BETTER THAN CASH ALLIANCE

BONNES PRATIQUES & INFORMATIONS DE BASE

JUILLET 2016

8 bonnes pratiques sur les paiements numériques responsables

8 BONNES PRATIQUES SUR LES PAIEMENTS NUMÉRIQUES RESPONSABLES

Photo de couverture : © The Coca-Cola Company

Veuillez noter que le présent document a fait l'objet de quelques modifications mineures en juin 2017.

Afin que les clients adoptent l'usage des paiements numériques, il est important qu'ils soient traités équitablement et qu'ils se sentent en sécurité et à l'abri de risques tels que la perte de confidentialité, l'exposition aux fraudes et l'imposition de frais non autorisés. Ainsi, il faut donc que les prestataires financiers prennent l'initiative de protéger leurs clients mais aussi que les autorités de réglementation assurent la mise en place d'un cadre réglementaire robuste de protection des consommateurs. Ces enjeux sont particulièrement importants pour les clients qui étaient jusqu'alors exclus ou avaient un accès limité au système financier, notamment les femmes, ainsi que pour ceux dont les capacités financières et technologiques sont restraintes. Ces derniers vont en effet être amenés à évoluer dans un contexte de mutations et d'innovations rapides au sein des secteurs des services financiers, des prestataires de services et des canaux de distribution. Les parties prenantes des écosystèmes de paiements numériques inclusifs doivent prendre la mesure de leur rôle pour faire en sorte que les paiements numériques soient effectués de manière responsable.

Parmi les grandes orientations concernant les paiements numériques responsables, l'Alliance Better Than Cash a retenu huit bonnes pratiques relatives aux interactions avec les clients qui émettent ou reçoivent des paiements numériques et qui étaient auparavant exclus du système financier ou n'avaient à ce système qu' un accès limité.

Ces bonnes pratiques visent avant tout la conception et la distribution des services de paiement des fournisseurs de services financiers. Elles peuvent également constituer une liste de contrôle utile (sous réserve des dispositions juridiques en vigueur) pour :

» Les autorités de réglementation lors de l'examen des règles à adopter;

» Le secteur privé (par exemple les entreprises de transport ou de grande distribution) lors du choix des fournisseurs de services de paiement;

» Les bailleurs de fonds et les organismes de développement lors de l'utilisation de services de paiement auprès de prestataires

» Toutes les parties prenantes dans leur plaidoyer en faveur d'une protection appropriée des consommateurs.

Les 8 bonnes pratiques portent principalement sur les types de paiements numériques les plus courants, fournis aux servicex traditionnellement exclus des systèmes financiers, tels que les comptes d'opérations financières numériques. Elles sont neutres du point de vue des technologies et des prestataires. Étant conçues pour s'appliquer aux innovations actuelles en matière de paiements numériques, elles devront faire l'objet d'examens et être actualisées de temps à autre. Chaque orientation inclut des exemples de ce qu'un client pourrait attendre d'un marché des paiements numériques responsables.

Depuis son lancement en 2012, l'Alliance Better Than Cash interagit avec des parties prenantes dans le cadre de nombreux forums pour la mise en place de systèmes de services de paiements numériques responsables qui servent les intérêts des émetteurs et destinataires de paiements.

Les présentes directives sont l'aboutissement de plusieurs années de consultations avec les acteurs du secteur financier, menées lors de rassemblements internationaux; elles reflètent notamment les conclusions du rapport global du Forum de la Finance Responsable sur les finances numériques de 2014 et de 2015 et de sa réunion régionale de 2016. Les Réunions du Forum de la Finance Responsable ont eu lieu conjointement à celles du Partenariat mondial pour l'inclusion financière issu du G20 et à la demande de ce dernier. Ces considérations découlent de la reconnaissance, au lendemain de la crise financière, de l'importance des pratiques responsables dans l'inclusion financière, et notamment des principes adoptés par le G20 en la matière.

D'autres directives proviennent des principes, normes et codes examinés dans la publication de 2015 intitulée Better *Than Cash Alliance Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services*[1] ainsi que d'autres publications et rapports scientifiques internationaux récents[2]. Les bonnes pratiques ont été largement diffusées sous forme d'ébauches afin d'obtenir des commentaires, et les remarques et retours issus de ce processus de consultation ont été incorporés dans le document rendu public.

L'objectif des bonnes pratiques est de fournir un outil utile à toutes les parties prenantes afin de favoriser l'adoption de pratiques responsables dans la transition des paiements en espèces à ceux numériques, en vue de réduire la pauvreté, d'impulser une croissance inclusive et de contribuer à une participation accrue des femmes à la vie économique.

8 Bonnes pratiques

1 Traiter les clients de manière équitable

Les clients, et en particulier ceux qui possèdent peu de capacités financières et technologiques, doivent être traités de manière équitable pour faire confiance aux processus de paiements numériques.

2 Assurer la sécurité des fonds des clients

Les clients, en particulier ceux qui étaient exclus ou avec un accès limité au système financier, doivent bénéficier d'un accès fiable et sécurisé aux fonds déposés sur leurs comptes bancaires numériques.

3 Assurer la transparence des produits pour les clients

L'environnement numérique requiert une volonté particulière de fournir aux clients des informations transparentes sur les produits, en particulier lorsque ces informations ne sont disponibles que par voie électronique, par exemple via le téléphone portable.

4 Concevoir des produits adaptés aux besoins et aux capacités des clients

La prise en compte des des besoins, des rôles économiques et des capacités des clients, et notamment des femmes, lors de la conception des services de paiements numériques accroît l'utilisation de ces services et réduit le nombre de problèmes et de réclamations.

5 Favoriser l'accès et l'utilisation des clients par l'interopérabilité

Tout en reconnaissant la nécessité de concilier la concurrence et l'innovation, assurer l'interopérabilité des plateformes, des agents et des clients est hautement recommandée, afin que les clients de différents systèmes puissent se faire des paiements entre eux et que les agents puissent travailler pour différents prestataires. Ceci est particulièrement important pour les clients vivant dans des zones rurales reculées.

6 En tant que prestataire de services, assumer la responsabilité des actes de tous les intervenants de la chaîne de valeur

Les clients sont plus susceptibles d'avoir confiance dans les moyens de paiements numériques et de les utiliser si les prestataires de services assument la responsabilité des actes de leurs agents, employés et prestataires de services tiers tout au long de la chaîne de valeur.

7 Protéger les données des clients

La protection des données numériques des clients prend une importance croissante, vu le volume, la vitesse d'utilisation et la diversité des données employées pour le marketing et les systèmes de notation de crédit, tout en sachant que l'utilisation des données des clients peut élargir la gamme des produits auxquels ces derniers peuvent avoir accès.

8 Offrir des moyens de recoursaux clients

Les clients doivent avoir accès à un système de recours équitable pour déposer des réclamations au sujet de leurs paiements numériques. Cette démarche est nécessaire tout particulièrement pour les réclamations ayant trait aux nouveaux produits, peu connus et délivrés par des canaux innovants, et pour les clients en situation d'isolement géographique dont les contacts directs avec les prestataires peuvent être limités, voire inexistants.

1 Traiter les clients de manière équitable

"Nous voulons que nos clients, dont la plupart sont non bancarisés et novices en matière de paiements numériques, se sentent respectés et traités équitablement et fassent l'objet de soins particuliers de la part de nos agents et de nos points de service. "

M. DASGUPTA ASIM KUMAR
CONSEILLER DES RELATIONS REGLEMENTAIRES

Les clients, et en particulier ceux qui possèdent peu de capacités financières et technologiques, doivent être traités de manière équitable pour avoir confiance dans les paiements numériques.

EXEMPLES DE TRAITEMENT ÉQUITABLE DES CLIENTS UTILISATEURS DE PAIEMENTS NUMÉRIQUES :

1. Tous **les supports de publicité et d'information commerciale** sont rédigés en langage simple et en termes clairs, exacts et non trompeurs.
2. Les conditions d'utilisation des produits **concilient raisonnablement les intérêts des clients et ceux des prestataires.**
3. Les clients sont traités avec respect, par exemple en ne leur vendant que les produits numériques dont ils ont réellement besoin.
4. **Les exigences relatives à l'identification** sont appropriées aux besoins des clients, de manière à leur faciliter l'accès aux services.
5. Les clients sont traités sur un pied d'égalité, **sans discrimination**, par exemple, sans distinction de sexe, de religion, d'ethnicité, d'opinions politiques, d'orientation sexuelle, d'âge, de lieu de résidence ou de handicap.
6. En cas **de perte ou de vol de codes d'accès** ou de justificatifs d'identité, le prestataire rembourse le client pour toute opération effectuée après la déclaration de perte ou de vol au prestataire. Le client a également droit à un remboursement si le montant d'une transaction dépasse un plafond quotidien ou périodique.
7. Les frais de paiement tardifs sont remboursés au client si le retard a été occasionné par une **interruption plannifiée du service** dont le client n'a pas été informé.
8. Les paiements numériques émis par les clients lors d'une **panne d'électricité** sont traités par le prestataire dans les meilleurs délais.

Assurer la sécurité des fonds des clients

"La confiance dans les paiements numériques étant indispensable à leur adoption, des cadres réglementaires appropriés et proportionnés doivent être mis en place pour assurer 24h/24 la protection des comptes des clients."

MME PIA ROMAN TAYAG
RESPONSABLE DE LA PROMOTION DES SERVICES FINANCIERS ACCESSIBLES À TOUS
BANGKO NG PILIPINAS

Les clients, en particulier ceux qui étaient exclus ou avec un accès limité au système financier, doivent avoir un accès fiable et sécurisé aux fonds déposés sur leurs comptes de paiements numériques.

EXEMPLES DE SAUVEGARDE DES FONDS DÉTENUS SUR LES COMPTES DE PAIEMENTS NUMÉRIQUES :

1. **Fonds de garantie :** Les prestataires non assujettis à la réglementation prudentielle tiennent en dépôt, dans un ou plusieurs comptes distincts auprès d'institutions soumises à cette réglementation, des fonds inutilisés d'un montant égal au total de tous les soldes impayés des clients. Une autre option envisageable est que les fonds de garantie soient investis dans des titres mobiliers autorisés (tels que des titres d'État ayant un marché secondaire actif). Autant que possible, les comptes et les investissements doivent etre détenus pour le bénéfice des clients (par exemple sur un compte fiduciaire). Ces fonds de garantie ne sont employés que pour effectuer des paiements aux clients et non à des fins opérationnelles. Ils sont par ailleurs tenus à l'abri de potentielles revendications des créanciers du prestataire. Les autorités de surveillance ont accès aux informations sur les comptes et les investissements en temps réel, lorsque ceci est faisable.
2. **Capacités et sécurité du système :** De solides mesures sont prises pour assurer la fiabilité du réseau et des systémes operationnels ainsi que d'un réseau et des canaux de paiements protégés de la fraude, du piratage et de toute autre forme d'utilisation non autorisée.
3. **Fraude :** Les clients sont remboursés par le prestataire en cas de perte directe due aux actes de fraude commis par des agents, des employés et des tiers prestataires de services (tels que les gestionnaires de réseaux d'agents) ou encore pour des fraudes tierces dues à un problème de sécurité raisonnablement évitable. Les clients sont informés promptement de tout soupçon d'activité frauduleuse.
4. **Transactions erronées ou non autorisées :** L'interface usager est conçue pour être claire, simple et sécurisée. Elle exige également une confirmation des détails du paiement avant la finalisation de la transaction. Le but visé est de minimiser le risque de transactions erronées et non autorisées, ainsi que de faciliter l'accès au service.

Assurer la transparence des produits pour les clients

"Tout produit qui vaut la peine d'être fourni doit l'être de manière transparente, en particulier pour les personnes qui effectuent ou reçoivent peut-être des paiements numériques pour la première fois. Il incombe aux prestataires de communiquer aux clients des informations claires et complètes nécessaires pour leur permettre de décider au mieux pour leur intérêt."

PR. BITANGE NDEMO
PROFESSEUR ASSOCIÉ,
ÉCOLE DE COMMERCE DE L'UNIVERSITÉ DE NAIROBI, ANCIEN SECRÉTAIRE PERMANENT, MINISTÈRE DE L'INFORMATION ET DE LA COMMUNICATION DU KENYA

L'environnement numérique requiert une volonté particulière de fournir aux clients des informations transparentes sur les produits, en particulier lorsque ces informations ne sont disponibles que par voie électronique, par exemple via la téléphonie mobile.

EXEMPLES DE RENFORCEMENT DE LA TRANSPARENCE DES PRODUITS DANS UN ENVIRONNEMENT NUMÉRIQUE :

1. **Information sur les produits :** Chaque client a accès (éventuellement sous forme numérique) à un descriptif clair, simple et facilement comparable des caractéristiques des produits, des conditions générales, des frais d'utilisation et des intérêts éventuels à payer. Cette information est communiquée avant que les services de paiement ne soient fournis; elle est actualisée périodiquement et présentée sous une forme que le client peut conserver et/ou à laquelle il peut accéder, notamment par voie électronique. Le prestataire de services fournit également des explications sur l'information lorsque le client en fait la demande ou s'il apparaît qu'il n'est pas en mesure de la comprendre (par exemple si elle est communiquée dans une langue que le client ne parle pas).
2. **Relevés des transactions et des comptes :** Le client reçoit une preuve de chaque transaction et peut accéder facilement à des relevés clairs et simples de ses transactions et de son compte. Ces relevés peuvent être communiqués sous forme numérique; ils doivent également être présentés sous une forme que le client peut conserver ou à laquelle il peut accéder, et consister, par exemple, en un récapitulatif chronologique numérique.

4

Concevoir des produits adaptés aux besoins et aux capacités des clients

"Les clients de BIM trouvent notre produit intuitif, facile à utiliser et transparent. Cela vient du fait que nous avons conçu BIM en fonction des besoins et des capacités des clients".

MME CAROLINA TRIVELLI
DIRECTRICE GÉNÉRALE
PAGOS DIGITALES PERUANOS

La prise en compte des besoins, des rôles économiques et des capacités des clients, et notamment des femmes, lors de la conception des services de paiements numériques accroît l'utilisation de ces services et réduit le nombre de réclamations.

EXEMPLES D'ACTIONS LIEES A LA CONCEPTION DES SERVICES DE PAIEMENTS NUMÉRIQUES :

1. **Conception des services de paiement :** Les services de paiements numériques sont conçus sur la base de recherches portant sur les besoins, les préférences et les comportements des clients. Ils tiennent également compte des niveaux probables de capacités financières et technologiques et, ils se caractérisent plus particulièrement pour les marchés avec un accès limité aux services financiers, par la simplicité et la clarté. Étant donné la forte exclusion financière des femmes, il est particulièrement important de concevoir les services de paiement en tenant compte des besoins, des capacités et des rôles économiques de celles-ci.
2. **Soutien aux utilisateurs :** Chaque client des services de paiements numériques reçoit :
   - **(a)** Des instructions faciles sur la façon de faire usage du service et sur la protection de leurs authentifiants (tels que les mots de passe et les PIN) accompagnées d'un descriptif sur les responsabilités des clients;
   - **(b)** Les coordonnées d'une permanence téléphonique où le prestataire peut être informé 24 heures sur 24 de la perte ou du vol de dispositif d'accès ou d'authentifiant, d'une transaction erronée ou non autorisée, ou d'une atteinte à la sécurité;
   - **(c)** Les coordonnées du prestataire joignable en heure ouvrée de travail, afin que le client puisse disposer d'une source d'information fiable sur la façon de faire usage des services financiers numériques et sur leurs caractéristiques;
   - **(d)** Un soutien supplémentaire pour les nouveaux utilisateurs, en particulier les femmes, selon qu'il est nécessaire et réalisable, afin d'appuyer l'adoption et l'utilisation du service dans de bonnes conditions de sécurité.

5 Appuyer l'accès des clients et l'utilisation des services par l'interopérabilité

"Les autorités de réglementation ont un rôle à jouer dans la mise en place de systèmes de paiements interopérables qui contribuent à réduire les coûts de transaction et à accroître la commodité pour les clients."

M. SETTOR AMEDIKU
CHEF DU SERVICE DE
LA STABILITÉ FINANCIÈRE
BANK OF GHANA

Tout en reconnaissant la nécessité de concilier la concurrence et l'innovation, le fait d'assurer l'interopérabilité des plateformes, des agents et des clients est important afin de permettre aux clients de différents systèmes de se faire, des paiements les uns aux autres et afin que les agents puissent travailler pour différents prestataires. Ceci est d'autant plus important pour les clients habitant des zones rurales éloignées.

EXEMPLES DE MESURES DE FACILITATION DE L'INTEROPÉRABILITÉ :

1. Encourager les initiatives d'interopérabilité menées en collaboration et émanant du secteur financier pour faire en sorte que les clients puissent effectuer des transactions financières numériques quels que soient leur lieu de résidence ou leur prestataire de services.
2. Décourager tout obstacle s'opposant délibérément à l'interopérabilité (tels que les accords d'exclusivité conclus avec les agents).

6 En tant que prestataire de services, assumer la responsabilité des actes de tous les intervenants de la chaîne de valeur

"Nous ne pouvons, en tant que prestataires de services, acquérir la confiance des clients que si nous veillons à ce que tous les intervenants de notre chaîne de valeur agissent de manière responsable et à ce que les systèmes et les processus nécessaires à cette fin soient en place. Tel est le message qu'il faut communiquer aux clients, en particulier aux nouveaux venus aux paiements numériques."

MR. RAJPAL DUGGAL
OXIGEN SERVICES INDIA

Les clients sont plus susceptibles d'accorder leur confiance aux moyens de paiements numériques et de les utiliser si les prestataires de services assument la responsabilité des actes de leurs agents, employés et prestataires de services tiers tout au long de la chaîne de valeur.

EXEMPLES DE RESPONSABILITÉ DES ACTES DES AGENTS, DES EMPLOYÉS ET DES TIERS PRESTATAIRES DE SERVICES :

1. **Responsabilité :** Les prestataires assument la responsabilité des actes et des omissions de leurs agents, employés et prestataires de services tiers.
2. **Formation et supervision :** Les agents et les employés, ainsi que les prestataires de services tiers, sont formés (notamment aux caractéristiques des produits, à leurs responsabilités juridiques et aux comportements sensibles aux sexospécificités) et supervisés de manière appropriée. Ils disposent également des ressources nécessaires pour fournir desservices de paiements de manière compétente et conforme aux règlements.
3. **Connaissance des prestataires :** Les agents communiquent aux clients le nom et les coordonnées du prestataire de services lors de l'ouverture de leur compte et sur demande.

7 Protéger les données des clients

"Avec les progrès de l'inclusion financière, il devient de plus en plus important d'assurer la sécurité de l'énorme masse de données traitée par les divers prestataires de services financiers inclusifs."

M. TAO SUN
SENIOR DIRECTOR
ANT FINANCIAL

La protection des données numériques des clients revêt une importance croissante, vu le volume, la vitesse d'utilisation et diversité des données employées pour le marketing et les systèmes de notation de crédit, tout en sachant que l'utilisation des données des clients peut élargir la gamme des produits auxquels ces derniers peuvent avoir accès.

EXEMPLES DE MESURES POSSIBLES DE PROTECTION ÉLÉMENTAIRE DES DONNÉES DES CLIENTS DANS UN ENVIRONNEMENT NUMÉRIQUE :

1. **Confidentialité et sécurité :** Des mesures appropriées sont prises afin d'assurer la confidentialité et la sécurité des données des clients en rapport avec les paiements numériques. Les données dont il s'agit comprennent, par exemple, l'identité des clients et les informations sur leur contrat, les relevés des transactions; les authentifiants; le dispositif utilisé, le téléphone mobile utilisé, les données d'usage de l'internet et les données de géolocalisation. Ces données peuvent, avec le consentement explicite et éclairé des clients, être utilisées et divulguées à des fins spécifiques, notamment pour la commercialisation de nouveaux services.
2. **Piste d'audit :** Les clients et les superviseurs ont accès à une piste d'audit claire des relevés de transaction.

Offrir des moyens de recours aux clients

"L'expérience du Mexique est que les mécanismes de recours opérants en place dans un environnement numérique sont essentiels pour que les clients utilisent les services financiers en toute confiance."

MME MARÍA FERNANDA TRIGO,
DIRECTRICE GÉNÉRALE
POUR L'ACCÈS AUX SERVICES FINANCIERS
COMMISSION NATIONALE BANCAIRE ET
FINANCIÈRE DU MEXIQUE

Il faut que les clients aient accès à un système de recours équitable pour recevoir leurs réclamations concernant les paiements numériques. Ceci est nécessaire tout particulièrement pour les réclamations ayant trait aux nouveaux produits, mal connus et délivrés par des canaux innovants, et pour les clients en situation d'isolement géographique dont les contacts directs avec les prestataires peuvent être limités, voire inexistants.

EXEMPLES DE SYSTÈMES DE RECOURS EFFICACES POUR LES CLIENTS DES SERVICES DE PAIEMENTS NUMÉRIQUES :

1. **Réclamations :** Les clients ont facilement accès à un système de dépôt de réclamations transparent, gratuit ou peu coûteux, et efficace, qui, autant que possible, tient compte des clients vulnérables (tels que les personnes handicapées). Un tel système doit être accessible à tous les clients, quelles que soient leurs normes culturelles, leur langue, leur mobilité, etc.
2. **Litiges :** Les clients ont également accès à un tiers indépendant qui traite les litiges avec les prestataires lorsque ceux-ci n'ont pas répondu aux réclamations des clients de manière adéquate et lorsuq'ils n'ont pas résolu le problème. Ce système de tiers indépendant est d'accès facile (notamment par téléphone ou par voie électronique), transparent, gratuit ou peu coûteux, et efficace.
3. **Informations sur les systèmes de recours :** Les Informations sur le système de recours sont énoncées dans les conditions générales disponibles sur le site Web du prestataire ainsi que dans ses locaux et ceux de l'agent. En outre, après qu'un client ait déposé une réclamationune copie de ces informations leur est communiquée. Cela peut se faire sous forme numérique.
4. **Données relatives aux réclamations :** Les prestataires tiennent des archives contenant les détails des réclamations des clients ainsi que leur réponse à chaque plainte. Des comptes rendus périodiques sur les réclamations sont également communiqués aux autorités de réglementation. Les problèmes systémiques affectant le secteur sont rendus publics, mais sans que ne soit divulgué l'identité des plaignants.

Informations complémentaires

DIRECTIVE 1 : Traiter les clients de manière équitable

Les clients doivent être traités équitablement pour avoir confiance dans les paiements numériques et en particulier ceux qui possèdent peu de connaissances financières et technologiques.

EXEMPLES DE TRAITEMENTS ÉQUITABLES DES UTILISATEURS DE PAIEMENTS NUMÉRIQUES :

1. Tous les **supports de publicité et d'information commerciale** sont rédigés en langage simple et en termes clairs, précis et non trompeurs.
2. Les conditions d'utilisation des produits **concilient raisonnablement les intérêts des clients et ceux des prestataires.**
3. **Les clients sont traités avec respect,** par exemple en ne leur vendant que les produits numériques dont ils ont réellement besoin.
4. **Les exigences relatives à l'identification** sont appropriées pour les clients, de manière à faciliter l'accès aux services.
5. Les clients sont traités sur un pied d'égalité, **sans discrimination.** Par exemple, les prestataires les traitent sans distinction de sexe, de religion, d'ethnicité, d'opinions politiques, d'orientation sexuelle, d'âge, de lieu de résidence ou de handicap.
6. En cas **de perte ou de vol de codes d'accès** ou de justificatifs d'identité, le prestataire rembourse le client pour toute opération effectuée après la déclaration de perte ou de vol au prestataire. Le client a également droit à un remboursement si le montant d'une transaction dépasse un plafond quotidien ou périodique.
7. Les frais de paiements tardifs sont remboursés au client si le retard de paiement a été occasionné par une **interruption prévue du service** dont le client n'a pas été informé.
8. Les paiements numériques émis par les clients lors d'une **panne d'électricité** sont traités par le prestataire dans les meilleurs délais.

CONTEXTE

Les clients doivent être traités de manière équitable pour utiliser les paiements numériques avec confiance. Ceci est particulièrement important pour les nouveaux clients ou ceux qui n'en ont que peu d'expérience des services financiers, catégorie où les femmes sont, en raison de leur manque d'accès, surreprésentées. Cette approche est énoncée clairement dans les *"Principes de haut niveau sur la protection financière des consommateurs"* du G20, au principe 3 : "Tous les consommateurs de produits financiers devraient être traités de manière équitable, honnête et juste à tous les stades de leurs relations avec les fournisseurs de services financiers. [...] Les besoins des groupes vulnérables devraient faire l'objet d'une attention particulière[3]."

1.1 Publicité et autres informations sur les ventes

La ligne directrice 1.1 est semblable, par son sujet, à la norme 3 du principe 1 de la nouvelle version des Normes de certification - Protection des clients de la Smart Campaign, qui prévoit qu'une politique et des processus doivent être en place pour empêcher l'emploi de techniques de ventes agressives et l'exercice de toute pression à la signature des contrats.

La ligne directrice 1.1 pourrait couvrir tous les supports promotionnels communiqués à un client actuel ou prospect à travers tous les canaux ainsi que les informations relatives aux produits figurant dans les brochures de promotion et communiquées par les agents et les employés.

1.2 Les conditions d'utilisation des produits concilient raisonnablement les intérêts des clients et ceux des prestataires

Le traitement équitable des clients consiste en partie à s'assurer que les conditions générales d'utilisation des paiements numériques n'exploitent pas les clients. Parmi les exemples de conditions injustes figurent les clauses contractuelles qui tiennent le client responsable de tous les paiements effectués par erreur (même après notification du prestataire) ou par lesquelles le prestataire se dégage de toute responsabilité du fait de ses agents ou en cas de non fourniture du service payé par le client. Le Règlement 16/1/PBI/2014 de Bank Indonesia sur la protection des usagers des systèmes de paiement (ci-après le Règlement indonésien sur la protection des usagers de systèmes de paiement) est un exemple de dispositions réglementaires spécifiques portant sur la question des conditions inéquitables[4].

1.3 Les clients sont traités avec respect

Comme le note le principe 5 des Principes de protection des clients de la Smart Campaign, le respect des clients et leur traitement équitable sont indissociables. Ce respect peut se manifester de multiples manières : ne vendre aux clients que des produits qui correspondent à leurs besoins et à leurs capacités; s'abstenir d'exercer des pressions sur un client potentiel pour lui faire acheter un produit de paiements numériques sans se préoccuper de savoir si le produit répondra à ses besoins en la matière; ne pas encourager l'adoption de tels produits lorsque le client n'a pas accès facilement à un réseau d'agents pour les services de dépôt et de décaissement. Avant de proposer un microprêt lié à un compte numérique, il convient également de déterminer si le client titulaire du compte numérique sera réellement en mesure de rembourser le prêt. Enfin, les clients, femmes et hommes, doivent être traités strictement avec le même respect.

1.4 Exigences relatives à l'identification des clients

Les clients à bas revenu ne détiennent généralement pas de documents d'identité traditionnels, tels qu'une carte d'identité nationale, un permis de conduire, un certificat de naissance ou un justificatif de domicile, et peuvent donc pour cette raison se voir refuser l'accès aux services de paiements numériques.

Toutefois, les *Recommandations du Groupe d'action financière (GAFI) : Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération* de 2012 révisées en 2016 (ci-après les *Recommandations du GAFI*), sur lesquelles sont fondées les lois nationales visant la lutte contre le blanchiment d'argent et contre le terrorisme, prévoient l'application de règles d'identification des clients fondées sur le risque[5].

Un service de paiements tel qu'un compte de paiements électroniques, peut être un exemple de ce type de produit, reposant sur des facteurs comme la limite de plafonds sur les transactions et les soldes. Les directives du GAFI relatives à l'obligation de vérifier l'identité des clients, sont également claires sur le fait qu'il n'est pas nécessaire de faire usage de pièces d'identité émises par les pouvoirs publics (que beaucoup de clients à bas revenu ne possèdent pas) et que cette flexibilité est d'une pertinence particulière pour l'inclusion financière[6].

1.5 Discrimination

La ligne directrice 1.5 est semblable aux normes 2 du principe 5 des *Normes de certification – Protection des clients* de la *Smart Campaign* (ci-après les Normes de certification de la Smart Campaign). Ces normes, pour les résumer, visent à limiter la discrimination fondée sur l'appartenance ethnique, le sexe, l'âge, le handicap, l'affiliation politique, l'orientation sexuelle, la caste et les croyances religieuses.

1.6 Perte ou vol de dispositifs d'accès, d'authentifiant ou d'identité

La ligne directrice 1.6 propose le remboursement de toute transaction ayant été effectuée après que le prestataire ait été notifié d'un vol ou d'une perte et dans les cas de dépassement d'un plafond limitant le montant quotidien ou périodique des transactions. Cette approche est comparable à celle, par exemple, du Code australien des e-paiements, administré par la Commission australienne des valeurs mobilières et des placements (ci-après le Code des e-paiements de l'Australie), encore que le processus de détermination de la responsabilité soit plus complexe dans ce dernier[7].

1.7 Défaillance du système

La Note d'information du Groupe consultatif d'assistance aux pauvres (CGAP) intitulée *Réussir la finance numé-*

rique : pourquoi atténuer davantage les risques pour les clients (ci-après la Note d'information du CGAP sur la finance numérique) a retenu "l'incapacité d'effectuer une transaction en raison d'une défaillance du réseau ou du service" comme le premier des sept principaux risques auxquels sont exposés les consommateurs[8].

Les défaillances du système électronique sont un sujet de préoccupation courant pour les clients, lesquels s'attendent, on le conçoit, à pouvoir accéder aux fonds déposés sur leur compte lorsqu'ils en ont besoin. Ceci revêt une importance particulière pour les clients à bas revenu qui n'ont sans doute pas accès à d'autres sources de fonds. Néanmoins, selon ces directives, les clients ne pourraient en tout réalisme s'attendre à des réparations qu'en cas de perte directe résultant de l'imposition de frais de paiement tardif lorsque le retard est dû à une non disponibilité du système dont ils n'avaient pas été notifiés à l'avance (et pas en cas de pertes indirectes telles qu'un manque à gagner).

On trouve un exemple d'approche plus large de la question des défaillances du système à la clause 14.2 du Code des e-paiements de l'Australie, selon laquelle un usager ne saurait se voir contester le droit de réclamer des indemnités pour dommage indirect subi du fait d'un défaut de fonctionnement d'un système ou d'un matériel fourni pas un tiers qui s'est opposé à son accès à un réseau électronique partagé (sauf si le client aurait dû, raisonnablement, être au courant du défaut de fonctionnement ou de la non disponibilité du système)[9].

1.8 Pannes d'électricité

La ligne directrice 1.8 traite du problème commun des pannes d'électricité qui affectent les paiements numériques. Dans une telle éventualité, les clients doivent avoir la garantie que les paiements qui ont été émis mais qui n'ont pas été reçus seront traités dans les meilleurs délais.

DIRECTIVE 2 : Assurer la sécurité des fonds des clients

Les clients, en particulier ceux qui étaient exclus ou avaient un accès un access limité au système financier, doivent avoir un accès fiable et dans de bonnes conditions de sécurité aux fonds déposés sur leurs comptes de paiements numériques.

EXEMPLES DE SÉCURISATION DES FONDS DÉTENUS SUR LES COMPTES DE PAIEMENT NUMÉRIQUE :

1. **Fonds de garantie :** Les prestataires non assujettis à la réglementation prudentielle tiennent en dépôt, dans un ou plusieurs comptes distincts auprès d'institutions soumises à cette réglementation, des fonds inutilisés d'un montant égal au total de tous les soldes impayés des clients. Une autre option envisageable est que les fonds de garantie soient investis dans des titres mobiliers autorisés (tels que des titres d'État ayant un marché secondaire actif). Autant que possible, les comptes et les investissements doivent etre détenus pour le bénéfice des clients (par exemple dans un compte fiduciaire). Ces fonds de garantie ne sont employés que pour effectuer des paiements aux clients et non à des fins opérationnelles. Ils sont par ailleurs tenus à l'abri de potentielles revendications des créanciers du prestataire. Lorsque ceci est possible, les superviseurs ont accès aux informations sur les comptes et les investissements en temps réel.
2. **Capacités et sécurité du système :** De solides mesures sont prises pour assurer la fiabilité du réseau et des systémes operationnels ainsi que d'un réseau et des canaux de paiements protégés de la fraude, du piratage et de toute autre forme d'utilisation non autorisée.
3. **Fraude :** Les clients sont remboursés par le prestataire en cas de perte directe due aux actes de fraude commis par des agents, des employés et des tiers prestataires de services (tels que les gestionnaires de réseaux d'agents) ou d'autres organisations dus a un probleme de sécurité raisonnablement évitable. Les clients sont informés promptement de tout soupçon d'activité frauduleuse.
4. **Transactions erronées ou non autorisées :** L'interface usager est conçue pour être claire, simple et sécurisée. Elle exige également une confirmation des détails du paiement avant la finalisation de la transaction. Le but visé est de minimiser le risque de transactions erronées et non autorisées, ainsi que de faciliter l'accès au service.

CONTEXTE

2.1 Fonds de garantie

Le risque le plus fondamental auquel sont exposés les clients d'un produit de paiements numériques est qu'ils ne puissent pas accéder à leurs fonds lorsqu'ils en ont besoin. À cet égard, la *Note d'information du CGAP sur la finance numérique* inclut dans sa liste des principaux risques «[l']insuffisance du flottant ou des liquidités du détaillant, ce qui influe également sur la capacité à effectuer une transaction».

Il existe également le risque que le prestataire ou sa banque deviennent insolvables. Enfin, les risques opérationnels généraux peuvent affecter la capacité des clients à effectuer des transactions[10].

La ligne directrice 2 de l'Alliance Better Than Cash donne en particulier les exemples de bonnes pratiques suivants :

- Les fonds de garantie des soldes et titres impayés devraient être « non grevés », c'est-à-dire non utilisés pour garantir un autre élément de passif.
- Ces fonds peuvent être détenus dans un compte distinct auprès d'une institution soumise à la réglementation prudentielle (tel qu'un compte fiduciaire) ou en titres mobiliers autorisés (tels que des titres d'État).
- Les fonds de garantie ne servent qu'à effectuer des paiements aux clients et doivent être à l'abri de revendications de tiers créanciers du prestataire de manière à assurer une protection contre les risques d'illiquidité et d'insolvabilité.

Il existe de nombreux exemples de principes, normes et codes ainsi que de mesures législatives nationales portant sur la protection du flottant pour les fonds des clients détenus dans des comptes de paiements numériques. Figurent parmi ces exemples :

- Le principe guide 2 du *Rapport sur les aspects de l'inclusion financière relatifs aux paiements [Payment Aspects of Financial Inclusion] (ci-après le Rapport PAFI),* émanant du Comité sur les infrastructures de paiement et de marché de la Banque des règlements internationaux et de la Banque mondiale;
- Le principe 1 du *Code de conduite* de la GSMA; et
- La législation et les directives de pays tels que l'Afghanistan, le Kenya, le Malawi, les Philippines et la Tanzanie[11].

Ces exemples proposent différents traitements face au problème de la protection des fonds des clients mais ils portent tous sur cette question essentielle.

2.2 Capacités et sécurité du système

Les clients s'attendent, à l'évidence, à ce qu'une attention sérieuse et constante soit accordée aux capacités et à la sécurité des systèmes de paiements numériques. Le *Rapport PAFI* souligne la nécessité de points d'accès et de canaux fiables et de haute qualité (avoir le principe guide 5). Le *Code de conduite* de la GSMA contient des dispositions détaillées sur la sécurité et les capacités des systèmes (voir en particulier les directives 4 et 5), de même que le principe guide 3 du *Rapport PAFI* et le *Guide du Projet Level One* de la Fondation Bill & Melinda Gates (ci-après le *Guide du Projet Level One* de la Fondation Gates).

Ces préoccupations ont été prises en considération dans les mesures législatives nationales. C'est ainsi, par exemple, que la circulaire 649 des Philippines sur l'argent électronique (2009) exige la mise en place de politiques et de mesures de sécurité appropriées pour garantir l'intégrité, l'authenticité et la confidentialité des données et des systèmes d'exploitation[12]. Le Règlement indonésien sur la protection des usagers des systèmes de paiement traite aussi généralement des questions de sécurité[13]. Le nouveau Cadre de protection des consommateurs du Nigéria est plus spécifique en ce qu'il précise que la Banque centrale « doit fixer les normes technologiques minimales des plateformes de paiement »[14].

Les clients sont également en droit de s'attendre à un règlement des paiements numériques immédiat et en temps réel. Toutefois, la présente ligne directrice ne traite pas de cette question car tous les systèmes de paiement ne sont pas en mesure d'assurer un tel règlement. Pour des directives sur le règlement des paiements en temps réel, voir la position du *Guide du Projet Level One* de la Fondation Gates concernant les transferts de fonds immédiats et le règlement le jour-même, ainsi que la directive 1.2.1 du *Code de conduite* de la GSMA, qui portent toutes deux sur le débit et le crédit des fonds en temps réel.

2.3 Fraude

La plupart des clients s'attendent à être indemnisés par le prestataire en cas de fraude commise par les employés, les agents et les tiers prestataires de services. Ils peuvent également s'attendre à des dédommagements en cas de fraude résultant d'une atteinte à la sécurité qui aurait pu raisonnablement être évitée (suite, par exemple, à l'attaque d'un pirate informatique). À certains égards, la ligne directrice 2.3 peut sembler lourde pour le prestataire, mais la fraude constitue un risque important pour les clients ainsi que le met en évidence le *Rapport final du Ve Forum sur la finance* responsable de 2014 (ci-après le *Rapport final du Ve Forum sur la finance responsable*). Les clients s'attendent généralement à ce que les prestataires de services de paiements soient tenus responsables de toute fraude commise par des personnes ou des entités qui sont ou devraient être sous le contrôle de ceux-ci.

Ainsi qu'il est noté dans le préambule de la Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiements dans le marché intérieur (ci-après la PSD2) : «Tous les services de paiements proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude[15]». La PSD2 contient également des dispositions très strictes pour appuyer les utilisateurs qui présentent une réclamation concernant les opérations de paiement non autorisées[16].

La nécessité d'appliquer des mesures de prévention de la fraude est également un thème abordé tout au long du *Guide du Projet Level One* de la Fondation Gates ainsi que lors de divers forums et dans d'autres publications. Par exemple, la *Note d'information du CGAP sur la finance numérique* signale « la fraude ciblant les clients » en tant que risque clé; le *Rapport final du Ve Forum sur la finance responsable* a de même retenu la fraude comme un risque clé qui doit être pris en considération.

2.4 Transactions erronées ou non autorisées

La plupart des experts et des commentateurs conviennent que les systèmes de paiements numériques devraient être dotés d'une interface claire et facile à utiliser afin de réduire le risque de transactions erronées ainsi que d'encourager l'utilisation régulière des services de paiements. La *Note d'information du CGAP sur la finance numérique* signale parmi les principaux risques celui qui est lié à « des interfaces utilisateurs que beaucoup trouvent complexes et déroutantes ». Le *Rapport du VIe Forum sur la finance responsable : éléments probants et innovation en faveur d'une amplification de la finance numérique inclusive (ci-après le Rapport du VIe Forum sur la finance responsable)* traite également de l'importance de la convivialité des interfaces utilisateurs.

Les transactions non autorisées sont, elles aussi, un sérieux sujet de préoccupation pour les clients, lesquels s'attendent à ce que l'interface utilisateur soit sécurisée. La PSD2 impose aux prestataires la charge de la preuve de la bonne exécution des transactions lorsqu'un utilisateur présente une réclamation relevant selon lui, du fait que ces transactions n'étaient pas autorisées ou ont été mal exécutées[17].

DIRECTIVE 3 : Assurer la transparence des produits pour les clients

L'environnement numérique requiert une volonté particulière de fournir aux clients des informations transparentes sur les produits, en particulier lorsque ces informations ne sont disponibles que par voie électronique, par exemple via la téléphonie mobile.

EXEMPLES DE RENFORCEMENT DE LA TRANSPARENCE RELATIVE AU PRODUIT DANS UN ENVIRONNEMENT NUMÉRIQUE :

1. **Information sur les produits :** Chaque client a accès (éventuellement sous forme numérique) à un descriptif clair, simple et facilement comparable des caractéristiques des produits, des conditions générales, des frais d'utilisation et des intérêts éventuels à payer. Cette information est communiquée avant que les services de paiement ne soient fournis; elle est actualisée périodiquement et présentée sous une forme que le client peut conserver et/ou à laquelle il peut accéder, notamment par voie électronique. Le prestataire de services fournit également des explications sur l'information lorsque le client en fait la demande ou s'il est évident qu'il n'est pas en mesure de la comprendre (par exemple si elle est communiquée dans une langue que le client ne parle pas).
2. **Relevés des transactions et des comptes :** Le client reçoit une preuve de chaque transaction et peut accéder facilement à des relevés clairs et simples de ses transactions et de son compte. Ces relevés peuvent être communiqués sous forme numérique; ils doivent également être présentés sous une forme que le client peut conserver ou à laquelle il peut accéder, et consister, par exemple, en un récapitulatif chronologique numérique.

CONTEXTE

3.1 Informations sur les produits

La communication d'informations claires et faciles à comprendre sur les produits aide à créer une clientèle plus disposée à avoir confiance dans les paiements numériques et à les utiliser. Elle permet également des comparaisons entre différents produits et peut encourager la concurrence et réduire les coûts. Toutefois, les descriptifs perdent toute utilité s'ils sont d'une longueur et d'une complexité telles que les clients ne peuvent plus les comprendre.

Par ailleurs, les informations communiquées sur le petit écran d'un téléphone portable peuvent ne pas suffire, comme le précise le Rapport final du Ve Forum sur la finance responsable. Et en tout état de cause, les informations doivent pouvoir être accessibles pour référence ultérieure, par exemple en cas de réclamation des clients. Les conditions d'utilisation des produits peuvent être communiquées par courriel ou par le biais d'un site Web ou être remises par un agent. La ligne directrice 3.1 est conçue pour tenir compte de ces considérations.

L'importance de la transparence est largement reconnue par d'autres directives et normes internationales. Par exemple, la *Note d'information du CGAP sur la finance numérique* inclut parmi les principaux risques « le manque de transparence des frais et d'autres conditions de services », et elle insiste sur le fait que « la transparence de l'information sur les produits est un élément clé de la mise en place de services de finance numérique responsable». Elle souligne également l'importance de compléments d'information comparables aussi bien conçues.

De même, encore qu'à différents degrés, tous les textes suivants insistent sur l'importance de la transparence :

- La directive 6.1.1 du *Code de conduite* de la GSMA;
- Le principe 3 des *Principes de protection des clients* de la Smart Campaign; et.
- Les principes guides 2 et 5 du *Rapport PAFI.*

Ces derniers principes mentionnent aussi la nécessité d'utiliser des « méthodologies comparables » et suggère que des informations soient fournies sur les risques associés à l'utilisation d'un produit ainsi que sur la façon de minimiser les coûts tout en maximisant les avantages.

Il existe également de nombreux exemples de dispositions prises par les autorités gouvernementales nationales ainsi que d'initiatives législatives qui visent à assurer la transparence de l'information sur les produits financiers et sur leur performance. Ces dispositions et initiatives peuvent s'appliquer aux produits de paiements numériques de même qu'à d'autres types de services financiers.

Le Bureau des entités financières du Mexique en offre un excellent exemple[18]. Il publie sur son site Web des informations sur les produits, les redevances et commissions, les conditions non équitables, les réclamations, les sanctions et diverses données sur la performance des institutions financières. Ces dernières sont également tenues de publier ces informations sur leur propre site Web. On trouvera d'autres exemples de règles sur la transparence dans le Règlement indonésien sur la protection des usagers de systèmes de paiement et de celles sur les obligations relatives à la divulgation des redevances et frais dans le Règlement tanzanien sur l'argent électronique de 2015.

3.2 Relevés des transactions et des comptes

Les clients peuvent s'attendre à avoir accès en tous temps à des relevés clairs et simples des transactions et de leur compte, lesquels, pour être utiles, doivent se présenter sous une forme facilement compréhensible et être fiables. Ces relevés sont particulièrement importants en cas de réclamations portant sur une transaction donnée, qu'il s'agisse, par exemple, d'un paiement effectué par erreur ou d'un paiement qui n'a pas été reçu. Les relevés peuvent être sous format numérique, à condition que le client puisse y accéder et/ou conserver les informations qu'ils contiennent sans difficulté.

DIRECTIVE 4 : Concevoir des produits adaptés aux besoins et aux capacités des clients

La prise en compte des besoins, des rôles économiques et des capacités des clients, et notamment des femmes, lors de la conception des services de paiements numériques accroît l'utilisation de ces services et réduit le nombre de problèmes et de réclamations.

EXEMPLES D'ACTIONS LIEES À LA CONCEPTION DES SERVICES DE PAIEMENTS NUMÉRIQUES :

1. **Conception des services de paiement :** Les services de paiements numériques sont conçus sur la base d'études portant sur les besoins, les préférences et les comportements des clients. Leur modèle, prenant également en compte le niveau probable de capacités financières et technologiques des clients, en particulier pour les marchés avec un accès limité aux services financiers, se veut simple et clair.
2. **Soutien aux utilisateurs :** Il est fourni à chaque client des services de paiements numériques :
   - **(a)** Des instructions faciles à comprendre sur la façon de faire usage du service et de protéger leurs authentifiants (tels que les mots de passe et les PIN), accompagnées d'un descriptif relatif aux responsabilités des clients;
   - **(b)** Les coordonnées d'une permanence téléphonique où le prestataire peut être informé 24 heures sur 24 de la perte ou du vol de dispositif d'accès ou d'authentifiant, d'une transaction erronée ou non autorisée, ou d'une atteinte à la sécurité;
   - **(c)** Les coordonnées du prestataire durant les heures normales de service, pour que le client dispose d'une source d'information fiable sur la façon de faire usage des services financiers numériques et sur leurs caractéristiqu es.
   - **(d)** Un soutien supplémentaire pour les nouveaux utilisateurs, notamment pour les femmes, selon qu'il est nécessaire et réalisable, afin d'appuyer l'adoption et l'utilisation du service dans de bonnes conditions de sécurité.

CONTEXTE

4.1 Conception des services de paiements

Comme le souligne le *Rapport du VI^e Forum sur la finance responsable*[19], pour être utiles et utilisés, les services de paiements numériques doivent être conçus pour répondre aux besoins de groupes de clients cibles. Ils doivent également tenir compte des préférences et des comportements escomptés des clients. Le principe 1 des *Principes de protection des clients* de la *Smart Campaign* traite de la conception et de la distribution appropriées des produits, alors que le principe guide 4 du *Rapport PAFI* mentionne la nécessité que les transactions et les produits de paiements répondent à une large gamme de besoins de la population cible, à moindre coût ou gratuitement. Les bonnes pratiques de l'Alliance Better Than Cash, elles, ne font pas référence au coût des paiements, étant donné que cela peut limiter l'innovation et la concurrence. Elles s'attachent à encourager une élaboration appropriée des produits, ce qui peut se faire, par exemple, au moyen de recherches axées sur les clients, de réunions de consommateurs et d'enquêtes, qui prennent en considération les sous-segments du marché, notamment les femmes, dans leurs divers rôles économiques.

4.2 Soutien aux utilisateurs

Les clients ayant un accès limité aux services financiers et qui utilisent les paiements numériques possèdent généralement des niveaux peu élevés de capacités financières ou technologiques, ce qui peut faire obstacle à l'utilisation de ces produits. Le renforcement des capacités des femmes en la matière est un investissement utile. Les clients peuvent également ne pas comprendre les risques de communication de leur PIN à autrui ou la façon d'éviter les erreurs de transactions, ou même les caractéristiques des services de paiements numériques et la façon de les utiliser.

La ligne directrice 4 de l'Alliance propose des mesures simples et pratiques qui peuvent contribuer à lever ces difficultés. Pour autant, par souci de spécificité et d'applicabilité concrète, elle ne vise pas à couvrir toute la gamme des stratégies et programmes de renforcement des capacités financières utilisables pour les paiements numériques. En revanche, le principe guide 6 du *Rapport PAFI* de la Banque mondiale, qui traite des questions de compétences financières élémentaires, émet des suggestions spécifiques et recommande notamment :

- Des efforts constants d'éducation financière sur le secteur public et le secteur privé;
- Une attention particulière portée aux comptes de transactions dans les programmes d'éducation financière;
- Une attention particulière à la publication d'informations sur les types de comptes disponibles, les exigences relatives à leur ouverture, les frais applicables et les façons de minimiser les coûts, les risques, les mesures de sécurité fondamentales et les obligations générales des prestataires et des utilisateurs;
- Une formation pratique dans le cadre des opérations de lancement des nouveaux produits.

DIRECTIVE 5 : Appuyer l'accès des clients et l'usage des services par l'interopérabilité

Tout en reconnaissant la nécessité de concilier la concurrence et l'innovation, le fait d'assurer l'interopérabilité des plateformes, des agents et des clients est éminemment souhaitable, pour que les clients de différents systèmes puissent se faire des paiements les uns aux autres et que les agents puissent travailler pour différents prestataires. Ceci est particulièrement important pour les clients habitant des zones rurales éloignées.

EXEMPLES DE MESURES DE FACILITATION DE L'INTEROPÉRABILITÉ :

1. Encourager les initiatives d'interopérabilité menées en collaboration et émanant du secteur financier pour faire en sorte que les clients puissent effectuer des transactions financières numériques quels que soient leur lieu de résidence ou leur prestataire de services.
2. Décourager tout obstacle s'opposant délibérément à l'interopérabilité (tels que les accords d'exclusivité conclus avec les agents).

CONTEXTE

L'interopérabilité est une caractéristique indispensable à l'accroissement de l'utilisation des services de paiements numériques. Elle se situe au niveau des plateformes, des agents et des clients, le contenu de ce concept présentant alors certaines variations.

Les recherches du CGAP sur la question distinguent trois formes d'interopérabilité : l'interopérabilité des plateformes, qui permet d'effectuer des paiements entre différents prestataires de services; l'interopérabilité des agents, qui permet à un agent d'agir pour de multiples prestataires de services; et l'interopérabilité des clients, qui permet à un client donné d'accéder à n'importe quel téléphone d'un réseau avec une carte SIM et d'accéder à de multiples comptes au moyen d'une seul carte SIM[20].

5.1 Une démarche coopérative

La présente directive encourage les efforts de coopération déployés par le secteur financier dans le sens d'une augmentation de l'interopérabilité qui bénéficiera aux clients. Ceci devrait se faire idéalement sous la direction des principaux superviseurs, en particulier a cause du risque d'arrangements anti-concurrence qui pourraient enfreindre les lois anti-trust. On peut citer comme exemple de cette démarche, la nouvelle plateforme mobile Bim lancée récemment au Pérou, en un effort de coopération notable entre les autorités gouvernementales, les institutions financières, les opérateurs de télécommunications et diverses autres parties prenantes du pays. Cette plateforme assure l'interopérabilité des services de paiement numériques via tous les réseaux mobiles participants et tous les prestataires de services de paiement et leurs agents[21]. On trouve de même un autre exemple de cette coopération avec la démarche « essai et apprentissage » suivie en Tanzanie. Pour plus de détails, voir le rapport de la Société financière internationale (SFI/IFC) de 2016 intitulé *Tanzania Case Study : Achieving Interoperability in Mobile Financial Services.*

A l'inverse des initiatives du secteur privé est l'adoption par les autorités gouvernementales de mesures réglementaires prévoyant expressément l'interopérabilité. Il en est ainsi, par exemple au Kenya, qui a formulé en 2014 des Règles nationales sur les systèmes de paiements *[National Payment System Regulations]*, contenant l'énoncé suivant « Le prestataire de services de paiements est tenu d'utiliser des systèmes capables de devenir interopérables avec les autres systèmes de paiements dans le pays et sur le plan international » (règle 21.1). Le Nigéria a lui aussi rendu obligatoire l'interopérabilité pour les prestataires de services d'argent mobile en 2012[22].

Diverses organisations internationales promeuvent également l'interopérabilité. Le *Guide du Projet Level One* de la Fondation Gates, par exemple, l'encourage pour les virements et préconise un soutien de l'État à divers niveaux. Les principes guides 3 et 5 du *Rapport PAFI,* appellent à la mise en place d'une infrastructure qui permet l'échange, le traitement, la compensation et le règlement d'instruments de paiement du même type, en sus de canaux d'accès interopérables.

5.2 Obstacles à l'interopérabilité

Il importe également de veiller à ce qu'il n'y ait pas d'obstacles artificiels venant limiter la concurrence et s'opposer à l'interopérabilité. Un exemple classique de ce type d'obstacle est la clause d'exclusivité, interdiction imposée par le prestataire à ses agents de travailler pour d'autres prestataires. Une telle exclusivité peut présenter des inconvénients majeurs pour les clients d'autres prestataires résidant dans la zone considérée et n'ayant pas facilement accès à un réseau d'agents. Un autre exemple est celui de dispositions contractuelles en vertu desquelles les clients d'un prestataire ne peuvent effectuer des paiements qu'à d'autres clients du même prestataire ou ne recevoir de paiements que de ces autres clients. Il est toutefois reconnu qu'il y a lieu de trouver un équilibre entre les préoccupations relatives à la concurrence et la nécessité pour les prestataires de bénéficier d'un rendement approprié de leurs investissements dans l'innovation.

DIRECTIVE 6 : En tant que prestataire de services, assumer la responsabilité des actes de tous les intervenants de la chaîne de valeur

Les clients sont plus susceptibles d'avoir confiance dans les moyens de paiements numériques et de les utiliser si les prestataires de services assument la responsabilité des actes de leurs agents, employés et tiers prestataires de services tout au long de la chaîne de valeur.

EXEMPLES DE RESPONSABILITÉ DES ACTES DES AGENTS, DES EMPLOYÉS ET DES TIERS PRESTATAIRES DE SERVICES :

1. **Responsabilité :** Les prestataires assument la responsabilité des actes et des omissions de leurs agents, employés et tiers prestataires de services.
2. **Formation et supervision :** Les agents et les employés, ainsi que ceux des tiers prestataires de services, sont formés (notamment aux caractéristiques des produits, à leurs responsabilités juridiques et aux comportements sensibles aux sexospécificités) et supervisés de manière appropriée. Ils disposent également des ressources nécessaires pour fournir les services de paiements de manière compétente et conforme aux règlements.
3. **Connaissance des prestataires :** Les agents communiquent aux clients le nom et les coordonnées du prestataire de services lors de l'ouverture de leur compte et sur demande.

CONTEXTE

6.1 Responsabilité

Une des caractéristiques clés d'un marché responsable des paiements numériques est la mise en place d'un mécanisme par lequel les prestataires de services sont tenus responsables des actes et des omissions des personnes qui agissent en leur nom, ainsi que de l'effet de ces actes et omissions sur les clients. Ces personnes sont en particulier les agents et les « tiers prestataires de services », par exemple les gestionnaires des réseaux d'agents. Dans certains pays, la législation en vigueur assure déjà le jeu de cette responsabilité, mais ce n'est pas le cas partout et la question est d'une importance primordiale.

On trouve un exemple de telles dispositions législatives dans la règle 37 du Règlement tanzanien sur l'argent électronique de 2015, dont le libellé est le suivant : « Le prestataire de services de paiements est responsable envers ses clients des actes et omissions de ses agents commis dans le cadre du contrat de représentation ».

La directive 3 de la GSMA couvre également la question de la responsabilité du fait des agents, mais ne mentionne pas les employés ni les tiers prestataires de services. Le Règlement indonésien sur la protection des usagers de systèmes de paiement en donne un autre exemple, en prévoyant que le prestataire est responsable envers ses clients de toute perte découlant d'erreurs commises par les gestionnaires et les employés[23].

6.2 Formation et supervision

Les clients sont en droit de s'attendre à ce que le prestataire de services veille à former et à superviser de manière appropriée ses agents, ses employés et les tiers prestataires de services. Cette formation peut porter, par exemple, sur les caractéristiques et les risques des services de paiement, la façon d'utiliser les services, la façon de communiquer avec les clients, les dispositifs de protection (relatifs, par exemple, aux PIN), les mécanismes de recours des clients et les pratiques interdites (en rapport, par exemple, avec la fraude et la discrimination). La formation devrait inclure aussi les comportements sexospécifiques appropriés, par exemple le fait pour les agents de sexe masculin de ne pas toucher la main des clientes lors de la prise des empreintes digitales en Inde Dans le cas des tiers prestataires de services, ces obligations pourraient être imposées par le biais du contrat de représentation conclu avec le prestataire principal.

6.3 Connaissance des prestataires

En règle générale, le client de services de paiements est appelé à traiter principalement avec un agent du prestataire de services ou même un employé de celui-ci. Mais il est important qu'il connaisse l'identité du prestataire pour pouvoir déterminer s'il souhaite ou non faire usage du produit et, dans l'affirmative, pour savoir à qui il doit adresser d'éventuelles réclamations.

DIRECTIVE 7 : Protéger les données des clients

La protection des données numériques des clients revêt une importance croissante, vu le volume, la vitesse d'utilisation et diversité des données employées pour le marketing et les systèmes de notation de crédit, tout en sachant que l'utilisation des données des clients peut élargir la gamme des produits auxquels ces derniers peuvent avoir accès.

EXEMPLES DE MESURES POSSIBLES DE PROTECTION ÉLÉMENTAIRE DES DONNEES DES CLIENTS DANS UN ENVIRONNEMENT NUMÉRIQUE :

1. **Confidentialité et sécurité :** Des mesures raisonnables sont prises pour assurer la confidentialité et la sécurité des données des clients en rapport avec les paiements numériques. Les données dont il s'agit comprennent, par exemple, l'identité des clients et les informations sur leur contrat, les relevés des transactions; les identifiants; le dispositif utilisé, le téléphone mobile utilisé, les données d'usage d'internet et les données de géolocalisation. Ces données peuvent, avec le consentement exprès et éclairé des clients, être utilisées et divulguées à des fins spécifiques, notamment pour la commercialisation de nouveaux services.
2. **Piste d'audit :** Les clients et les superviseurs ont accès à une piste d'audit claire des relevés de transaction.

CONTEXTE

7.1 Confidentialité et sécurité

La protection des données personnelles et de la vie privée dans le monde du numérique est un problème clé qui est abordé dans le *Rapport final du Ve Forum sur la finance responsable et le Rapport du VIe Forum sur la finance responsable.* Elle est également reconnue comme une question centrale relevant de la réglementation dans le rapport sur les principes de l'inclusion financière novatrice du G20 (2010)[24] "La ligne directrice 7.1 porte sur les préoccupations relatives aux données personnelles sensibles pour les clients des systèmes de paiements numériques, mais ne prétend pas traiter de tous les problèmes potentiels liés aux données. Elle ne traite pas non plus des questions suivantes : droits d'accès et de correction; limites en matière de recueil et d'utilisation des informations personnelles (par exemple à des fins de marketing); limites de durée des périodes de rétention des données; obligation de publier les détails de la politique des prestataires concernant le respect de la vie privée. La ligne directrice 7 n'aborde pas non plus la question de l'analyse des données massives en rapport avec les services de paiements numériques[25].

Il existe divers exemples de principes, de normes et de codes (ainsi que de lois nationales) qui traitent largement les questions relatives à la protection des données, et notamment :

- Les principes de l'inclusion financière novatrice du G20 (2010);
- Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE de 2013;
- La résolution de Madrid de 2009 concernant la *Proposition conjointe visant à établir un projet de normes Internationales sur la protection de la vie privée au regard du traitement de données personnelles.*
- *Les Principes de Windhover pour l'identité numérique, la confiance et les données personnelles* de Data Driven Design de 2014;
- Le principe 6 des Principes de protection des clients de la Smart Campaign (qui limite aussi l'utilisation des données aux activités primaires de recueil, sous réserve du consentement des intéressés); et
- La directive 8 du Code de conduite de la GSMA.

Il existe également des dispositions de niveau national imposant des obligations en matière de protection des données concernant les services financiers numériques, notamment en Indonésie et aux Philippines[26].

7.2 Piste d'audit

La disponibilité d'une piste d'audit permet aux clients d'obtenir des preuves de transactions passées. Ceci peut être d'une utilité particulière dans le cas de différents relatifs aux transactions ainsi qu'à des fins de supervision (par exemple pour déterminer si les dispositions relatives à la protection des fonds des clients ont été respectées).

DIRECTIVE 8 : Offrir des moyens de recours aux clients

Il faut que les clients aient accès à un système de recours équitable pour recevoir leurs réclamations concernant les paiements numériques. Ceci est nécessaire tout particulièrement pour les réclamations ayant trait aux nouveaux produits, mal connus et délivrés par des canaux innovants, et pour les clients en situation d'isolement géographique dont les contacts directs avec les prestataires peuvent être limités, voire inexistants..

EXEMPLES DE SYSTÈMES DE RECOURS EFFICACES POUR LES CLIENTS DES SERVICES DE PAIEMENTS NUMÉRIQUES :

1. **Réclamations :** Les clients ont facilement accès à un système de dépôt de réclamations transparent, gratuit ou peu coûteux, et efficace, système qui, autant que possible, tient compte des clients vulnérables (telles que les personnes handicapées). Un tel système doit être accessible à tous les clients, quelles que soient leurs normes culturelles, leur langue, leur mobilité, etc.
2. **Litiges :** Les clients ont également accès à un tiers indépendant qui traite les litiges avec les prestataires lorsque ceux-ci n'ont pas répondu aux réclamations des clients de manière adéquate et résolu le problème. Ce système de tiers indépendant est d'accès facile (notamment par téléphone ou par voie électronique), transparent, gratuit ou peu coûteux, et efficace.
3. **Informations sur les systèmes de recours :** Les Informations sur le système de recours sont énoncées dans les conditions générales disponibles sur le site Web du prestataire et dans les locaux de celui-ci et de l'agent. En outre, après qu'un client ait déposé une plainte, il leur est communiqué une copie de ces informations, sous forme numérique.
4. **Données relatives aux réclamations :** Les prestataires tiennent des archives contenant les détails des réclamations des clients et de leur réponse à chaque plainte. Des comptes rendus périodiques sur les réclamations sont également communiqués aux autorités de réglementation. Les problèmes systémiques affectant le secteur sont rendus publics, mais sans divulguer l'identité des plaignants

CONTEXTE

8.1 et 8.2 Réclamations et litiges

La *Note d'information du CGAP sur la finance numérique signale* « l'insuffisance des voies de recours pour les clients » parmi les sept principaux risques auxquels sont exposés les consommateurs. Nombre de principes, normes, codes et règlements nationaux traitent de la nécessité de systèmes de recours internes et externes pour les clients, notamment la directive 7 du *Code de conduite* de la GSMA, le principe guide 2 du Rapport PAFI et la directive 7 des Principes de protection des clients de la Smart Campaign[27].

La ligne directrice 8 porte tant sur les systèmes de recours des clients mis en place par les prestataires que sur les systèmes externes de résolution des litiges. Parmi ces derniers, on peut citer à titre d'exemple les systèmes de médiateurs financiers prévus par le secteur financier ou par la loi, ou les services de médiation offerts par une autorité de supervision. Au niveau des pays, figurent parmi les entités de résolution des différends la CONDUSEF du Mexique[28], le nouveau système de médiateur financier de la Malaisie[29], le médiateur des services bancaires de l'Afrique du Sud[30] et l'Office du médiateur du Rwanda[31].

8.3 Informations sur les systèmes de recours

Les clients doivent savoir à qui ils peuvent s'adresser s'ils ont des réclamations à présenter ou des litiges à résoudre et il faut donc veiller à ce que les informations concernant les systèmes de recours soient largement disponibles. De récents sondages effectués à ce sujet par le projet « Voix des clients » *[Client Voice Project]* de

la Smart Campaign ont révélé un manque de connaissances généralisés de la part des clients sur les recours dont ils disposent au Bénin, en Géorgie, au Pakistan et au Pérou (les quatre pays objets de l'enquête), y compris en Géorgie et au Pérou qui semblent posséder un solide cadre juridique de protection des consommateurs[32]. Au Bénin, seuls 14 % des clients enquêtés se souvenaient avoir été informés des modalités de réclamation ou de résolution des problèmes. En Géorgie, au Pakistan et au Pérou, cette proportion était de 37 %, 34 % et 29 % respectivement[33].

Les *Normes de certification - Protection des clients* de la Smart Campaign exigent à présent que « "[l'institution financière] informe les clients du droit de réclamation et des procédures de présentation des réclamations »[34].

8.4 Données relatives aux réclamations

Du point de vue des clients, il est important que les prestataires conservent des traces écrites du traitement et de l'issue des réclamations. Les données doivent aussi être communiquées, autant que possible, à l'entité de réglementation compétente de manière à lui permettre de repérer les problèmes systémiques susceptibles d'affecter les clients. Pour être utiles pour les clients, ces informations devraient, en outre, être publiées.

La ligne directrice 8.4 ne prévoit pas de dispositions concernant la divulgation de l'identité des prestataires lors de la publication d'informations sur les réclamations systémiques. Cependant, de telles données peuvent aider non seulement les clients, et les guider dans le choix d'un prestataire, mais aussi les prestataires eux-mêmes en leur permettant de faire des comparaisons et de se situer par rapport à leurs concurrents. Ces informations pourraient être fournies par un service de supervision ou un médiateur financier. On peut citer en exemples de ce principe le Consumer Financial Protection Bureau des États-Unis[35], qui tient une base de données sur les réclamations, la Financial Conduct Authority du Royaume-Uni[36] qui tient des données sur les diverses institutions financières, et le Bureau des entités financières du Mexique[37], qui publie des informations à ce sujet[38].

Abréviations et acronymes

CGAP	Groupe consultatif d'assistance aux populations pauvres
CGAP – *Note d'information sur la finance numérique*	Note d'information du CGAP : Réussir la finance numérique : pourquoi atténuer davantage les risques pour les clients (2015)
Code des e-paiements de l'Australie (Australia ePayments Code)	ePayments Code, administré par la Commission australienne des valeurs mobilières et des placements
GAFI	*Groupe d'action financière*
GAFI – Recommandations	*Les recommandations du GAFI : Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération* (2012 – Mises à jour en février 2016))
GSMA	Association du Groupe spécial mobile (Association des opérateurs de téléphonie mobile)
GSMA – Code de conduite	Code de conduite des prestataires de service d'argent mobile de la GSMA (2016)
Guide du Projet Level One de la Fondation Gates	The Bill and Melinda Gates Foundation, Guide du Projet Level One : Concevoir un nouveau système pour l'inclusion financière (2015)
LCB/FT	Lutte contre le blanchiment de capitaux et le financement du terrorisme
***Normes de certification* de la Smart Campaign**	*Normes de certification – Protection des clients* de la Smart Campaign (2016)
OCDE	Organisation de coopération et de développement économiques
PSD2	Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015
Rapport du VIe Forum sur la finance responsable	The Responsible Finance Forum VI : Evidence and Innovation for Scaling Inclusive Digital Finance Report 2015
Rapport final du Ve Forum sur la finance responsable	*Responsible Finance Forum V : Responsible Digital Finance Outcomes Report* (2014)
Rapport PAFI	*Payments Aspects of Financial Inclusion Report du Comité sur les infrastructures de paiement et de marché de la Banque des règlements internationaux et de la Banque mondiale* (2016)
Règlement indonésien sur la protection des usagers de systèmes de paiement	Règlement 16/1/PBI/2014 de Bank Indonesia
Règlement tanzanien sur l'argent électronique	Tanzania Electronic Money Regulations, 2015
SFI	Société financière internationale

Références bibliographiques

31e Conférence des commissaires à la protection des données et à la vie privée (2009), Résolution de Madrid sur les Normes internationales relatives à la protection des données personnelles et de la vie privée http ://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf Version française disponible à l'annexe A de https ://www.privacycommission.be/sites/privacycommission/files/documents/normes_internationales_madrid_2009.pdf

Afghanistan : Mobile Service Providers Regulation
http ://www.fintraca.gov.af/assets/pdf/money_service_providers_regulation.pdf

Afghanistan : The Afghanistan Bank Law (2003)
http ://dab.gov.af/Content/Media/Documents/DABLaw211020151441970755332 5325.pdf

Australia ePayments Code (2016)
http ://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf

Bank Indonesia Regulation (2014) No. 16 /1/PBI Consumer Protection in Payment System Service
http ://www.bi.go.id/en/peraturan/sistem-pembayaran/Documents/pbi_160114.pdf

Centre for Financial Inclusion (2016) 'BiM The First Fully - Interoperable Mobile Money Platform : Now Live in Peru'
https ://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru/

Consumer Financial Protection Bureau, (2016) 'Consumer Complaints Database'
http ://www.consumerfinance.gov/data-research/consumer-complaints/

CGAP (2015) 'Réussir la finance numérique'
http ://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015-French.pdf

CGAP (2016) 'Interoperability in Branchless Banking and Mobile Money'
http ://www.cgap.org/blog/interoperability-branchless-banking-and-mobile-money-0

Committee for Payments and Markets Infrastructure of the Bank for International Settlements and the World Bank Group (2016) 'Payments Aspects of Financial Inclusion Report'
http ://pubdocs.worldbank.org/pubdocs/publicdoc/2016/4/963011459859364335/payment-systems-PAFI-Report2016.pdf

Financial Conduct Authority (United Kingdom) (2016) 'Complaints Data'
https ://www.the-fca.org.uk/firms/complaints-data

G20 (2011) 'High-Level Principles on Financial Consumer Protection'
https ://www.oecd.org/daf/fin/financial-markets/48892010.pdf - Version préliminaire en français http ://www.oecd.org/fr/finances/marches-financiers/48521198.pdf

G20 Global Partnership for Financial Inclusion (2016) 'Global Standard-Setting Bodies Financial Inclusion The Evolving Landscape' http ://www.gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-evolving-landscape

G20 Principles for Innovative Financial Inclusion (2010). Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group. https://www.gpfi.org/sites/default/files/documents/Principles%20and%20Report%20on%20Innovative%20Financial%20Inclusion_0.pdf

J Greenacre and RP Buckley, University of New South Wales (2014) 'Using Trusts to Protect Mobile Money Customers'
http ://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454

Groupe d'action financière (2012) 'Normes internationales sur la lutte contre le blanchiment des capitaux et le financement du terrorisme et de la prolifération'
http ://www.fatf-gafi.org/media/fatf/documents/recommendations/Recommandations_GAFI.pdf

GSMA (2014) 'Code de conduite des prestataires de service d'argent mobile'
http ://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/2015_GSMA_Code-de-conduite-des-prestataires-de-services-d'argent-mobile-V2.pdf

ID3 (2014) 'The Windhover Principles for Digital Identity, Trust, and Data' https ://idcubed.org/about/vision-mission-2/

IFC (2016) 'Tanzania Case Study Achieving Interoperability in Mobile Financial Services'
http ://www.ifc.org/wps/wcm/connect/8d518d004799ebf1bb8fff299ede9589/IFC+Tanzania+Case+study+10_03_2015.pdf?MOD=AJPERES

Kenya : The National Payment System Act, 2011 (No. 39 of 2011)
https ://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf

Kenya : The National Payment System Regulations (2014)
https ://www.centralbank.go.ke/images/docs/legislation/NPSRegulations2014.pdf

Malawi Mobile Payments Guidelines (2011)
https ://www.rbm.mw/PaymentSystems/

Nigeria (2012) : Central Bank of Nigeria Direction BPS/DIR/GEN/CIR/01/014
http ://www.cenbank.org/out/2012/ccd/timeline%20for%20interoperability%20&%20interconnectivity.pdf

OCDE (2013) 'Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel'
http ://www.oecd.org/fr/sti/ieconomie
lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm

Philippines Central Bank E-Money Circular 649 (2009)
http ://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf

Responsible Finance Forum V (2014) 'Responsible Digital Finance Outcomes Report'
https ://www.responsiblefinanceforum.org/wp-content/uploads/RFFVSummaryRepor.pdf

Responsible Finance Forum VI (2015) 'Evidence and Innovation for Scaling Inclusive Digital Finance Report'
https ://responsiblefinanceforum.org/wp-content/uploads/RFF6-report-5_21-final-low_res.pdf

Tanzania : The National Payments System Act (2015)
https ://www.bot-tz.org/PaymentSystem/NPS%20Act%202015.pdf

Tanzania : The Electronic Money Regulations (2015)
https ://www.bot-tz.org/PaymentSystem/GN-THE%20ELECTRONIC%20MONEY%20REGULATIONS%202015.pdf

The Bill and Melinda Gates Foundation (2015) 'Guide du Projet Level One : Convevoir un nouveau système pour l'inclusion financière'
https ://leveloneproject.org/wp-content/uploads/2016/08/The-Level-One-Project-Designing-a-New-System-for-Financial-Inclusion_FR.pdf

The Smart Campaign (2011) ''Principes de protection des clients'
https ://centerforfinancialinclusionblog.files.wordpress.com/2012/03/principes-de-protection-des-clients-revises.pdf

The Smart Campaign (2015) 'My Turn to Speak : Voices of Microfinance Clients in Benin, Pakistan, Peru and Georgia'
http ://smartcampaign.org/storage/documents/Synthesis_Report_ENG_FINAL.pdf

The Smart Campaign (2016) 'Normes de certification – protection des clients'
http ://www.smartcampaign.org/storage/documents/Standards_2.0_French.pdf

World Bank (2012) 'Good Practices on Financial Consumer Protection'
http ://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf

Notes finales

1. The Better Than Cash Alliance, Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services (à paraître en août 2016).
2. Voir par exemple le rapport Payments Aspects of Financial Inclusion (PAFI) du Comité sur les infrastructures de paiement et de marché de la BRI et de la Banque mondiale; les Good Practices for Financial Consumer Protection de la Banque mondiale; les Principes de protection des clients de la Smart Campaign; le Guide du Projet Level One : Concevoir un nouveau système pour l'inclusion financière de la Fondation Bill & Melinda Gates; le rapport au G20 de 2016 du Global Partnership for Financial Inclusion intitulé Global Standard-Setting Bodies and Financial Inclusion : The Evolving Landscape; et le Code de conduite des prestataires de service d'argent mobile de la GSMA.
3. À titre d'exemple, voir aussi le Règlement indonésien sur la protection des consommateurs usagers des systèmes de paiements, dont le premier principe (article 3a) est que le traitement des consommateurs doit être « équitable et juste ». Pour un autre exemple, voir le principe 5 des Principes de protection des clients de la Smart Campaign, qui appelle à un traitement respectueux et équitable des clients.
4. Article 8 du Règlement indonésien sur la protection des usagers de systèmes de paiement.
5. Voir la recommandation 10 des *Recommandations du Groupe d'action financière (GAFI) : Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération* (2012) qui exige (entre autres) qu'au titre du devoir de vigilance relatif à la clientèle les institutions financières prennent des mesures pour « identifier le client et vérifier son identité au moyen de documents, données et informations de sources fiables et indépendantes » et qui prévoit que ces institutions « devraient déterminer l'étendue de ces mesures en se fondant sur l'approche fondée sur les risques conformément aux notes interprétatives de la présente recommandation et de la recommandation 1 ». Pour la résumer, la note interprétative de la recommandation 1 indique que, lorsque les risques sont relativement faibles, des mesures simplifiées peuvent être appliquées aux fins de l'identification, de l'évaluation, de la surveillance, de la gestion et de l'atténuation des risques de blanchiment des capitaux et de financement du terrorisme. Toutes les directives énoncées sont, à l'évidence, sous réserve des lois en vigueur et notamment de celles concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT). Par ailleurs, la note interprétative de la recommandation 10 décrit parmi les situations à faibles risques celles qui concernent « les services ou produits financiers qui fournissent des services limités et définis de façon pertinente afin d'en accroître l'accès à certains types de clients à des fins d'inclusion financière ». En outre, la directive 2.5.1 du *Code de conduite des prestataires de service d'argent mobile de l'Association du Groupe spécial mobile* (GSMA) (ci-après the Code de conduite de la GSMA) prévoit que les prestataires « peuvent utiliser une méthode de vérification [de l'identité des clients] adaptée au niveau de risque si les lois et réglementations locales les y autorisent ».
6. *FATF Guidance : Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, (2013),* paragraphe 67.
7. Chapitre C du Code des e-paiements de l'Australie.
8. La *Note d'information du CGAP sur la finance numérique* est fondée sur les constats issus de recherches sur les consommateurs menées dans 16 marchés : Bangladesh, Colombie, Côte d'Ivoire, Ghana, Haïti, Kenya, Inde, Indonesia, Nigéria, Ouganda, Pakistan, Pérou, Philippines, Russie, Rwanda et Tanzanie. Elle présente également les conclusions d'une étude initiale de l'état des efforts d'atténuation des risques déployés par les prestataires de services financiers, ainsi que des règlements et des mesures de surveillance concernant la protection des consommateurs.Cláusulas 14.2 y 14.3 del Código de Pagos Electrónicos de Australia.
9. Clauses 14.2 et 14.3 du Code des e-paiements de l'Australie.
10. Greenacre and Buckley, Using Trusts to Protect Mobile Money Customers, (2014). http ://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454
11. Afghanistan : Da Afghanistan Bank Law and Mobile Service Providers Regulation; Kenya : The National Payment System Act, 2011 (No. 39 of 2011) et The National Payment System Regulations, 2014; Malawi : Guidelines for Mobile Payments Systems; Philippines : BSP E Money Circular 649, 2009; Tanzanie : National Payments System Act, 2015, et The Electronic Money Regulations, 2015.
12. Section 4(H) de la Circulaire 649 des Philippines sur l'argent électronique de 2009 [Circular No. 649 on Electronic Money]
13. Articles 3(c) et 14(2)(c) du Règlement indonésien sur la protection des usagers de systèmes de paiement.
14. Paragraphe 95 de la PSD2.
15. Nigeria Consumer Protection Framework 2016, Section 2.1.6(2)
16. Ibid., voir les articles 71-74 et la définition de « l'authentification forte du client » à l'article 4.
17. Ibid., article 72.
18. http ://www.buro.gob.mx/inicio.php?id_sector=0
19. Voir, par exemple, « Evidence Spotlight : How Commitment Products Break Down Behavioral Barriers to Savings », page 7du *Rapport du VI^e Forum sur la finance responsable.*
20. *Note d'information du CGAP sur la finance numérique*
21. https ://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperablemobile-money-platform-now-live-in-peru
22. Nigeria (2012) Central Bank of Nigeria Direction BPS/DIR/GEN/ CIR/01/014
23. Pages 4 et 8 du Guide du Projet Level One de la Fondation Gates.
24. Article 10 du Règlement indonésien sur la protection des usagers de systèmes de paiement.
25. Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group, page 13
26. Il existe plusieurs définitions des données massives, dites aussi « mégadonnées », mais celle de Gartner est utilisée couramment : Ces données sont « des avoirs d'information de volume, de vélocité et de variété élevés qui exigents des formes de traitement efficaces par rapport au coût et novatrices pour améliorer la compréhension et les processus décisionnels » (voir le glossaire des TI de Gartner, disponible à http ://www.gartner.com/itglossary/big-data).
27. Voir la section 4(H) de la Circulaire 649 des Philippines sur l'argent électronique (2009) et les articles 3(c), 14 et 15 du Règlement indonésien sur la protection des usagers de systèmes de paiement (2014).
28. On trouve un exemple de règlement de niveau national imposant un système interne de réclamations à la section 4(F) de la Circulaire 649 des Philippines sur l'argent électronique (2009), qui exige des émetteurs d'argent électronique qu'ils mettent en place un mécanisme de recours acceptable pour traiter les réclamations des consommateurs. La section 4(G) de la même circulaire exige que des informations sur les procédures de recours soient communiquées aux consommateurs. La règle 45 du Règlement tanzanien sur l'argent électronique (2015) contient des dispositions analogues sur les recours à offrir aux consommateurs..
29. http ://www.condusef.gob.mx/index.php/english
30. http ://www.bnm.gov.my/index.php?ch=en_press&pg=en_press_all&ac=3283
31. http ://www.obssa.co.za/
32. http ://ombudsman.gov.rw/
33. The Smart Campaign, My Turn to Speak : Voices of Microfinance Clients in Benin, Pakistan,Ibid., Figure 27.
34. Ibíd., Figura 27.
35. Principe de protection des clients 7, norme 2.
36. http ://www.consumerfinance.gov/complaintdatabase/
37. http ://www.fca.org.uk/firms/systems-reporting/complaints-data
38. http ://www.buro.gob.mx/inicio.php?id_sector=0

WWW.BETTERTHANCASH.ORG

Au sujet de l'Alliance Better Than Cash

L'Alliance Better Than Cash est un partenariat réunissant des gouvernements, des entreprises privées et des organisations internationales qui s'emploie à accélérer le passage des paiements en espèces aux paiements numériques en vue de réduire la pauvreté et d'instaurer une croissance inclusive. Établie au sein des Nations Unies, l'Alliance possède plus de 50 membres, œuvre en étroite coopération avec d'autres organisations mondiales et est un partenaire de réalisation du Partenariat mondial pour l'inclusion financière du G20.