Code de conduite des prestataires de service d'argent mobile

VERSION 2 - OCTOBRE 2015

Introduction

Le présent code de conduite a pour objet d'identifier des principes applicables aux prestataires d'argent mobile[1] en vue d'encourager l'adoption par ceux-ci de pratiques cohérentes de prévention des risques dans certains domaines essentiels de leur activité.

Pour que le secteur de l'argent mobile continue de stimuler le développement de l'écosystème financier numérique, les prestataires de services d'argent mobile (les « prestataires ») ont adopté un code de conduite qui vise à s'assurer que leur services soient solides, que le canal soit sûr et que le client soit traité de façon équitable. Ce code de conduite soutiendra la poursuite de la croissance du secteur :

- En améliorant la qualité des services et la satisfaction des clients ;
- En facilitant la mise en œuvre de partenariats de confiance ;
- En établissant des rapports de confiance avec les autorités réglementaires qui favorisent la mise en œuvre de normes réglementaires adaptées et proportionnées.

Les prestataires qui adhèrent au code formalisent leur engagement à l'égard de huit principes se rattachant à trois domaines d'importance primordiale :

i. Solidité des services;
ii. Sécurité des réseaux et canaux mobiles ;
iii. Traitement équitable des clients.

En adoptant ce code, les prestataires s'engagent à[2] :

1. Protéger les fonds des clients contre le risque de perte ;
2. Utiliser des mécanismes efficaces de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
3. Équiper et surveiller leur personnel, leurs agents et les entités leur fournissant des services en sous-traitance pour s'assurer de la sûreté et de la fiabilité des services fournis ;
4. Fournir un service fiable avec une capacité adéquate en termes de système et de réseau ;
5. Prendre des mesures solides pour garantir la sécurité des réseaux et canaux mobiles ;
6. Fournir des informations claires, adéquates et opportunes pour que les clients puissent prendre des décisions en connaissance de cause ;
7. Mettre en place des mécanismes permettant de s'assurer que les réclamations soient correctement traitées et que les problèmes soient résolus dans les meilleurs délais ;
8. Respecter des pratiques appropriées de protection de la confidentialité des données lors de la collecte, du traitement et/ou de la transmission des données personnelles des clients.

1. Voir en annexe la définition de l'argent mobile aux fins du présent document.
2. Dans de nombreux pays, les lois et réglementations locales couvrent tout ou partie des aspects mentionnés dans ces principes. Le présent code de conduite identifie certaines bonnes pratiques que les prestataires devraient respecter, que ces pratiques soient imposées ou non par la réglementation locale. Ce code n'affecte pas l'obligation des prestataires de se conformer aux exigences réglementaires locales. De la même manière, il n'a pas vocation à limiter ou affecter de toute autre manière les droits contractuels des prestataires.

REMARQUE CONCERNANT LES RÉVISIONS DE LA VERSION 2

Les amendements suivants ont été effectués en vue de simplifier le code tout en assurant une couverture complète de tous les sujets pertinents :

- Modification des alinéas des principes 1, 3, 4 et 5 ;
- Reformulation du principe 8 afin de clarifier le fait qu'il porte sur le respect de la confidentialité des données et non sur la sécurité de celles-ci. Les alinéas correspondants ne sont pas modifiés.
- Les principes 2, 6 et 7 ne sont pas modifiés.

Principes

Principe 1 : Les prestataires de services d'argent mobile (les « prestataires ») protègent les fonds des clients contre le risque de perte.

1.1 Protection contre les pertes résultant de la défaillance d'une banque, d'un prestataire ou d'une autre partie

1.1.1 Les prestataires doivent s'assurer que des sommes égales au montant total des engagements financiers correspondant à l'argent mobile en circulation soient conservées sur un ou plusieurs comptes de garde pour le compte des utilisateurs de l'argent mobile (les « utilisateurs »).

1.1.2 Les prestataires doivent veiller à ce que les fonds des utilisateurs soient isolés de tout autre actif afin d'empêcher leur saisie par les créanciers en cas d'insolvabilité du prestataire.

1.1.3 Les prestataires doivent prendre des mesures de prévention du risque de perte de ces sommes en cas d'insolvabilité de la banque, de l'émetteur obligataire ou de toute autre entité auprès de laquelle des sommes sont investies.

1.2 Protection contre le risque de règlement

1.2.1 Dans la mesure du possible, les prestataires n'autorisent que les opérations de client dans lesquelles le débit et le crédit des comptes d'argent mobile s'effectuent en temps réel.

1.2.1 Les prestataires doivent régulièrement effectuer un rapprochement des transactions et régler leurs soldes auprès de leurs partenaires de l'écosystème financier.[3]

3. Aux fins du présent code, les « partenaires de l'écosystème financier » désignent les entités connectées au service d'argent mobile dans le but de fournir un service financier. Cela comprend par exemple, sans s'y limiter, les banques (banques dépositaires et autres établissements financiers détenteurs de comptes), les entités émettant ou recevant des paiements groupés, les agrégateurs, les commerçants utilisant des terminaux de point de vente, les prestataires de GAB et autres prestataires de services de paiement (nationaux ou internationaux). Ces entités sont généralement connectées au service d'argent mobile par le biais d'interfaces de programmation d'application (API).

Principe 2 : Les prestataires disposent de mécanismes efficaces, proportionnés et adaptés au niveau de risque pour la prévention, la détection et le signalement de tout usage abusif des services à des fins de blanchiment de capitaux ou de financement du terrorisme

2.1 Politiques et procédures efficaces

2.1.1 Les prestataires doivent élaborer des politiques et procédures efficaces pour lutter contre le blanchiment de capitaux et le financement du terrorisme.

2.2 Engagement de la direction générale

2.2.1 La direction générale doit manifester son engagement à l'égard de la lutte contre le blanchiment de capitaux et le financement du terrorisme à travers une surveillance adaptée.

2.3 Responsable désigné pour la lutte contre le blanchiment de capitaux et le financement du terrorisme

2.3.1 Les prestataires doivent nommer une personne qualifiée chargée d'assurer la promotion et la surveillance du respect des règles de lutte contre le blanchiment de capitaux et le financement du terrorisme.

2.4 Logiciel de surveillance des transactions

2.4.1 Les prestataires doivent mettre en place un système de surveillance des transactions pour la lutte contre le blanchiment de capitaux et le financement du terrorisme.

2.5 Obligations de connaissance des clients (KYC) et plafonds d'opération et de solde de compte

2.5.1 Les prestataires doivent dûment vérifier l'identité des clients et peuvent utiliser une méthode de vérification adaptée au niveau de risque si les lois et réglementations locales les y autorisent.

2.5.2 Les prestataires doivent appliquer des plafonds appropriés d'opération et de solde de compte en fonction du niveau de risque et des exigences de vérification de l'identité des clients.

2.5.3 Les prestataires doivent pouvoir bloquer les opérations des comptes dans certaines circonstances.

2.5.4 Les prestataires doivent passer tous les comptes au crible des listes nationales et internationales de surveillance, de sanctions, de blanchiment de capitaux et de financement du terrorisme.

2.6 Procédures de formation du personnel et des agents à la lutte contre le blanchiment de capitaux et le financement du terrorisme

2.6.1 Les prestataires doivent veiller à ce que leur personnel et leurs agents soient correctement formés aux procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme.

2.6.2 Les prestataires doivent veiller à ce que leur personnel et leurs agents respectent les procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme.

2.6.3 Les prestataires doivent élaborer des politiques et des processus clairs de réponse aux violations des règles de lutte contre le blanchiment de capitaux et le financement du terrorisme par leur personnel ou leurs agents.

Principe 3 : Les prestataires sélectionnent, forment et surveillent leur personnel, leurs agents et leurs sous-traitants pour s'assurer que ceux-ci offrent des services sûrs et fiables et se conforment à toutes les exigences réglementaires et opérationnelles applicables.

3.1 Politiques et procédures de vérifications préalables

3.1.1 Les prestataires doivent effectuer des vérifications préalables appropriées concernant leur personnel, leurs agents et les entités offrant des services de sous-traitance.

3.2 Formation

3.2.1 Les prestataires doivent mettre en place des programmes de formation de leur personnel et de leurs agents.

3.3 Accords contractuels

3.3.1 Les prestataires doivent mettre en place des accords écrits régissant leurs relations avec les agents et les entités fournissant des services en sous-traitance.

3.3.2 Les prestataires doivent assumer la responsabilité des actions effectuées en leur nom par leurs agents (et sous-agents éventuels) dans le cadre du contrat prestataire-agent.

3.4 Gestion et surveillance

3.4.1 Les prestataires doivent mettre en place des politiques et des procédures pour la gestion et la surveillance dans le temps de leur personnel, de leurs agents et des entités fournissant des services de sous-traitance.

Principe 4 : Les prestataires disposent de politiques et processus bien définis et d'une capacité suffisante en termes de système et de réseau pour garantir une prestation de service fiable.

4.1 Surveillance par le conseil d'administration et la direction générale

4.1.1 Les prestataires doivent s'assurer que leur conseil d'administration et leur direction générale mettent en place un contrôle de gestion efficace.

4.2 Gestion et suivi des niveaux de service

4.2.1 Les prestataires doivent développer et mettre en œuvre des systèmes de surveillance et de déclaration des niveaux de service.

4.3 Gestion des capacités

4.3.1 Les prestataires doivent prendre des mesures visant à s'assurer de l'adéquation des capacités de système et de réseau par le biais de prévisions, de mesures de surveillance et de tests.

4.4 Gestion des incidents et des problèmes

4.4.1 Les prestataires doivent mettre en place un processus de gestion des incidents afin de restaurer le service conformément aux niveaux de service convenus et d'identifier les causes sous-jacentes des problèmes.

4.5 Gestion du changement et de la configuration

4.5.1 Les prestataires doivent mettre en place des processus permettant de s'assurer que les systèmes ou les applications restent robustes et sûrs à la suite de changements de système ou de configuration.

4.6 Gestion globale des risques

4.6.1 Les prestataires doivent mettre en place un cadre de gestion du risque permettant la détection, l'évaluation et le contrôle des risques.

4.7 Continuité de l'activité

4.7.1 Les prestataires doivent mettre en place des plans efficaces de poursuite de l'activité en cas d'urgence ou de sinistre.

Principe 5 : Les prestataires prennent des mesures solides pour garantir la sécurité des réseaux et canaux mobiles.

5.1 Gouvernance en matière de sécurité

5.1.1 Les prestataires doivent définir et mettre en œuvre et une politique formelle de sécurité des services d'argent mobile et l'examiner périodiquement.

5.1.2 Les prestataires doivent filtrer, former et surveiller leur personnel interne.

5.1.3 Les prestataires doivent veiller à ce que des politiques soient en place pour assurer un traitement sécurisé des informations et des actifs.

5.1.4 Les prestataires doivent assurer la protection des actifs accessibles aux fournisseurs ou à des tiers.

5.2 Conception et mise en place d'un réseau, de systèmes et d'applications sécurisés

5.2.1 Les prestataires doivent veiller à ce que les données soient protégées au moyen de la cryptographie et de systèmes de contrôle de la sécurité des réseaux.

5.2.2 Les prestataires doivent s'assurer que les systèmes et les applications soient conçus et développés de façon sécurisée et fassent l'objet de tests rigoureux.

5.3 Sécurité des opérations et prévention de la fraude

5.3.1 Les prestataires doivent identifier et évaluer les risques en matière de sécurité avant d'offrir des services d'argent mobile et doivent surveiller ces risques de façon continue.

5.3.2 Les prestataires doivent correctement identifier et authentifier les utilisateurs des systèmes.

5.3.3 Les prestataires doivent limiter l'accès aux données clients aux personnes qui en ont besoin.

5.3.4 Les prestataires doivent restreindre l'accès physique aux systèmes.

5.3.5 Les prestataires doivent s'assurer du fonctionnement correct et sécurisé du traitement des informations.

5.3.6 Les prestataires doivent mettre en place des processus garantissant l'enregistrement de toutes les opérations et actions des utilisateurs avec des pistes d'audit appropriées.

5.3.7 Les prestataires doivent effectuer des tests périodiques de leurs systèmes et de leurs procédures de sécurité.

5.3.8 Les prestataires doivent assurer une sécurité continue des informations.

5.3.9 Les prestataires doivent mettre en place un processus de détection, de traitement et de surveillance des incidents de sécurité et des réclamations liées à la sécurité.

5.3.10 Les prestataires doivent mettre en place des politiques et mesures de prévention/détection des fraudes adaptées au niveau de risque.

Principe 6 : Les prestataires fournissent des informations claires, adéquates, opportunes et compréhensibles par les clients pour que ceux-ci puissent prendre leurs décisions en connaissance de cause.

6.1 Communication efficace et transparente

6.1.1 Les prestataires doivent s'assurer que des informations claires, visibles et opportunes soient fournies aux clients concernant la tarification et les conditions générales du service.

6.2 Sécurité

6.2.1 Les prestataires doivent éduquer les clients sur la manière d'utiliser les services d'argent mobile en toute sécurité.

Principe 7 : Les prestataires disposent de mécanismes visant à s'assurer que les réclamations soient correctement traitées et que les problèmes soient résolus dans les meilleurs délais.

7.1 Politiques et procédures garantissant la bonne résolution des réclamations de clients

7.1.1 Les prestataires doivent mettre en place des politiques et procédures pour répondre aux réclamations des clients.

7.1.2 Les prestataires doivent informer les clients de l'existence de politiques et procédures de traitement de leurs réclamations.

7.1.3 Les prestataires doivent mettre en place des politiques spécifiques pour le traitement des annulations d'opération.

7.2 Disponibilité de l'assistance à la clientèle

7.2.1 Les prestataires doivent mettre à la disposition de la clientèle un mécanisme approprié pour répondre aux questions et problèmes de celle-ci.

7.3 Mécanismes de recours extérieurs

7.3.1 Les prestataires doivent spécifier un mode de résolution des litiges en cas d'échec des mécanismes internes.

Principe 8 : Les prestataires respectent des pratiques appropriées de protection de la confidentialité des données lors de la collecte, du traitement et/ou de la transmission des données personnelles des clients.

8.1 Gouvernance

8.1.1 Les prestataires doivent se conformer aux bonnes pratiques et aux réglementations applicables en matière de protection des données personnelles des clients.

8.2 Transparence et notification

8.2.1 Les prestataires doivent veiller à ce que des informations claires, visibles et opportunes soient fournies aux clients sur les pratiques de protection de leurs données personnelles.

8.3 Choix et contrôle par les utilisateurs

8.3.1 Les prestataires doivent veiller à ce que les clients soient informés de leurs droits et qu'ils aient la possibilité d'exercer de véritables choix et contrôles sur les informations les concernant.

8.3.2 Les prestataires doivent obtenir le consentement des clients sur tout changement affectant de façon significative la protection des informations personnelles de ceux-ci.

8.4 Minimisation de la collecte et de la conservation de données

8.4.1 Les prestataires doivent limiter les informations personnelles collectées auprès des clients et conservées, utilisées ou partagées.

Annexe : Définition de l'argent mobile

Aux fins du présent code de conduite, l'argent mobile est défini comme un service transformationnel qui utilise les technologies de l'information et de la communication (TIC) et des canaux de distribution non bancaires pour élargir la diffusion de services financiers auprès de clients ne pouvant pas être touchés de façon rentable par les services financiers traditionnels distribués par le biais de succursales bancaires. Les exemples typiques de services d'argent mobile sont les porte-monnaie électroniques utilisés pour effectuer des transferts de personne à personne (« P2P », de l'anglais *person-to-person*) et un éventail de paiements, pour recevoir des salaires ou des prestations publiques (paiements « G2P », de l'anglais *government-to-person*).

Les services d'argent mobile présentent les caractéristiques suivantes :

- Les clients déposent ou retirent de l'argent du système au moyen d'un réseau d'agents transactionnels fonctionnant en dehors des succursales bancaires ;
- Les clients peuvent initier des opérations au moyen d'une interface disponible sur des téléphones portables basiques.

Bien qu'il n'existe pas à l'heure actuelle de définition réglementaire normative de l'argent mobile et de la monnaie électronique (« *e-money* » en anglais) adaptée à une utilisation mondiale, les pays qui ont mis au point leur propre définition tendent à inclure un certain nombre d'éléments communs. L'argent mobile est une valeur monétaire qui :

- Permet à l'utilisateur d'effectuer des transactions au moyen d'un téléphone portable ;
- Est acceptée en tant que moyen de paiement par des parties autres que l'émetteur ;
- Est émise sur remise de fonds ;
- Est enregistrée de façon électronique ;
- Peut être échangée contre de l'argent liquide.

Dans les pays où la monnaie électronique est définie par la réglementation ou la législation, l'argent est une forme de monnaie électronique.

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