ces personnes se situent à un emplacement stratégique dans le cycle de paiement des services d'argent mobile: le chargement de sommes en espèces, le point de rachat ou retrait, et également la vente des appareils téléphoniques susceptibles d'être utilisés pour les opérations. Ces personnes ont donc la possibilité de falsifier leurs registres, d'ignorer des soupçons qui devraient sinon être signalés, ou simplement de constituer un point de faiblesse en n'exerçant pas leur fonction avec toute la vigilance nécessaire.

BC/FT par le biais des paiements transfrontaliers: ceux-ci peuvent servir à déplacer des fonds d'origine criminelle de leur juridiction d'origine vers une autre juridiction dans laquelle ils peuvent servir à d'autres activités criminelles, être extraits ou à nouveau déplacés vers une autre juridiction. Les mouvements de fonds transfrontaliers rendent les recherches des autorités plus difficiles et permettent de camoufler l'objet du transfert. Ils constituent par conséquent une source supplémentaire de risque.

Nouvelles typologies: les criminels continuant d'imaginer de nouvelles méthodes de financement du terrorisme et de blanchiment d'argent, il est important de noter que ces différentes typologies ne sont pas exhaustives.

3.3 Comment se prémunir contre les risques ayant été identifiés

Après avoir identifié les vulnérabilités potentielles (paragraphe 3.1) et les risques de BC/FT (section 3.2), il est maintenant possible de mettre en œuvre des mesures de prévention des risques appropriées. Le détail se trouve en annexe 5 dans laquelle les niveaux de risques sont évalués avant et après les mesures d'atténuation. Ce qui suit est un résumé de ces conclusions.

BC/FT par la clientèle: le risque peut être ramené à un niveau faible par l'application de quelques mesures de prévention simples. Ces quelques mesures essentielles de prévention du risque peuvent être mises en œuvre en fonction des environnements dans lesquels ces services sont offerts. La première est la mise en place de limites sur le nombre de comptes, fréquences d'opérations, volumes et montants de virement pouvant être réalisés sur une certaine période de temps. Cela peut être efficace si les montants et volumes d'opérations sont très bas. La seconde est la surveillance au niveau du système des flux d'opérations visant à signaler au prestataire d'argent mobile toute séquence d'opérations suspecte (de manière similaire aux systèmes de LAB/CFT actuellement utilisés par les banques et les systèmes de détection des fraudes utilisés par les opérateurs de téléphonie mobile). Ces mesures se renforcent l'une l'autre, parce que les limites imposées obligent les criminels et terroristes à fractionner leurs opérations, les rendant ainsi plus susceptibles d'être détectés par le système[23]. Lorsque les clients effectuent des volumes d'opérations importants avec une fréquence élevée, ce qui constitue un risque de BC/FT, ils peuvent alors être obligés de souscrire en personne et de confirmer leur identité. L'idée importante ici est la mise en œuvre de mesures de prévention proportionnées en fonction des risques rencontrés.

[22] GAFI, *Terrorist Financing Typologies Report* (Rapport sur les typologies de financement du terrorisme), 2008

BC/FT par les commerçants: ces intervenants présentent un niveau de risque plus élevé. La prévention du risque au moyen de procédures de vérification approfondies au début et en cours de relation permet néanmoins de réduire le risque jusqu'à un niveau faible. La sensibilisation des commerçants constitue également un élément essentiel: ils ont la préoccupation de la viabilité de leur entreprise, et la connaissance des conséquences des activités criminelles diminue la probabilité qu'ils y participent. Les autres méthodes d'évaluation et de réduction des risques sont la formation, les contrôles et les « visites mystère » de la boutique des commerçants.

BC/FT par les agents, intermédiaires et partenaires de détail: le risque le plus important de BC/FT dans le système d'argent mobile se trouve au niveau des agents et détaillants participants ayant la possibilité de donner accès au service de paiement, de charger des sommes sur le système ou de conduire les procédures de vérification pour le compte de l'opérateur de téléphonie mobile. Ces risques peuvent néanmoins être atténués, mais cela nécessite des procédures de vérification approfondies au début et en cours de relation ainsi qu'une surveillance continue du respect des obligations. Les prestataires peuvent par exemple vérifier le bon respect des règles et l'intégrité de leurs agents par le biais de « visites mystère » contrôlant ces agents. Ils peuvent également demander aux agents et détaillants associés d'assurer une formation de leur personnel sur LAB/CFT, en apportant leur assistance et en effectuant une surveillance de cette formation. Par le biais d'une surveillance des activités sur site, ils peuvent aussi identifier les activités inhabituelles et/ou suspectes, enquêter, et prendre les mesures correctives nécessaires.

BC/FT par le biais des paiements transfrontaliers: ces paiements sont susceptibles d'accroître les risques, mais les outils de surveillance des opérations, des limites sur les montants et la fréquence des opérations et des procédures de vérification appropriées au niveau des clients peuvent permettre de les contrôler et de repérer les opérations inhabituelles ou suspectes, ramenant ainsi le risque à un niveau faible.

Cette analyse repose sur une approche adaptée au niveau de risque. Les procédures de vérification préalables (« *due diligence* ») et autres mesures de préventions doivent être appliquées de manière proportionnée par rapport aux risques présentés par chaque catégorie d'intervenants. Dans le cas des clients ayant des limites d'opération faibles associés à une surveillance en temps réel par les systèmes, les risques sont faibles. Les commerçants et les agents présentent cependant des risques plus élevés étant donné que certains contrôles (par exemple les limites sur opérations) ne peuvent pas leur être appliqués de la même manière. La prévention des risques exige des procédures de vérifications approfondies, de la formation et une surveillance continue.

3.4 Risques comparés entre transactions en argent liquide et en argent mobile, avant et après contrôle des risques

Faisant le lien entre la mise en œuvre des mesures de prévention ci-dessus et notre analyse initiale des risques comparés entre transactions en espèces et transactions en argent mobile, nous pouvons tirer quelques conclusions d'ordre général concernant les risques. Le tableau ci-après fait suite à celui du paragraphe 3.1. Il montre les exemples de mesures de prévention des risques et leur impact sur le niveau de risque.

La mise en œuvre de mesures de prévention des risques en réduit l'intérêt pour les activités criminelles et terroristes. Les opérations sont nécessairement de faible montant à cause des limites imposées. Toute tentative de transfert de sommes importantes d'un endroit à un autre est donc facilement repérable. Le niveau de risque lié à la rapidité, jugé initialement plus élevé que pour les transactions en argent liquide, est désormais plus bas grâce aux systèmes de contrôle automatisés (les contrôles internes imposent les limites sur le montant et la fréquence des opérations et les montants en compte, et même si des transactions BC/FT sont fractionnées pour y échapper, le système de surveillance a la capacité de repérer au niveau de la plateforme les séries d'opérations suspectes). Les noms des clients peuvent être vérifiés rapidement par rapport aux listes nationales et internationales d'interdits et signalés automatiquement. Il est intéressant de noter que ces méthodes sont par bien des aspects beaucoup plus efficaces que celles d'autres prestataires habituels de services financiers dans les pays en développement, qui sont souvent manuelles et sujettes aux erreurs.

Comparaison des niveaux de risque entre opérations en espèces et opérations d'argent mobile avant et après mise en place des mesures de prévention

Facteurs généraux de risque	Espèces	Argent mobile		
		Avant	Contrôles	Après
Anonymat	***	**	Création de profils client, incluant les informations lors de la souscription (nom, numéro de téléphone spécifique, etc.)	*
Insaisissabilité (absence de traçabilité des opérations)	***	**	Mise en place de limites sur les montants, soldes, fréquences et nombre d'opérations Surveillance des opérations en temps réel	*
Rapidité	*	***	Surveillance des opérations en temps réel Restrictions sur la fréquence des opérations Restrictions sur le montant de chaque transaction et le montant total de celles-ci sur une période de temps donnée.	*
Absence de surveillance	***	*		*

*** Indique un niveau de risque élevé
** Indique un niveau de risque moyen
* Indique un niveau de risque faible

4. Conclusions de l'analyse de risque

L'évaluation des risques réels posés par les services d'argent mobile est capitale pour pouvoir concevoir des mesures de prévention qui: 1) doivent cibler efficacement les risques posés et 2) ne pas empêcher inutilement l'accès des personnes les plus pauvres à ces services. LAB/CFT et inclusion financière constituent des objectifs qui se renforcent mutuellement. Les efforts de lutte contre le blanchiment d'argent et contre le terrorisme se terminent là où commence l'économie informelle basée sur l'argent liquide. L'argent liquide est anonyme, non traçable et son utilisation échappe à toute surveillance. Le développement des services d'argent mobile constitue une excellente occasion de réduire l'économie basée sur l'argent liquide, améliorant la sécurité du marché en même temps que les conditions de vie des personnes les plus pauvres.

Nous espérons que cette méthodologie contribue au débat entre industrie et autorités réglementaires pour le développement de modèles d'exploitation et de réglementations susceptibles d'optimiser la portée des services d'argent mobile. Nous pensons que seule une analyse attentive des risques réels permet de développer une réglementation et des mesures de prévention adaptées, et nous tenons prêts à soutenir ces efforts à l'avenir.

Annexe 1 : Lexique

Services d'argent mobile: L'argent mobile est un terme générique désignant l'utilisation d'un téléphone portable pour accéder à des services financiers. Ce terme ne réfère pas à un modèle spécifique de déploiement ou à un type de transaction en particulier; il désigne simplement un service utilisant la technologie mobile pour permettre aux clients d'initier une activité financière. En tant que tel, il recouvre les services de simples renseignements (par exemple, consultation de solde de compte) et les services transactionnels (par exemple, l'utilisation de la technologie mobile pour envoyer de l'argent à une autre personne ou pour payer des marchandises ou des services, ainsi que recevoir le versement de salaires ou pensions en provenance des organismes publics). **Les paiements mobiles et les services bancaires mobiles font tous deux partie des services d'argent mobile.**

Que signifie le terme de service bancaire mobile ?
Les services bancaires mobiles constituent une sous-catégorie des services d'argent mobile, distincte des paiements mobiles au sens où l'entité réglementée est une banque fournissant des services bancaires classiques. L'élément mobile ne constitue qu'un simple moyen d'accès à des services bancaires traditionnels.

Annexe 2 : Question/réponses (FAQ)

Question/préoccupation	Réponse
Un criminel cherchant à blanchir des fonds peut-il utiliser un téléphone une seule fois puis s'en débarrasser pour conserver son anonymat?	Les criminels ont en premier lieu le choix entre les espèces et l'argent mobile pour protéger leur anonymat. Les espèces offrent un meilleur anonymat que l'argent mobile car les paiements mobiles sont enregistrés dans le système et sont traçables. Même si le criminel décidait de virer de l'argent par le biais de l'argent mobile, le plafonnement du montant et du nombre des transactions ainsi que sur les soldes en compte rendraient l'opération très fastidieuse et coûteuse, l'obligeant à acquérir de nombreux appareils et cartes SIM. Les dispositifs de contrôle sont susceptibles de repérer ce genre d'activité comme étant suspecte. Et même si l'expéditeur se sert de plusieurs appareils et cartes SIM, le système enregistrerait le compte bénéficiaire, à moins que les appareils et cartes SIM soient également éliminés à chaque fois à l'autre extrémité de la transaction. Dans ce cas, le transfert d'espèces serait probablement moins coûteux, plus sûr et plus pratique pour les criminels que l'achat d'un grand nombre de téléphones portables et de cartes SIM, sachant que seul un nombre limité de paiements de petit montant est possible.
Que se passe-t-il en cas d'utilisation de l'appareil par une personne autre que l'utilisateur enregistré?	L'utilisateur enregistré doit communiquer son code secret à l'utilisateur non enregistré pour qu'un paiement mobile puisse être effectué. Le risque est le même que pour les paiements par carte bancaire (à savoir que le titulaire de la carte doit communiquer son code secret pour qu'un paiement par carte soit possible). L'opérateur conserve la trace de l'utilisateur enregistré, lequel conserve au final l'entière responsabilité des opérations.
Il est presque impossible de repérer des activités suspicieuses sans connaître l'identité de la personne effectuant les opérations. Les obligations de vérification préalable sont essentielles pour LAB/CFT. Comment cela peut-il fonctionner avec les comptes prépayés d'argent mobile, le nom de l'utilisateur n'ayant pas été vérifié ?	Les mesures de vigilance ne se limitent pas à recueillir l'identité des clients. Elles permettent également de détecter les liens existant entre certains comptes et de repérer les comptes suspects. Dans les économies où l'argent mobile rencontre le plus de succès, l'argent liquide constitue encore le moyen de paiement le plus courant. Il est complètement anonyme et intraçable. Il est impossible pour qui que ce soit de découvrir des connections entre des utilisateurs d'argent liquide et de surveiller leurs activités. L'argent mobile par comparaison est traçable par nature. Le numéro de téléphone constitue un identifiant unique fournissant plus d'informations que de l'argent liquide par nature anonyme, et augmentant la visibilité des transactions suspectes
Il est plus efficace d'améliorer l'inclusion financière par le biais d'un modèle de banque à distance non basé sur la technologie, qui ne présente pas de risques d'anonymat, d'insaisissabilité, de rapidité, etc. Pourquoi donc envisager des services d'argent mobile ?	Les deux principaux freins à l'inclusion financière sont le coût et la distance. Les deux sont souvent mêlés étant donné que le déplacement jusqu'à l'agence bancaire ou de transfert d'argent la plus proche implique des frais pour l'utilisateur. La technologie, et notamment la téléphonie mobile, offrent la possibilité de surmonter ces deux obstacles. Les services d'argent mobile éliminent la nécessité des déplacements vers une institution financière et coûtent nettement moins chers. Il n'existe pas de modèle bancaire non technologique présentant des caractéristiques équivalentes.

Question/Concern	Answer
Les services d'argent mobiles ne se faisant pas en face à face, sont par conséquent plus risqués.	L'expérience actuelle ne montre aucun risque supplémentaire en matière d'argent mobile par rapport aux autres moyens de paiement. Des plafonds d'opération très bas, ainsi que la surveillance des comptes et d'autres dispositifs de contrôle, permettent de limiter l'intérêt de ces services pour des activités criminelles en dépit de la possibilité d'effectuer des transactions sans présence physique des personnes concernées. Les plafonds en place dans la plupart des réseaux d'argent mobile sont peu élevés. Il serait possible d'avoir plus d'argent liquide en poche que ce qui est possible de transférer électroniquement. En outre, des dispositifs de surveillance permettent de détecter les opérations suspectes. Par exemple, les dispositifs de contrôle en place signaleraient tout compte recevant des sommes inhabituelles en provenance de différents endroits du pays, ainsi que les comptes d'origine de ces virements.
La vitesse avec laquelle la valeur peut être transférée électroniquement et la facilité avec laquelle il est possible d'envoyer des cartes SIM, représentent un risque qui n'existe pas avec l'argent liquide.	Les limites en place dans la plupart des modèles d'argent mobile sont très faibles. Il est possible d'avoir sur soi beaucoup plus d'argent sous forme de liquidités que de le transférer électroniquement à la vue de ces limites. De plus, la surveillance de ces systèmes permet de détecter des activités anormales. Par exemple, si un compte reçoit un montant inhabituel d'argent du pays tout entier, ce compte serait qualifié de suspect et toutes les activités provenant de ce compte aussi.
Les services d'argents mobiles méritent un traitement juridique en matière de LAB/CFT.	L'association GSM suggère que les obligations de vérification préalable à l'égard de la clientèle la plus pauvre (vivant avec moins de $2 par jour) et effectuant des opérations en conséquence (opérations de faibles montants et peu fréquentes – dans la limite des plafonds des services) sont disproportionnées. Cette opinion s'applique à l'ensemble des prestataires et pas seulement aux opérateurs mobiles. Elle respecte les recommandations du GAFI pour une approche graduée en fonction des risques.
À quoi ressemblerait une solution issue de la méthodologie recommandée par ce document ?	Les clients envoyant de très petites sommes d'argent à intervalles irréguliers (sous la surveillance des dispositifs de détection des opérations suspectes) seraient soumis à des mesures de vigilance allégées, et les fonctionnalités offertes à ce type de clientèle seraient limitées. Lorsque ces clients ont l'expérience du service, lui font plus confiance et réclament une certaine flexibilité pour des opérations de montant plus élevé, ils doivent alors s'enregistrer en personne pour obtenir un élargissement des services offerts. Les agents ou intermédiaires ne peuvent néanmoins accéder au service sans vérifications préliminaires approfondies car leur profil de risque est plus élevé.
Bien qu'avec les nouvelles méthodes de paiement l'ensemble des transactions soit généralement enregistré (« papiers électroniques »), cela ne sert à rien si le client conserve son anonymat ou bien utilise une fausse identité.	Même en l'absence de vérification approfondie du nom figurant sur un compte d'argent mobile, l'anonymat n'est pas le même qu'avec de l'argent liquide. Les enregistrements électroniques permettent à l'opérateur ainsi qu'aux autorités de surveiller l'activité des comptes et d'identifier les complices d'un crime. Si un compte apparaît particulièrement suspect, l'opérateur a la possibilité de le bloquer immédiatement et de demander aux agents de conduire des vérifications d'identité approfondies. La trace électronique des opérations d'argent mobile améliorera la fourniture de preuves aux autorités pénales et judiciaires chargées des enquêtes criminelles.

Annexe 3 : Procédures d'identification et BC/FT

Dans certains pays, un obstacle majeur pour l'accès des personnes les plus pauvres aux services financiers formels fournis par les banques et les institutions non bancaires est l'application excessivement stricte des mesures de vérifications préalables du client (ou *customer due diligence*) telles que définies par le Groupe d'action financière (GAFI) sur le blanchiment de capitaux.[24] Le GAFI a établi des normes de procédure concernant le devoir de vigilance relatif la clientèle et comprenant: (a) la vérification de l'identité du client au moyen de documents ou d'informations en provenance de sources fiables et indépendantes, (b) l'obtention d'informations concernant l'objet et la nature de la relation d'affaires et (c) l'examen attentif des transactions effectuées pendant toute la durée de la relation avec le client.

La vérification de l'identité des clients peut s'avérer particulièrement difficile dans les pays ne disposant pas d'un système avancé ou général d'enregistrement civil ou de carte nationale d'identité (à savoir, d'un système de pièces d'identité). Ces systèmes reposent sur l'enregistrement de la population. Les systèmes nationaux de pièces d'identité sont des systèmes où les États délivrent des cartes d'identité aux individus à compter d'un certain âge, sur la base des lois ou réglementations nationales. Ces systèmes peuvent fonctionner sur la base du volontariat, lorsque les personnes font la demande d'une carte, ou être obligatoires, lorsque l'ensemble de la population doit détenir une carte d'identité à un certain âge.

Des études récentes menées par Jentzsch (2009)[25] montrent que sur un échantillon de 173 pays[26], 136 pays au total (79% de l'échantillon) disposaient en 2007 d'un système volontaire ou obligatoire de carte d'identité. 37 pays (21%) ne disposaient pas d'un système de carte d'identité. Ces chiffres sont également présentés dans le tableau 1. Il existe également des pays utilisant des systèmes de remplacement, comme l'Australie, le Canada, les Etats-Unis ou le Royaume-Uni, dans lesquels le permis de conduire ou le numéro de sécurité sociale sont utilisés pour la vérification de l'identité des personnes, et qui sont inclus ici dans les pays n'ayant pas de système national de carte d'identité.

[24] Bester, H., de Koker, L., et Hawthorne, R., (2003), *Legislative and Regulatory Obstacles to Mass Banking* (Obstacles législatifs et réglementaires aux services bancaires de masse), pages 1-116, Genesis Analytics; De Koker, L. 2004. "*Client identification and money laundering control: perspectives on the Financial Intelligence Act 38 of 2001,*" (Identification des clients et mesures de prévention du blanchiment de capitaux : points de vue sur le Financial Intelligence Act 38 de 2001) Journal of South African Law 715-746; De Koker, L. 2006. *Money laundering control and suppression of financing of terrorism : some thoughts on the impact of customer due diligence measures on financial exclusion* (Mesure de prévention du blanchiment de capitaux et élimination du financement du terrorisme), Journal of Financial Crime, 26-50; Isern, J., D. Porteous, R. Hernandez-Coss, et C. Egwuagu. 2005. "*AML/CFT Regulation: Implications for the Financial Service Providers that Serve Poor People*" (Réglementations LAB/CFT : conséquences pour les prestataires de services financiers servant les personnes les plus pauvres) Focus Note 29. Washington, D.C.: CGAP; Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, et R. Walker. 2008. *Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines* (Application des normes du GAFI dans les pays en voie de développement et inclusion financière : conclusions et recommandation générales). The FIRST Initiative. Washington, D.C.: Banque Mondiale; Isern, J., et L. de Koker. 2009. "*AML/CFT: Strengthening Financial Inclusion and Integrity.*" (LAB/CFT : Intégrité et amélioration de l'inclusion financière) Focus Note 56. Washington, D.C.: CGAP.

[25] Les données chiffrées présentées ici constituent une mise à jour du rapport de N. Jentzsch de 2009. *Financial Services for the Poor: Lack of Personal Identification Documents Impedes Access* (Services financiers pour les pauvres : l'absence de documents d'identification personnelle empêche l'accès), DIW Weekly Report, 17 / 2009, pages 114-121. Ces données chiffrées sont préliminaires.

[26] Échantillonnage basé sur l'échantillon de « *Doing Business* » de la Banque Mondiale.

Existence et typologie des systèmes de carte d'identité - Tableau 1

	Nombre de pays	Pourcentage de l'échantillon
Existence d'un système de carte d'identité		
Nombre total de pays dans l'échantillon*	173	
Existence d'un système de carte d'identité volontaire ou obligatoire	136	78.61
Pas de système de carte d'identité	37	21.39
Type de système de carte d'identité		
Nombre total d'observations	135	
- avec un système obligatoire	112	82.96
- avec un système volontaire	23	17.04
Nombre de pays sans observation	38	

*La marge d'incertitude correspond aux observations des Comores, de Kiribati, Vanuatu, Palau et de la République démocratique du Congo. Le chercheur attend actuellement la réponse des autorités. Il existe des informations contradictoires concernant l'existence et le type de système de carte d'identité au Nigéria, lequel était recensé comme n'ayant pas de système de carte d'identité en 2007. Source : Jentzsch (2009), révisé.

Le type de système a pu être déterminé pour 135 pays seulement. Dans ce sous échantillon, 112 nations possédaient un système obligatoire (représentant 82.96% du sous échantillon) et 23 pays possédaient un système volontaire (soit 17.04%).

L'existence d'un système de carte d'identité ainsi que le caractère obligatoire de celui-ci n'implique pas forcément une couverture complète de la population économiquement active. Cette couverture peut être incomplète pour un certain nombre de raisons: par exemple, l'éloignement géographique des autorités délivrant les cartes peut être significatif et les moyens de déplacement pour s'y rendre excessivement lents, coûteux et/ou dangereux. De plus, les registres civils sont souvent incomplets lorsque des naissances ne sont pas enregistrées, notamment dans les zones rurales où les enfants naissent souvent en dehors des hôpitaux.

De plus, pour de nombreuses personnes pauvres ou très pauvres, le coût des cartes rend ce document important inabordable. Les prix peuvent varier de 3,41US$ pour une nouvelle carte en Angola à 5,44 US$ au Bénin et jusqu'à 68 US$ pour une nouvelle carte d'identité électronique en République Centrafricaine (sur la base des cours de change du 15 octobre 2009).[27]

[27] Ces estimations sont basées sur différentes sources officielles ou en ligne.

Existence et typologie des systèmes de carte d'identité - Tableau 2

Pays	Chiffres
Pakistan (système de carte d'identité obligatoire)	
Population totale	172.800.048
Population économiquement active (plus de 15 ans: 62.2%)	107.481.630
Population identifiée (détenant une carte nationale d'identité)	62.000.000
Population non identifiée (sans carte nationale d'identité)	45.481.630
% de la population totale sans carte nationale d'identité	42%
Indicateur d'accès aux services financiers (en pourcentage) (1)	12%
Cameroun (système de carte d'identité obligatoire)	
Population totale	18.060.382
Population économiquement active (plus de 15 ans: 58.7%)	10.601.444
Population identifiée (détenant une carte nationale d'identité)	7.209.916
Population non identifiée (sans carte nationale d'identité)	3.391.528
% de la population totale sans carte nationale d'identité	31%
Indicateur d'accès aux services financiers (en pourcentage) (1)	24%
Tanzanie (pas système de carte d'identité)	
Population totale	39.477.000
Population économiquement active (plus de 15 ans: 56.1%)	22.146.597
Population identifiée (détenant un passeport)	Est. 500.000
Population non identifiée	21.646.597
% de la population totale sans mode d'identification	97%
Indicateur d'accès aux services financiers (en pourcentage) (1)	5%

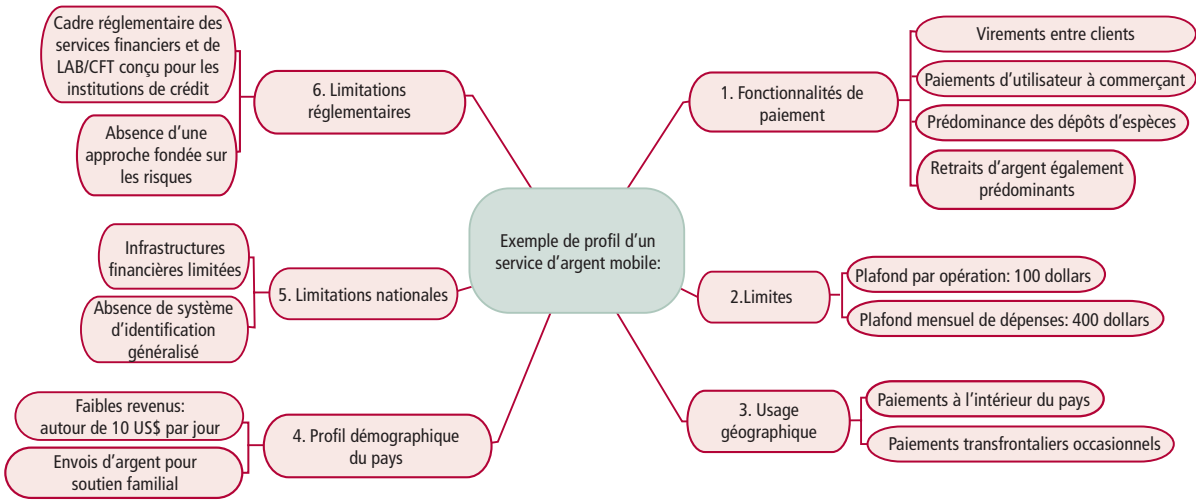
Notes (1) Pourcentage de la population adulte ayant accès à un compte auprès d'un intermédiaire financier formel. Sources: 2007 CIA World Factbook; Beck, Demirgüç-Kunt, Martinez Peria (2007); calculs par Jentzsch (2009), sur la base des chiffres fournis par les autorités locales.

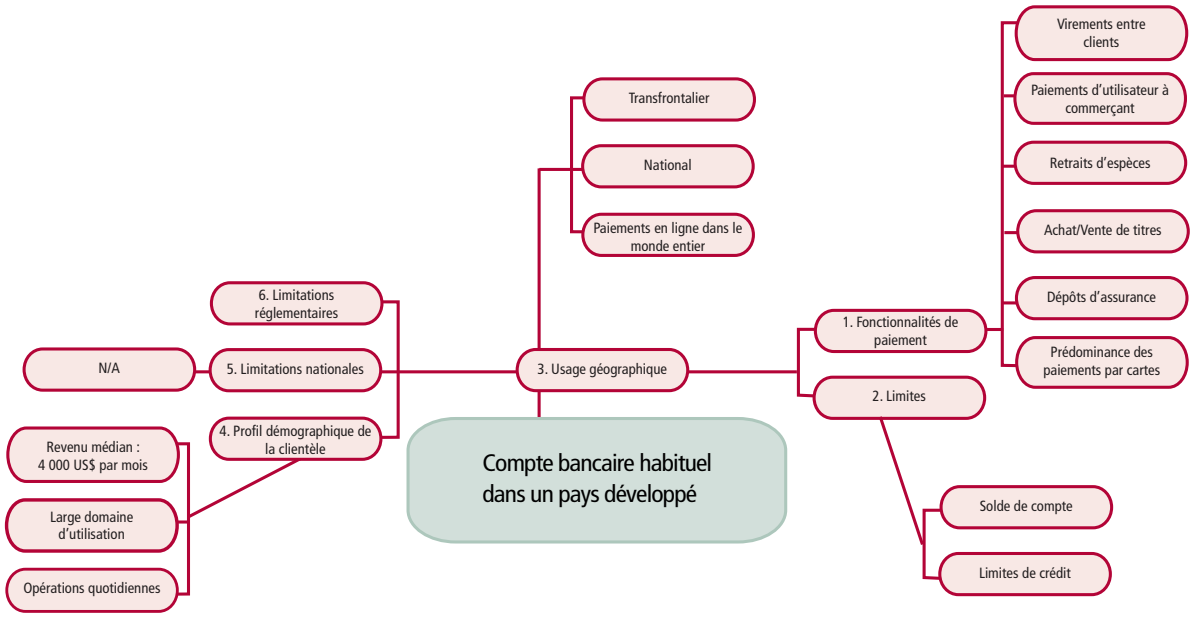
Le tableau 2 montre le pourcentage de la population possédant une carte d'identité dans des pays ayant un système de carte d'identité obligatoire (Pakistan et Cameroun) ainsi que dans un pays sans système de carte d'identité (Tanzanie). Les exemples du Pakistan et du Cameroun montrent que même dans les pays ayant un système de carte d'identité obligatoire, 30 à 40% des personnes économiquement actives ne possèdent pas de pièce d'identité. Il n'existe généralement pas de base de données internationale répertoriant le nombre de citoyens ayant une pièce d'identité dans les différents pays. Il existe dans un certain nombre de pays en cours d'émission de cartes d'identité (comme au Bangladesh ou au Botswana) ou de remplacement de celles-ci par des cartes à puce contenant des informations biométriques (en Albanie ou en République démocratique du Congo). D'autres pays prévoient de lancer des cartes multifonctions dans un avenir proche (en Inde).

Bien que la plupart des pays soient désormais membres du GAFI ou d'organismes équivalents, il n'existe actuellement aucune information indiquant dans quelle mesure les pays en développement peuvent dans la pratique se conformer aux mesures du GAFI. Il s'agit d'un domaine ouvert à des recherches supplémentaires.

Annexe 4 : Comparaison des paiements par argent mobile et des services bancaires

Exemple de profil d'un service d'argent mobile:





Annexe 5 : Tableau d'analyse des risques par typologie et impact après mesures de prévention

Légende : FOC = fonds d'origine criminelle; MV = mesures de vérifications préalables (« *due diligence* »);
BC = blanchiment de capitaux

	Typologie	Indicateur	Vulnérabilité	Mesures de gestion des risques et commentaires	Niveau de risque après gestion des risques
1	**BC/FT par les consommateurs**				
a.	Fraude lors de la souscription	Échantillonnage statistique des enregistrements pour audit et suivi	Moyenne	Les systèmes doivent inclure des programmes de détection des activités frauduleuses. Les dispositifs de surveillance des opérations doivent être en mesure de repérer les activités anormales par comparaison avec le comportement habituel d'utilisateurs comparables pour une zone donnée. La mise en place de dispositifs de contrôle supplémentaires à d'autres niveaux dans le système (plafonds, surveillance, etc) permet de réduire les risques d'ouvertures de compte frauduleuses en réduisant l'intérêt du système pour des activités criminelles.	Faible
b.	Souscriptions multiples	Les séquences d'opérations signalent la possibilité d'usages multiples	Moyenne	Les comptes rattachés à une même personne sont susceptibles d'être repérés par le système en présence de plafonds d'opérations peu élevés. Le système détecterait par exemple une augmentation soudaine des dépôts/retraits au niveau d'un agent particulier.	Faible
c.	Transfert du service après souscription	Utilisation en dehors de la zone géographique attendue ou contraire au profil attendu	Moyenne	Ceci est commun à l'ensemble des services financiers, mais les services mobiles présentent de meilleures mesures de détection grâce à l'existence de dispositifs de contrôle automatisés permettant de signaler et/ou bloquer toute activité anormale	Faible

	Typologie	Indicateur	Vulnérabilité	Mesures de gestion des risques et commentaires	Niveau de risque après gestion des risques
d.	Dépôt de fonds d'origine criminelle	Dépôts excessivement élevés, fréquents ou juste en dessous des limites	Faible	Les dispositifs de contrôles sont généralement en mesure de détecter ce genre d'anomalies. Les paiements mobiles présentent des risques moindres vis-à-vis de cette typologie compte tenu des faibles montants d'opération et de la détection possible de toute utilisation trop fréquente. Le risque pourrait augmenter dans le cas d'opérations régulières de montant plus élevé, mais serait détecté de la même manière que dans les services de paiement classiques.	Faible
e.	Utilisation de FOC pour faire des achats	Transactions anormalement élevées ou achats de biens/services sans logique économique	Faible	Les systèmes devront chercher à repérer ce type d'anomalie. Une fois de plus, les paiements mobiles présentent des risques moindres vis-à-vis de cette typologie compte tenu des faibles montants d'opération et de la détection possible de toute opération de montant inhabituel. Si des paiements de montant plus élevé devaient être régulièrement effectués, l'accent devrait être mis sur des systèmes permettant de détecter des transactions atypiques, sans logique économique apparente	Faible
f.	Transfert de FOC vers le compte de complices	Les transferts sont susceptibles d'être atypiques par rapport aux flux géographiques habituels. Montants et fréquences peuvent également être atypiques	Moyenne	Des dispositifs de détection des anomalies doivent être mis en place. Des plafonds sur les comptes peuvent également limiter les risques en poussant au fractionnement des opérations entre un grand nombre de comptes d'argent mobile.	Faible

	Typologie	Indicateur	Vulnérabilité	Mesures de gestion des risques et commentaires	Niveau de risque après gestion des risques
g.	Regroupement de FOC sur un seul compte	Toute activité de regroupement de fonds de multiples origines est anormale, sauf dans le cas d'un commerce de détail	Faible	Des dispositifs de détection des anomalies doivent être mis en place. La détection d'activités criminelles par le biais de ces dispositifs est facilitée par la mise en place de limites strictes sur les comptes. Ces limites peuvent également gêner ce genre d'activité en rendant nécessaire le fractionnement des FOC entre plusieurs comptes d'argent mobile.	Faible
h.	Retrait de FOC sous forme d'argent liquide	Montants anormalement élevés ou opérations anormalement fréquentes	Faible	Les retraits suspects sont détectables par les systèmes les plus simples. Les soldes de compte sont limités et ces limitations permettent de prévenir ce typ d'activité, en rendant nécessaire le fractionnement des FOC entre plusieurs comptes d'argent mobile, forçant ainsi les criminels à effectuer une multitude de retraits répétés et donc plus facilement repérables	Faible
i.	Virements en faveur ou en provenance de personnes ayant des liens avec le terrorisme	L'identité de l'utilisateur figure sur les listes de suspects nationales ou internationales	Faible	Le système a la capacité de repérer automatiquement les noms des personnes ayant des liens connus avec le terrorisme, et peut être programmé pour bloquer immédiatement et signaler toute transaction ayant un lien avec ces personnes. Il s'agit d'une méthode de dissuasion efficace.	Faible
2	**BC par les commerçants**				
a.	Complicité du commerçant pour le recyclage de FOC	(i) Procédure de vérification du commerçant, préliminaires ou ultérieures, l'existence de fraude, ou (ii) présence d'opérations inhabituelles pour ce type de commerce	Moyenne	L'obligation de vérification préalable (ou *due diligence*) est nécessaire, ainsi que des dispositifs de détection des comportements anormaux, recherchant les anomalies au niveau du commerçant ou pour la classe de commerçants en question.	Faible

	Typologie	Indicateur	Vulnérabilité	Mesures de gestion des risques et commentaires	Niveau de risque après gestion des risques
b.	Détournement de fonds par le commerçant	Les procédures de vérification du commerçant, préalables et régulières, visent à détecter ce genre d'incidents	Moyenne	Les risques de fraude ne peuvent être complètement éliminés, mais des mesures de vérification préalable adaptées et une surveillance attentive des opérations permettent de les réduire.	Faible
3	**BC par un agent ou détaillant partenaire**				
a.	Permet le dépôt ou le retrait de FOC connue	Les procédures de vérification préalables constituent un bon indicateur de risque. Elles peuvent être approfondies en fonction du niveau de risque	Élevée	Les agents ou les détaillants partenaires sont susceptibles de constituer le point faible de la chaîne des paiements et une attention particulière doit leur être apportée, incluant des procédures de vérification approfondies, un suivi permanent des opérations et des audits réguliers. Des « visites mystère » peuvent également être utilisées pour vérifier l'intégrité du fonctionnement des agents et autres partenaires.	Faible à modéré
b.	Le partenaire ne se conforme pas à ses obligations de verifications préalables, intentionnelle-ment ou par négligence	Idem	Élevée	Les agents ou les détaillants partenaires sont susceptibles d'être le point faible de la chaîne des paiements et une attention particulière doit leur être apportée, incluant des procédures de vérification approfondies, une surveillance permanente des opérations et des audits réguliers. Des « visites mystère » peuvent également être utilisées pour contrôler l'intégrité du fonctionnement des agents et autres partenaires.	Faible à modéré
c.	Le partenaire laisse les clients enfreindre les limites imposées sur les dépôts ou les retraits	Les systèmes ont la capacité de signaler immédiatement ce genre de situation	Moyenne	Les systèmes doivent prévenir ce genre de situation et enregistrer tout incident pour suivi ultérieur. Le prestataire peut également mettre en place des mesures de prévention des abus par les agents (utilisation de « visites mystère » par ex.)	Faible

	Typologie	Indicateur	Vulnérabilité	Mesures de gestion des risques et commentaires	Niveau de risque après gestion des risques
4	**BC par le biais des fonctionnalités transfrontalières**				
a.	Les FOC sont transférés hors des frontières par l'uilisation de multiples comptes	Fréquence et/ ou montants inhabituels en provenance ou à destination d'un même endroit	Moyenne	Les situations de collusion peuvent se manifester au travers des données relatives à un agent particulier, ainsi que par le montant ou la fréquence des transferts. Les systèmes peuvent se baser sur des références d'opérations habituelles, qui, combinées à des informations géographiques, peuvent permettre de fournir des données supplémentaires susceptibles de permettre le repérage des situations de collusion (par exemple, montants ou fréquences inhabituelles de transferts à destination ou en provenance d'un agent donné ou d'agents proches).	Faible
b.	FOC transférés par un individu isolé	Fréquence et/ ou montant inhabituel des virements	Moyenne	Tout blanchiment d'une somme significative serait difficile à effectuer sans s'éloigner du profil d'opération habituel pour ce genre de transfert.	Faible
c.	Transfert de fonds à des fins de financement du terrorisme	Origine ou destination des fonds inhabituelles. Destination répertoriée sur les listes ONU/GAFI ou les listings nationaux.	Moyenne	Les outils automatiques et instantanés de signalement et blocage facilitent la prévention des risques et réduisent l'intérêt de ce mode de transfert par rapport à d'autres méthodes de transfert de fonds.	Faible
5	Typologies en évolution	Les systèmes ont la capacité de détecter les comportements anormaux par rapport à des typologies standard pouvant inclure des références de montants, de volumes, ainsi que des paramètres géographiques, d'activité ou de profil des utilisateurs, etc.	Moyenne	Des dispositifs de détection des comportements atypiques doivent être mis en place pour pallier les risques permanents de BC. Compte tenu du faible montant des opérations effectuées, le risque global reste faible tant que les systèmes continuent de détecter les anomalies.	Faible

Annexe 6 : Récapitulatif des mesures de LAB/CFT les plus pertinentes pour les prestataires d'argent mobile

Recommandation du GAFI	Obligation	Comment se conformer et difficultés potentielles	Solutions
Mesures de vigilance			
Recommandation 5	(i) Interdiction des comptes anonymes ou ouverts sous des noms manifestement fictifs (ii) L'application de mesures de vérifications préalables (due diligence) lors de l'établissement de relations d'affaires ou de la qualification d'opérations ponctuelles, ainsi qu'en cas de suspicion de BC (iii) Identification et vérification de l'identité du titulaire du compte (iv) Obtention d'informations sur l'objet de la relation d'affaires (v) Vigilance constante pendant toute la durée de la relation d'affaires et examen attentif des transactions effectuées	Les comptes d'argent mobile sont généralement enregistrés sous le nom de l'utilisateur. La vérification de l'identité des clients est difficile dans les nombreux pays où une grande partie de la population de dispose pas de pièces d'identité. Ces comptes sont soumis à des limitations de montant et de fréquence des opérations, ce qui limite les possibilités de BC/FT par ce canal. L'application complète des MV dans des environnements de faibles risques représente néanmoins un énorme fardeau pour les prestataires d'argent mobile.	Il est important de distinguer le degré de MV nécessaires pour chaque catégorie d'utilisateurs (clients, agents, commerçants) étant donné que le niveau de risque varie en fonction des services utilisés. Des mesures de vérifications préalables complètes doivent être la norme pour les agents et les commerçants. Lorsque cela est possible, les documents nationaux d'identité du pays seront utilisés pour vérifier l'identité des clients. Lorsque l'identité des clients ne peut être vérifiée de façon conventionnelle, des mesures de vérification alternatives seront utilisées (par ex. lettres de référence ou facture de service public). Il existe cependant des cas dans lesquels des MV simplifiées ou allégées peuvent être appropriées compte tenu d'un niveau de risque limité. Par exemple, les risques peuvent être limités par la mise en place de limites sur les comptes et par une surveillance attentive des opérations. Voir R15
Recommandation 6	Mesures de vérifications préalables améliorées relatives aux personnes politiquement exposées (PPE)	L'ensemble des commerçants, agents et utilisateurs doivent être vérifiés contre les bases de données commerciales de PPE afin d'identifier celles-ci. Une fois les PPE identifiées, tout établissement d'une relation d'affaires devra être autorisé par la direction générale, qui devra exercer une vigilance accrue pendant toute la durée de la relation en fonction du niveau de risque. L'origine des fonds devra être identifiée et enregistrée.	

Recommandation du GAFI	Obligation	Comment se conformer et difficultés potentielles	Solutions
Recommandation 8	Risque d'anonymat découlant des nouvelles méthodes de paiement qui n'impliquent pas la présence physique des parties.	La présente analyse vise à adresser spécifiquement ces risques.	La présente méthodologie vise à faciliter l'évaluation et la prévention des risques. Il existe différentes manières de réduire significativement les risques dans les transactions sans présence physique des parties, comme par exemple un système de limite et de suivi d'activité des comptes.
Recommandation 9	Recours à des tierces parties réglementées pour l'exécution de certaines obligations relatives au devoir de vérification préalable. Définition des conditions relatives à la disponibilité des informations et à la surveillance de la tierce partie concernée.	Cette recommandation ne s'applique pas dans le cas d'accord contractuels au titre desquels l'agent s'engage à appliquer les MV pour l'institution financière. (Voir méthodologie du GAFI). Les agents sont habituellement sous contrat. Lorsqu'une institution financière s'appuie sur des données de l'opérateur en matière d'identification des clients, elle doit vérifier le processus et s'assurer que celui-ci est approprié et disponible immédiatement pour inspection. L'institution financière conserve au final l'entière responsabilité du processus complet d'identification du client.	
Recommandation spéciale VII	Inclusion des informations de la personne à l'origine du transfert d'argent afin de limiter les risques de FT et autres activités criminelles.	Cette recommandation s'applique aux transferts de montants élevés entre comptes de deux institutions financières différentes. Elle n'est pas applicable à la plupart des services domestiques d'argent mobile. Les transferts domestiques et internationaux excédant un certain montant (fixé par le GAFI à 1 000 US$) doivent contenir le nom du donneur d'ordre ainsi qu'un renseignement supplémentaire au minimum (adresse, date de naissance, numéro d'identité, etc). Il existe certaines exceptions définies par le GAFI pour les transferts domestiques.	Les mesures de prévention doivent être proportionnées au niveau de risque. Des transactions de montant plus élevé (à savoir de sommes ou fréquence élevées) peuvent présenter des risques plus élevés et donc nécessiter des mesures de connaissance de la clientèle renforcées.

Recommandation du GAFI	Obligation	Comment se conformer et difficultés potentielles	Solutions
Archivage des documents relatifs aux comptes et à la clientèle			
Recommandation 10	Archivage pendant cinq ans des données relatives aux transactions effectuées, et pendant cinq ans au moins après la fin de la relation d'affaires des données d'identification obtenues au titre des mesures de vérification préalable.	Cette recommandation s'applique dans tous les cas. Les opérateurs téléphoniques conservent généralement les données concernant leurs clients, mais pour une période plus brève (généralement un an pour les données relatives aux appels).	Les données financières, y compris les données d'identification relatives aux obligations de vigilance, doivent être conservées pendant cinq ans au moins, en conformité avec les normes du GAFI.
Recommandation 11	Les données relatives aux transactions complexes, de montant ou fréquence anormalement élevés doivent être conservées pendant cinq ans au moins, et rester à la disposition des autorités pour l'accomplissement de leur mission.	Les prestataires de services de paiement devraient pouvoir respecter facilement cette obligation, toutes les transactions et données étant enregistrées électroniquement.	
Déclaration d'opérations suspectes			
Recommandation 13	Déclaration des suspicions de BC ou FT auprès de la cellule de renseignements financiers (CRF).	L'ensemble des prestataires de services financiers mobiles, qu'il s'agisse des opérateurs de téléphonie mobile ou des banques, doit déclarer toute activité suspecte aux autorités compétentes.	
Recommandation 19	Déclaration des transactions supérieures à un certain montant.	Cette recommandation est sans objet dans la plupart des pays où les services d'argent mobile se sont développés. Les transactions habituelles sont de montant très faible, et les plafonds sur les soldes et opérations sont bien inférieurs au montant fixé par le GAFI. Cette question ne s'est manifestée qu'en Corée du Sud, où les utilisateurs ont la possibilité d'effectuer des opérations de montant élevé, mais dans le cadre de mesures de vigilance renforcées.	

Recommandation du GAFI	Obligation	Comment se conformer et difficultés potentielles	Solutions
Surveillance des activités des clients et formation des employés			
Recommandation 15	Dispositifs de contrôle et formation pour la dissuasion et la détection des vulnérabilités et des activités de BC.	Les prestataires de services financiers mobiles disposeront naturellement de systèmes informatiques sophistiqués pour le traitement des opérations de la clientèle.	
Réglementation et surveillance			
Recommandation 23	Mesures visant à empêcher les criminels d'occuper des positions au sein des institutions financières.	Les prestataires de services financiers mobiles se trouvent déjà sous la supervision des autorités réglementaires financières, que ce soit par le biais de partenariats avec des banques agréées ou via leur propre agrément en tant que prestataire de services de paiements ou d'argent électronique.	Le processus d'autorisation doit inclure une vérification des antécédents criminels éventuels de l'ensemble des postes de responsabilité.
Recommandation spéciale VI	Agrément/ autorisation d'exercerci pour les services de transferts de valeur afin de prévenir les activités de BC/FT.	Les prestataires de services financiers mobiles doivent être agrées par les autorités compétentes ou faire l'objet d'une autorisation d'exercer avant de pouvoir effectuer des opérations.	

Exemple d'évaluation des risques (cette évaluation n'est représentative de la situation d'aucun pays en particulier et n'est présenté qu'à titre d'exemple)

Facteurs		Impact sur les risques de BC/FT
Fonctionnalités de paiements	Transfert d'argent entre personnes	La possibilité pour les individus de recevoir et d'effectuer des paiements **entraîne des risques plus élevés**.
	De personne à commerçant	Les limitations sur les paiements effectués vers les commerçants, limitent le champ d'application et de ce fait **réduisent le risque**.
	Limitations sur le montant des paiements	**Réduisent le risque** par la mise en place de plafonds sur les paiements et d'un montant maximum limitant les montants susceptibles de faire l'objet de BC.
Caractéristiques du service	Faibles montants d'opération	**Réduisent le risque** étant donné que les opérations de faible montant limitent dans l'absolu les possibilités de BC.
	Usage occasionnel	**Réduit le risque**
	Dépôts et retraits d'espèces	**Augmentent le risque** compte tenu de la faible traçabilité des espèces.
	Services domestiques	**Réduit le risque** compte tenu de la facilité de suivi des mouvements d'argent à l'intérieur du pays.
	Services transfrontaliers	**Augmentent le risque** étant donné que les frontières constituent autant d'obstacles au suivi des mouvements d'argent.
	Paiements faits à la famille	Lorsqu'il s'agit de l'objet principal des services, l'utilisation des fonds peut être facilement reconnue et mesurée. Ils s'accompagnent donc de **risques moins élevés**.
Profil démographique de la clientèle	Faibles revenus	**Réduit le risque** compte tenu du faible montant ou de la faible fréquence des paiements effectués.
	Rurale	Les clients des zones rurales sont généralement connus dans leur communauté et sont moins en mesure de dissimuler leurs activités. **Réduit le risque.**
	Urbaine	**Augmente le risque** étant donné que les environnements urbains favorisent la dissimulation d'activités criminelles.
Infrastructures financières	Réseau d'agence dûment réglementé	**Réduit le risque** en facilitant l'emploi d'un personnel formé ayant une certaine connaissance des services financiers.
	Réseau informel peu réglementé	**Augmente le risque car il n'y a pas d'employés** ayant la formation nécessaire et une connaissance des services financiers.
Infrastructures d'identification officielle de la population	Bonne pénétration des systèmes publics de cartes d'identité	**Réduit le risque** en permettant leur utilisation pour la vérification de l'identité des clients.
	Absence de système public de cartes d'identité	**Augmente le risque**
Cadre réglementaire	Présent et appliqué	**Réduit le risque**
	Présent mais inégal ou disproportionné	**Augmente le risque**
	Inexistant	**Augmente le risque**

Les facteurs considérés ici n'ont pas vocation à être exhaustifs ou à servir de référence pour les risques relatifs aux paiements mobiles. Ils illustrent les types de questions qui doivent être examinées dans le cadre d'une analyse des risques, ainsi que les effets contradictoires susceptibles d'être rencontrés. (Il est également important de noter que cette liste est axée sur les services de paiement déployés dans les pays développement et à faibles revenus.)

Les facteurs de risques doivent être replacés dans un contexte approprié, permettant de bien comprendre les effets relatifs et leurs interactions en vue de l'évaluation du profil de risque général du service. La présente méthodologie se propose d'y parvenir par le biais de l'utilisation des typologies de blanchiment de capitaux (c'est-à-dire les scénarios connus ou prévisibles de blanchiment d'argent) comme référence pour l'évaluation des différents facteurs de risque.

Pour plus d'informations, contactez:

mmu@gsm.org

GSMA London Office

T +44 (0) 20 7356 0600