CGAP

NOTE

Services financiers mobiles : protéger les clients, les prestataires et le système de la fraude

L'expansion rapide des services financiers mobiles a sans doute contribué le plus au renforcement de l'inclusion financière dans les marchés émergents actuels. En effet, elle a favorisé l'accès du segment sans cesse croissant de la population autrefois non bancarisée à des services financiers moins chers et fiables. Des produits d'argent mobile innovants comme M-Pesa au Kenya et en Tanzanie se sont transformés en des moyens de paiement d'envergure par lesquels transitent des milliards de dollars chaque année. Malheureusement, les services financiers mobiles sont aussi devenus très vite des relais de la fraude et d'autres activités criminelles.

Divers types de fraudes sont observés sur des marchés clés de services financiers mobiles, parmi lesquels la fraude commise par des agents et des tiers à l'égard des clients, et la fraude perpétrée contre les agents. De plus, la fréquence de la fraude interne engendre des pertes économiques considérables pour les prestataires et affecte un nombre substantiel d'utilisateurs d'argent mobile dans ces marchés.

Les niveaux de fraude déclarés par les clients et les agents sont relativement élevés dans certains marchés – générant des pertes pour les utilisateurs, les agents et les prestataires de services financiers –, alors qu'ils sont plutôt bas dans d'autres. Ce qui donne à penser que même si la fraude peut être une préoccupation de premier plan, elle présente aussi un risque que l'on peut atténuer de façon efficace[1]. La peur ou le fait de subir des pertes attribuables à la fraude peut contribuer à freiner l'adoption et l'utilisation continue des services financiers mobiles par des clients peu nantis. Ces préoccupations peuvent aussi contribuer à restreindre la demande d'autres produits ne servant pas à effectuer des paiements, que les clients considèrent à la fois comme plus complexes et plus risqués.

L'incapacité à juguler la fraude interne et externe peut réduire les avantages perçus par les clients et les gains de l'inclusion financière dans ces marchés, et battre en brèche l'argument commercial des prestataires de services financiers. Par ailleurs, les organes de régulation peuvent être moins enclins à ouvrir l'espace nécessaire à l'innovation destinée à élargir et diversifier les services financiers mobiles, dans la mesure où ils considèrent que les contrôles internes des prestataires sont insuffisants pour déceler et atténuer la fraude. Par conséquent, les prestataires doivent mettre en place des systèmes de contrôle qui assurent un bon équilibre entre la gestion du risque et d'autres objectifs institutionnels[2].

En 2015, le CGAP a entrepris une étude approfondie de la fraude dans six marchés d'avant-garde pour les services financiers mobiles : Ghana, Kenya, Ouganda, Pakistan, Rwanda et Tanzanie. Cette étude s'appuyait sur des analyses de cas de fraude signalés par des clients et effectuées par les experts de la lutte contre la fraude et de la gestion des risques rencontrés dans le cadre des enquêtes du programme FII ; des discussions avec des responsables politiques sur les risques majeurs et les mesures correspondantes ; la cartographie des bonnes pratiques de détection et d'atténuation de la fraude ; et des ateliers et formations avec des professionnels du secteur et des responsables administratifs, dont certains organisés conjointement avec la GSMA (l'association mondiale du secteur du mobile). Cette note présente les principales conclusions et recommandations issues de ce travail de recherche. Elle met en exergue plusieurs facteurs importants de vulnérabilité ainsi que des stratégies à appliquer par les prestataires de services financiers et les responsables politiques pour lutter contre les risques de fraude et atténuer le préjudice que pourraient subir les utilisateurs, les agents et les entreprises de prestation de services financiers.

Fraude dans les services financiers mobiles : facteurs de risque et de vulnérabilité

Avant de pouvoir appliquer des solutions efficaces, il faut analyser les facteurs qui rendent les services d'argent mobile vulnérables à la fraude et aux activités de blanchiment de capitaux, ainsi que les divers types de fraude correspondants.[3]

Les principaux facteurs et indicateurs de risque de fraude à l'argent mobile sont, entre autres :

- **Risque lié au produit.** Alors que sa vitesse, sa portabilité et sa sécurité font de l'argent mobile un service privilégié dans les marchés émergents, ces mêmes qualités font qu'il est un moyen privilégié d'exécution rapide de fraudes et d'escroqueries. L'avènement de nouveaux services financiers mobiles, y compris les paiements de gros montants, l'assurance, l'épargne et le crédit mobiles, les cartes prépayées et les services de transfert d'argent transfrontière et international, peut créer des opportunités de fraude.
- **Risque lié au canal.** Ce risque découle du caractère ubique des téléphones portables et de la mesure dans laquelle de nouveaux utilisateurs moins expérimentés intègrent le marché à travers ce canal.
- **Risque lié aux agents.** Les prestataires disposant d'un vaste réseau d'agents ont du mal à bâtir l'infrastructure et les systèmes qui conviennent pour assurer efficacement le contrôle des agents et la surveillance des infractions, particulièrement dans les zones reculées.
- **Risque lié au client et risque de non-conformité.** Les pays dotés d'une importante population non bancarisée, illettrée et/ou rurale, qui ne possèdent pas un système national d'identification, ont du mal à accomplir les diligences nécessaires pour connaître la clientèle et surveiller les activités criminelles, surtout parce que les contrôles d'identité des clients sont souvent effectués en première ligne par des agents plutôt que par le personnel des agences.
- **Risque lié au système et aux prestations.** Les périodes d'indisponibilité du système peuvent générer des retards dans la prestation des services et créer des opportunités de fraude. Des commandes de système et d'accès déficientes peuvent aussi faciliter les violations des droits d'accès et ouvrir la porte à la fraude. Le manque de systèmes automatisés de lutte contre la fraude empêche une surveillance globale des transactions permettant de détecter des actes frauduleux et des activités terroristes, ainsi que l'imposition de sanctions appropriées.

1 Les questionnaires d'enquêtes du programme *Intermedia Financial Inclusion Insight* — FII — (http://finclusion.org/) contiennent plusieurs questions relatives à la fraude perpétrée à l'endroit des clients par des agents, qui a une incidence variable selon les marchés. Ces enquêtes montrent comment les risques de fraude peuvent affecter différemment chaque marché de services financiers mobiles. Par exemple, les participants à l'enquête de 2014 ont fait état de la surfacturation par les agents ou des frais excessifs imposés pour des dépôts en Ouganda (11 %), de faibles niveaux de fraude au Rwanda voisin (1 %) et au Pakistan (1 %), et d'une incidence modérée de la fraude en Tanzanie (5 %). En outre, les données d'enquêtes du programme FII laissent entrevoir une plus forte prévalence de la fraude commise par des agents à l'égard des clients en Ouganda et en Tanzanie — 5 % en moyenne — qu'au Kenya où la fréquence moyenne de tels actes est bien plus faible — 2 %. Voir également la figure 1.

2 Voir également Mudiri (n.d.).

3 La fraude étant une infraction sous-jacente du délit de blanchiment de capitaux, une discussion sur les risques de fraude et les contrôles connexes doit aborder en même temps les mesures de prévention du blanchiment de capitaux et des activités criminelles associées.

Avril 2017

- **Risque lié à la réglementation, la supervision et l'application des règles.** Sur ces marchés, le cadre réglementaire des services d'argent mobile n'est pas suffisamment rigoureux, ce qui peut donner lieu à une prolifération d'agences de transfert d'argent non agréées ou de produits non réglementés, qui à leur tour favorisent la fraude, le blanchiment de capitaux et d'autres activités criminelles.

Nouveaux modes et types de fraude

Les caractéristiques particulières et les facteurs de risque relevés ci-dessus sont tels que les types de fraude en vogue dans les services financiers mobiles sont distincts de ceux observés dans les services bancaires classiques. Globalement, on peut regrouper les types de fraude selon qu'ils affectent les clients, les agents et les prestataires.

Fraude affectant les clients

Les types de fraude perpétrés à l'encontre des clients varient d'un marché à l'autre. Par exemple, les principales préoccupations concernant la fraude à l'égard des clients signalées par les prestataires de services financiers mobiles au Rwanda et en Ouganda étaient les suivantes :

- le vol d'identité résultant d'une permutation frauduleuse/hors-réseau de cartes SIM au moyen duquel le compte mobile rattaché à la carte SIM d'un client est transféré sur la carte SIM du fraudeur, de sorte que ce dernier peut accéder au porte-monnaie mobile et au compte bancaire dudit client.
- les fausses promotions, le hameçonnage ou les escroqueries basées sur des techniques d'ingénierie sociale, par lesquelles les fraudeurs se font passer pour les prestataires et informent les clients qu'ils ont gagné un prix dans le cadre d'une campagne de promotion, en leur demandant d'envoyer de l'argent aux numéros des fraudeurs pour rentrer en possession dudit prix.
- les périodes d'interruption du réseau, qui peuvent créer des opportunités de fraude, surtout à travers la permutation de SIM hors-ligne et des transactions de gré à gré ne pouvant être vérifiées et rapprochées que plus tard, lorsque la connexion est rétablie[4].
- les agents qui demandent au client leur numéro d'identification personnel (PIN). Même lorsqu'une telle demande ne vise pas nécessairement à escroquer les clients, elle expose davantage ces derniers à des risques de fraude.
- les agents qui escroquent les clients, surtout dans le cadre de transactions de gré à gré, notamment en surfacturant des transactions comme les dépôts directs ou en imposant des frais pour des dépôts ordinaires qui ne sont généralement pas facturés[5].
- l'usurpation de l'identité du prestataire par les fraudeurs, qui appellent les clients en prétendant représenter le prestataire et peuvent les amener à révéler leur PIN ou d'autres renseignements personnels associés à leurs comptes d'argent mobile, lesquels peuvent servir à les escroquer.
- les pertes attribuables à des transferts effectués par erreur au profit de bénéficiaires involontaires qui refusent de rétrocéder l'argent reçu.

Les enquêtes du programme FII révèlent que le type de fraude le plus répandu concerne des agents qui demandent les codes PIN des clients (bien que cela ne soit pas nécessairement dans le but de les escroquer), suivi du cas des agents qui surfacturent des transactions comme les dépôts directs (ces dépôts étant illégaux dans bon nombre de pays) ou imposent des frais pour des dépôts ordinaires qui ne sont généralement pas facturés[6]. Il faut noter que les interruptions de réseau étaient la préoccupation la plus souvent citée, notamment par 50 % en moyenne des clients interrogés.

En dépit de la prévalence relativement élevée d'actes frauduleux ou d'autres problèmes affectant les clients, en moyenne, seuls 11 % des clients de services financiers mobiles ayant rencontré des difficultés liées à l'utilisation de l'argent mobile les ont signalées via des mécanismes de plainte formels comme des centres de service-client[7]. Cela s'explique principalement par l'inefficacité des moyens de recours des prestataires ou le manque d'informations sur lesdits moyens. Dans certains cas, les clients effectuant des transactions de gré à gré semblent moins enclins à utiliser les mécanismes de plainte formels que les utilisateurs de porte-monnaie mobile (Mazer et Garg, 2015). Ce qui fait qu'il est extrêmement difficile pour les prestataires de services financiers d'avoir une image complète des niveaux de fraude commise sur leur réseau et de prendre des mesures à l'effet de sanctionner les auteurs d'actes frauduleux visant les clients ou de prévenir de tels actes.

Fraude affectant les agents

Les agents et les prestataires de services financiers mobiles sont aussi exposés à la fraude. Les enquêtes réalisées par *Helix Institute of Digital Finance* sur les facteurs de développement accéléré des réseaux d'agents ont démontré que 53 et 42 % des agents de services financiers mobiles en Ouganda et en Tanzanie, respectivement, ont été victimes de fraude l'année précédente (Khan et Bersudskaya, 2016). La proportion d'actes frauduleux et criminels enregistrée par les agents de services d'argent mobile en Ouganda était la plus élevée de la région (Bersudskaya et Kuijpers, 2016). Les fraudes affectant communément les agents sont surtout les déficits de fonds par suite d'un emploi non autorisé, la compromission de codes PIN et les escroqueries fondées sur l'usurpation de l'identité de membres du personnel des opérateurs de réseaux mobiles par des fraudeurs qui parviennent ainsi à accéder sans autorisation au fonds de caisse de l'agent. Les clients peuvent aussi commettre des fraudes au préjudice des agents — qui prennent alors la forme d'annulations frauduleuses de retraits[8] ou de dépôts de fausses monnaies. Les enquêtes réalisées par *Helix Institute* en 2015 indiquent que la fraude est la principale préoccupation de nombreux agents. C'est le cas surtout dans les marchés d'Afrique de l'Est, comme l'illustre la figure 1.

Fraude interne aux prestataires de services d'argent mobile

La fraude interne aux prestataires pose aussi problème. Plusieurs affaires célèbres de fraude interne ont engendré des pertes considérables pour les prestataires de services financiers mobiles, tout en compromettant les comptes des utilisateurs et en remettant en cause l'intégrité financière du système. Par exemple, MTN, le plus grand opérateur d'argent mobile d'Ouganda, a perdu un montant estimé à 3,4 millions de dollars par suite d'actes frauduleux perpétrés par des membres de son personnel en 2011 (Morawczynski, 2015), alors qu'un incident semblable a coûté à Tigo, au Rwanda, un montant estimé à 700 000 dollars en 2014 (Mugisha, 2014). Des contrôles internes insuffisants (favorisant le piratage des données internes), des procédures de vérification inadéquates, des structures de gouvernance interne déficientes, l'absence de sensibilisation des employés à la fraude et le manque de mécanismes de dénonciation sont autant de facteurs qui contribuent largement à la fraude interne.

4 Les transactions de gré à gré désignent des transactions dans le cadre desquelles l'agent prend l'argent d'un client et effectue directement la transaction demandée au lieu de charger l'argent sur le porte-monnaie mobile du client.

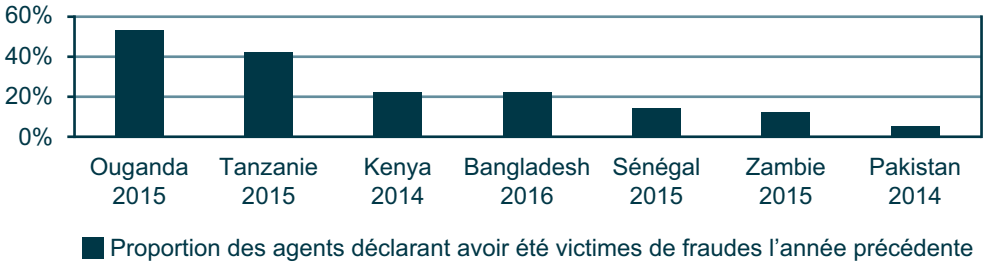
5 Les dépôts directs sont des transactions de gré à gré dans le cadre desquels les agents déposent directement de l'argent dans le porte-monnaie d'un tiers, normalement sur instructions du client. Les dépôts directs sont illégaux dans plusieurs pays parce qu'ils contreviennent aux règles de vérification de l'identité des clients et peuvent favoriser le blanchiment d'argent.

6 Enquêtes du programme FII (2014) dans les pays suivants : Ghana, Kenya, Rwanda et Ouganda (http://finclusion.org/).

7 Étude qualitative de la clientèle réalisée par le CGAP au Bangladesh, en Colombie et en Ouganda, selon McKee, Kaffenberger et Zimmerman (2015).

8 On parle d'annulations frauduleuses de retraits lorsqu'un client demande au prestataire d'annuler immédiatement un retrait effectué au motif que le destinataire n'a pas reçu les fonds concernés de l'agent.

Figure 1. Proportion des agents déclarant avoir été victimes de fraudes l'année précédente



Source: Bersudskaya et Kuijpers 2016.

Contrôles permettant d'atténuer les risques de fraude dans les services financiers mobiles[9]

Mesures à la disposition des prestataires

Les prestataires peuvent prendre des mesures particulières pour réduire la probabilité que se produisent certaines des formes de fraude les plus répandues, les surveiller lorsqu'elles surviennent et en gérer les conséquences[10]. Ces mesures sont, entre autres :

- des programmes intégrés de lutte contre la fraude, y compris des systèmes automatisés de contrôle des transactions et d'imposition de sanctions d'un bon rapport coût-efficacité, pour faciliter la détection rapide et la prévention de la fraude et d'autres activités douteuses comme les activités terroristes.
- le renforcement des programmes de surveillance de la conformité et de recrutement, formation et gestion des agents pour assurer le respect des procédures établies – aussi bien par la haute hiérarchie que par le personnel de terrain – et réduire les risques de fraude interne et externe.
- l'intégration de critères d'évaluation des risques dans chaque programme de gestion des risques liés aux services financiers mobiles de sorte que tous les risques soient répertoriés et atténués comme il se doit à l'aide de dispositifs de contrôle appropriés (renseignements exigés pour connaître la clientèle, sensibilisation des utilisateurs, normes de sauvegarde systémiques, etc.) avant le lancement de nouveaux produits financiers mobiles pouvant générer des risques supplémentaires. Les types de risques concernés sont généralement le vol et l'arnaque par hameçonnage qui favorisent l'usurpation d'identité et des fraudes semblables.
- des programmes complets de sensibilisation à la fraude et de prévention de ce phénomène mis en œuvre par les prestataires pour sensibiliser les clients, le personnel et les agents à l'évolution des techniques de fraude et aux mesures de prévention de cette dernière. Il peut s'agir de formations, de campagnes d'information et de bulletins périodiques transmis par courriel ou par SMS, de normes de sauvegarde systémiques pour prévenir la compromission de codes PIN et d'actions menées de concert avec des organismes de maintien de l'ordre pour l'instruction et la poursuite des affaires de fraude.
- la sensibilisation permanente des clients aux nouveaux types de fraudes et d'arnaques apparaissant sur le marché. L'accent devrait être mis sur les moyens par lesquels les clients peuvent se protéger, comme garder leurs codes PIN secrets et consulter leurs soldes avant de rétrocéder de l'argent qui leur aurait prétendument été envoyé par erreur.
- des mesures de prévention d'actes frauduleux perpétrés par des agents, y compris la formation, le contrôle de conformité, des programmes de sensibilisation et des normes de sauvegarde systémiques imposant des restrictions à l'utilisation des terminaux.
- la mise à disposition de services efficaces de gestion des plaintes dotés de personnels formés à faire face à la fraude et à d'autres griefs, ainsi que la mise en place de voies de recours dédiées pour les agents. Des moyens de recours efficaces permettent de rassurer les utilisateurs de nouveaux services financiers sur les mesures en place pour protéger leur argent et sur leur capacité à résoudre les problèmes qu'ils seraient amenés à rencontrer (Mazer et Garg, 2016).
- des procédures efficaces de recrutement du personnel qui incluent des enquêtes de moralité.
- la promotion d'une culture de probité, la formation continue du personnel et l'application de mesures disciplinaires.
- l'application de contrôles techniques qui limitent les droits d'accès des utilisateurs et imposent des contrôles binaires.

En plus de lutter contre la fraude dans leurs propres réseaux, les prestataires de services financiers mobiles doivent mener une action coordonnée à l'échelle du secteur tout entier pour juguler ce phénomène. Les fraudeurs utilisent souvent des tactiques semblables d'un réseau d'argent mobile à l'autre, et les clients présentent les mêmes points faibles quel que soit le prestataire choisi (dans de nombreux marchés, les clients utilisent généralement de multiples prestataires d'argent mobile). Par exemple, les associations professionnelles pourraient se charger de surveiller les tendances en matière de fraude et de promouvoir le partage mutuel d'informations sur lesdites tendances, ainsi que sur les meilleures méthodes de gestion prudente des risques de fraude[11]. Ces solutions ont obtenu d'excellents résultats dans la plupart des pays africains où existent de solides associations bancaires, et dans des pays comme l'Ouganda et le Zimbabwe qui possèdent des associations d'agents de services financiers mobiles. Cependant, ce dernier type d'association n'existe pas dans tous les pays. Par ailleurs, lorsqu'elles font office d'intermédiaire de services financiers mobiles, les banques n'accordent pas une place prioritaire auxdits services.

Surveillance réglementaire

L'absence de dispositifs réglementaires et d'organes de supervision appropriés peut créer des opportunités de fraude. Le manque d'un cadre réglementaire porteur peut aussi brider l'innovation, ce qui signifie que les prestataires ne seront pas en mesure de lancer de nouveaux produits faute de réglementations appropriées. Ce vide réglementaire est davantage exacerbé par la mauvaise formation et le manque d'équipements des agents de maintien de l'ordre, ce qui donne lieu à des retards dans l'instruction et la résolution des affaires de fraude.

Dans de telles circonstances, les instances de régulation doivent engager des réformes appropriées, y compris :

9 Les prestataires des pays étudiés qui ont appliqué les mesures de contrôle ci-après affichent de bons résultats. Au Kenya par exemple, la fonction de *Hakikisha* (vérification) sur M-Pesa a considérablement réduit la fréquence des transferts erronés. En Tanzanie, les périodes d'inaccessibilité d'un compte d'argent mobile après une permutation de SIM ont réduit le nombre d'incidences d'actes frauduleux de cette nature. Les fraudes au préjudice des agents sont combattues dans les marchés d'Afrique de l'Est par l'imposition de restrictions aux terminaux des agents, comme l'obstruction des appels et messages-textes provenant de numéros n'appartenant pas au prestataire. Au Cambodge, la formation des agents à la fraude permet à ces derniers de détecter et prévenir les formes d'escroquerie faisant appel à l'ingénierie sociale.

10 Voir également Buku (2012).

11 Conclusions des études menées par le CGAP au Ghana, au Kenya, au Rwanda, en Tanzanie et en Ouganda.

- l'adoption de textes législatifs appropriés qui confèrent un caractère obligatoire aux contrôles visant à atténuer les risques de fraude et garantissent l'application en bonne et due forme desdits contrôles par les prestataires. La récente promulgation de règlements en matière d'argent mobile et de monnaie électronique dans plusieurs grands marchés comme l'Afrique de l'Ouest, l'Afrique de l'Est et l'Asie du Sud a permis de formaliser ce secteur et de doter les organismes de contrôle des outils nécessaires pour appliquer et administrer des mesures plus robustes de surveillance de la fraude et d'atténuation des risques[12].
- un dialogue continu entre les groupes de défense des consommateurs et les organismes de promotion de l'inclusion financière d'une part et les organes de régulation d'autre part, afin d'apporter à ces derniers l'appui nécessaire à la réalisation des réformes législatives, le cas échéant. Cela est particulièrement important dans les pays où des dispositifs réglementaires propices à ce secteur d'activité ne sont pas encore en place.
- des réglementations portant agrément et supervision des prestataires de services financiers mobiles ; relatives à l'application de mesures obligatoires de protection des consommateurs afin de juguler la fraude ; et visant à atténuer d'autres difficultés rencontrées par les clients de services financiers mobiles comme des moyens de communication et de recours déficients et des pratiques déloyales appliquées par les prestataires. Un exemple typique est celui du Ghana où les réglementations portant sur les paiements électroniques adoptées en 2015 comportent des dispositions spécifiques à cet égard (Bank of Ghana, 2015, Section 26-28).
- la coordination transfrontière de la lutte contre la fraude dans les régions comportant des marchés multiples où l'utilisation de l'argent mobile est largement répandue. À titre d'exemple, on peut citer les efforts déployés par la Communauté d'Afrique de l'Est pour mettre en place un cadre commun d'enregistrement des cartes SIM dans le but exprès de contenir la fraude à l'argent mobile (Business Daily, 2015).

Conclusion

L'espace de l'argent mobile ne cesse de s'élargir. À mesure qu'un plus grand nombre d'acteurs intègre l'arène des services financiers mobiles et que de nouveaux produits sont offerts, les prestataires devront s'employer à travailler de concert et il faudra alors probablement adopter les réglementations qui conviennent. Les efforts visant à documenter et normaliser les solutions efficaces de lutte contre la fraude et de gestion des risques peuvent accélérer le développement d'approches cohérentes et efficaces dans tous les services financiers mobiles à travers le monde.

Cette note traite de la façon dont la fraude affecte les prestataires, les agents et les utilisateurs de services financiers mobiles, ainsi que les efforts déployés pour atténuer les vulnérabilités et les risques associés à la fraude dans les services d'argent mobile et d'autres prestations connexes. S'il n'est pas possible d'éradiquer complètement la fraude de tout service, argent mobile compris, les exemples présentés ici montrent que la fraude est un problème majeur dans plusieurs marchés importants pour les utilisateurs et les agents, et qu'il existe de simples mesures que les prestataires peuvent appliquer pour réduire leur vulnérabilité aux formes de fraude habituelles.

Parmi ces mesures, on peut citer : l'amélioration des contrôles internes, le renforcement de la capacité des agents à se protéger et à protéger leurs clients, et la révision de procédures comme l'accès aux comptes et la permutation des SIM, le cas échéant, pour prévenir des méthodes courantes de fraude. Avec le lancement de nouveaux produits et modes de prestation, les techniques de fraude vont continuer à évoluer. Cela signifie que des mécanismes de surveillance comme les contrôles de conformité et les dispositifs de retour des clients resteront des éléments essentiels pour lutter efficacement contre ce phénomène et réduire les risques. Les prestataires doivent partager les expériences réussies avec leurs pairs, afin que tous adoptent de bonnes pratiques et mènent des actions collectives au besoin. Il existe déjà des plateformes de communication entre des organisations nationales comme les associations de prestataires de services d'argent mobile. Ce partage d'expériences et de pratiques optimales va profiter à la communauté tout entière de prestataires de services financiers.

Les pouvoirs publics, les bailleurs de fonds et les partenaires de développement doivent continuer à soutenir les prestataires de services financiers et d'autres, comme les organismes de maintien de l'ordre, à travers des programmes d'assistance technique (sur des solutions d'infrastructures par exemple) et de renforcement des capacités. Le secteur des services financiers mobiles a certes mis au point un éventail de solutions de lutte contre la fraude, mais de nombreux responsables politiques restent à la traine car ne disposant pas de cadres réglementaires ou d'outils d'évaluation des risques adaptés à ces services. À l'avenir, les responsables politiques doivent participer davantage aux initiatives menées par le secteur pour réduire la fraude et, si possible, formaliser les bonnes pratiques en des prescriptions communes applicables aux prestataires de services financiers mobiles. Une confiance et un niveau d'utilisation accrus, la diversification des produits et la réduction des pertes pour les utilisateurs, les agents et les prestataires auront d'énormes effets positifs sur les services financiers mobiles, le bien-être des utilisateurs et la rentabilité des prestataires.

Références

Bank of Ghana. 2015. « Guidelines for E-Money Issuers in Ghana. » Bank of Ghana. https://www.bog.gov.gh/privatecontent/Banking/E-MONEYX20GUIDELINES-29-06-2015-UPDATED5.pdf

Bersudskaya, Vera, and Dorieke Kuijpers. 2016. « Agent Network Accelerator Survey: Uganda Country Report 2015. » Helix. http://www.helix-institute.com/data-and-insights/agent-network-accelerator-survey-uganda-country-report-2015

Buku, Mercy W. 2012. « Mobile Money: Balancing Financial Integrity with Business Expediency. » Blog post, 16 September. http://www.acamstoday.org/mobile-money/

Business Daily. 2015. « EAC Members Move to Tame Mobile Money Fraud." Business Daily, 24 September. http://www.businessdailyafrica.com/-/539546/2884060/-/12l92dtz/-/index.html

Khan, Maha, and Vera Bersudskaya. 2016. "Working Together to Fight DFS Fraud. » Blog post, 7 November. http://www.helix-institute.com/blog/working-together-fight-dfs-fraud

Mazer, Rafe, and Nitin Garg. 2015. « Recourse in Digital Financial Services: Opportunities for Innovation. » Brief. Washington, D.C. : CGAP.

_____. 2016. « Improving Recourse Systems in Digital Financial Services. » Blog post, 14 March. http://www.cgap.org/blog/improving-recourse-systems-digital-financial-services

McKee, Katharine, Michelle Kaffenberger, and Jamie M. Zimmerman. 2015. « Doing Digital Finance Right: The Case for Stronger Mitigation on Customer Risks. » Focus Note 103. Washington, D.C. : CGAP.

Morawczynski, Olga. 2015. « Fraud in Uganda: How Millions Were Lost to Internal Collusion. » Blog post, 11 March. http://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion

Mudiri, Joseck Luminzu. n.d. « Fraud in Mobile Financial Services. » Hyderabad : MicroSave. http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf

Mugisha, Ivan R. 2014. « Two Men Arrested for Allegedly Defrauding Rwf495m from Tigo. » Blog post, 20 November. http://www.newtimes.co.rw/section/article/2014-11-20/183244/

12 Le Kenya, la Tanzanie, le Ghana, le Bangladesh et l'Inde se sont dotés de législations relatives aux moyens de paiement électroniques

AUTEURS :
Mercy W. Buku et Rafe Mazer

CGAP

Avril **2017**

Toutes les publications du CGAP sont disponibles sur son site www.cgap.org.

CGAP
1818 H Street, NW
MSN IS7-700
Washington, DC
20433 USA

Tél. : 202-473-9594
Télécopie :
202-522-3744

Courriel :
cgap@worldbank.org