Banque de la République d'Haïti
Le Gouverneur

Réf. : CA/#21-2010

Le 17 septembre 2010

Monsieur Maxime D. Charles
Président
Association Professionnelle des Banques (APB)
Port-au-Prince

Monsieur le Président,

La Banque de la République d'Haïti (BRH), dans le cadre des mesures visant à promouvoir les activités de la banque à distance et à renforcer le système des paiements en général, vous fait parvenir, ci-joint, les lignes directrices relatives à la banque à distance.

Les présentes lignes directrices fixent les modalités et les différents types de transactions ou services qui peuvent être fournis par les agents de banque à distance.

La Banque de la République d'Haïti vous prie d'agréer, Monsieur le Président, ses salutations distinguées.

Charles Castel

P.O. Box 1570, Port-au-Prince, Haïti. Tél. :299-1244, 299-1200. Fax: 299-1045, 299-1191

LIGNES DIRECTRICES RELATIVES À LA BANQUE À DISTANCE

Conformément aux dispositions de l'article 2 de la loi du 17 août 1979 créant la Banque de la République d'Haïti (BRH), la banque centrale émet les présentes lignes directrices relatives aux activités de « Banque À Distance » (BAD).

Ces lignes directrices s'adressent aux institutions financières admises à recevoir des dépôts. Néanmoins, vu que d'autres acteurs peuvent intervenir lors des activités de banque à distance, ces lignes directrices leur serviront également de guide afin que chacun comprenne son rôle et ses responsabilités.

1. OBJECTIFS

Les objectifs visés par la BRH dans le cadre des présentes lignes directrices sont de:

- promouvoir l'inclusion financière ;
- veiller à ce que les services financiers soient fournis par des institutions financières réglementées ou leurs agents ;
- s'assurer de la conformité des transactions au regard des dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- promouvoir un environnement concurrentiel entre les divers acteurs ;
- protéger les clients.

2. DÉFINITIONS

Aux fins des présentes lignes directrices, on entend par :

- Certificat numérique : document électronique identifiant une personne physique ou morale ou un équipement ;
- Client : titulaire d'un compte domicilié dans une institution financière ou d'un porte-monnaie électronique ;

- Dépôt : tel que défini dans la législation en vigueur ;
- Institution financière : institution admise à recevoir des dépôts ;
- Interopérabilité : capacité d'un système à fonctionner avec d'autres systèmes existants ou futurs et ce, sans restriction d'accès ou de mise en œuvre ;
- Monnaie électronique : valeur monétaire stockée à travers ou sur un support électronique et qui est émise à la réception de fonds et acceptée comme moyen de paiement par des parties autres que l'émetteur ;
- Porte-monnaie électronique : dispositif qui permet de stocker de la monnaie et de régler directement des transactions sur des terminaux de paiement.

3. ACTIVITÉS PERMISES

Dans le cadre des présentes, on entend par opération de « banque à distance » (BAD) toute fourniture de services financiers en dehors des succursales traditionnelles, à travers des agents, en utilisant les Technologies de l'Information et de la Communication (TIC).

Les services financiers qui peuvent être fournis par les institutions financières, selon les limites définies ci-après, sont:

- l'ouverture de compte Banque à Distance (compte BAD): compte ouvert dans une institution financière à travers ses agents ;
- le transfert de fonds : a) transfert par un client de son compte BAD à un autre compte existant en son nom (compte d'épargne, compte courant) ; b) transfert par un client de son compte BAD à celui d'un autre client ;
- les dépôts et retraits : dépôt et retrait de fonds à partir d'un compte BAD en fonction des différentes options offertes par l'institution financière ;
- l'émission de monnaie électronique ;
- le paiement de biens et services : paiement effectué à partir d'un compte BAD pour acheter des biens ou services ;
- le paiement de salaires : paiement effectué par une entreprise à partir de son compte BAD ou de tout autre compte à celui d'un ou de ses employés ;

- le décaissement et remboursement de prêts : le décaissement d'un prêt accordé par une institution financière peut s'effectuer sur le compte BAD de son client ; lequel peut être utilisé par le client pour le repaiement.

Une limite de dix mille gourdes (G. 10,000.00) est appliquée au solde de tout compte BAD. Un maximum de dix mille gourdes (G. 10,000.00) par jour et soixante mille gourdes (G. 60,000.00) par mois est appliqué lors des transferts de fonds. La BRH se réserve le droit de modifier ces limites en fonction de la situation du marché.

4. LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET CONTRE LE FINANCEMENT DU TERRORISME

Les institutions financières doivent s'assurer que les exigences en matière de dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme sont respectées par leurs agents.

Les facteurs à considérer sont :

- les exigences relatives à la connaissance du client « know your customer » (KYC);
- les limites transactionnelles par jour, mois et année en fonction du profil du client ;
- les limites maximales de balance débitrice et créditrice ;
- les exigences de sécurité technologique ;
- l'authentification à deux facteurs pour tout client.

Les institutions financières doivent se conformer aux lois et règlements relatifs à la lutte contre le blanchiment des capitaux et contre le financement du terrorisme.

5. DES INSTITUTIONS FINANCIÈRES

Seules les institutions financières définies ci-devant peuvent exercer des activités de banque à distance et émettre de la monnaie électronique. Toute institution financière doit obtenir l'approbation de la BRH avant le lancement de tout projet de banque à distance. Le dossier

soumis pour approbation doit comprendre au minimum le plan d'affaire, les analyses coûts-bénéfice, les arrangements opérationnels, la technologie adoptée, les accords intervenus entre l'institution financière et ses fournisseurs de services technologiques, la politique de sécurité des transactions, une certification d'une firme reconnue attestant que les exigences en matière de sécurité des transactions sont satisfaites, le système et les procédures de contrôle à mettre en place pour atténuer les risques, les modèles de contrat à intervenir entre l'institution financière et les agents. La BRH peut réclamer tout autre document ou renseignement pouvant l'éclairer sur la faisabilité du projet.

Les institutions financières doivent s'assurer que les clients sont imbus, entre autres, des conditions d'utilisation, de la responsabilité de l'émetteur, des recours en cas de litige.

5.1. Rôle et responsabilités des institutions financières

Dans le cadre des activités de banque à distance, toute institution financière doit:

- s'assurer de l'honorabilité et de l'intégrité de ses agents ;
- superviser ses agents ;
- assumer entièrement la responsabilité des actions ou omissions de ses agents. Cette responsabilité s'étend aux actions de l'agent, même si elles ne sont pas autorisées dans l'accord qui lie les parties, tant qu'elles se rapportent aux services financiers fournis par l'agent ou les questions qui s'y rattachent ;
- maintenir un système efficace de contrôle interne et de supervision des activités de ses agents ;
- élaborer et mettre en œuvre des politiques de sécurité pour protéger les systèmes de communication et de technologie, et les données ;
- accorder une attention particulière au risque de crédit, au risque opérationnel, au risque juridique, au risque de liquidité, au risque de réputation et aux règles de conformité relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- contribuer à la formation de ses agents notamment en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme ;

- pourvoir ses agents des enseignes portant la mention claire et précise « Agent autorisé de X (*nom de l'institution financière*) ».

Par ailleurs, les risques liés à la banque à distance (risques bancaires pour les transactions électroniques) doivent être identifiés, traités et gérés par les institutions financières de manière prudente en fonction des caractéristiques fondamentales et des défis liés aux services bancaires électroniques. En ce sens, les risques technologiques en matière d'information et de sécurité des données dans les réseaux sans fil doivent être correctement identifiés et gérés.

Les institutions financières doivent établir des limites pour la fourniture des services convenus avec leurs agents. Les limites doivent être raisonnables et établies en raison du volume d'argent géré par l'agent et des risques associés à sa localisation géographique pour la conduite des affaires. Les institutions financières doivent fixer des limites pour chaque agent et le cas échéant, pour chaque type de transaction.

Les institutions financières doivent publier et afficher tant dans leurs locaux que chez leurs agents les tarifs et frais appliqués à chaque type d'opérations.

En outre, les institutions financières doivent publier et mettre à jour la liste de tous leurs agents sur leur site Web et dans d'autres publications qu'elles jugeront appropriées. Cette liste doit être, par ailleurs, communiquée à la BRH. La liste des agents doit être diffusée à l'ensemble de leurs branches et transmise à leurs propres agents.

6. DES AGENTS

Dans le cadre des présentes, un agent est une personne physique ou morale liée par un contrat à une institution financière pour offrir certains services financiers au nom de ladite institution.

Peut remplir la fonction d'agent :

a) Toute personne physique ayant un domicile connu, n'ayant pas été déclarée en faillite, n'ayant pas fait l'objet d'interdiction de chéquiers, n'ayant pas de casier judiciaire, et possédant une infrastructure physique appropriée.
b) Toute personne morale ayant une activité commerciale établie depuis au moins 24 mois, n'ayant pas été déclarée en faillite, n'ayant pas fait l'objet d'interdiction de chéquiers, possédant une infrastructure physique appropriée et des ressources humaines capables de fournir les services avec un degré d'efficacité et de façon sécuritaire.

Toute institution financière doit conclure un accord écrit avec l'agent qui agira en son nom. Les modèles de contrat doivent être soumis à la BRH pour approbation. Toute modification subséquente apportée à ces modèles doit être également soumise à la BRH pour agrément.

6.1. Rôle et responsabilités des agents

Un agent est habilité à fournir, dans le cadre des présentes, les services financiers suivants conformément aux termes de l'accord intervenu entre les parties :

a) Ouverture de compte BAD ;
b) Dépôt et retrait de fonds ;
c) Transfert de fonds.

Il revient à l'institution financière de déterminer, en fonction de l'évaluation des risques, quel type de services un agent peut fournir.

Dans le cadre de l'ouverture de compte, l'agent a la responsabilité d'identifier les nouveaux clients conformément aux procédures KYC.

Les agents ne peuvent pas être impliqués dans le marketing et la vente des autres produits de l'institution financière.

Un agent peut fournir ses services à plusieurs institutions financières à condition qu'il ait une entente de services distincte avec chaque institution.

7. NORMES DE SECURITÉ

Les transactions électroniques autorisées seront effectuées si et seulement si elles sont faites de façon sécuritaire. Les transactions de banque à distance utilisent des certificats numériques pour prouver l'authenticité de l'émetteur de la transaction.

Les institutions financières ont l'obligation de s'assurer que les transactions respectent les normes de sécurité généralement admises en matière de technologie de l'information et de la communication. En outre, elles doivent mettre en place des règles et procédures pour sauvegarder les données numériques, incluant les données personnelles des clients.

Les institutions financières doivent en tout temps veiller à la sécurité et à l'efficience des équipements utilisés par leurs agents afin de prévenir toute manipulation ou altération par des personnes non autorisées.

Les institutions financières doivent mettre en place les systèmes qui adressent les points suivants :

a) la sécurité physique et logique ;
b) la disponibilité des services ;
c) la disponibilité, la confidentialité et l'intégrité des données ;
d) le codage des Numéros d'Identification Personnelle (NIP)[1] et des transactions électroniques ;
e) la non-répudiation des transactions ;
f) le traitement des messages d'erreur.

[1] NIP : communément appelé PIN.

8. PROTECTION DU CLIENT

Des systèmes et des procédures appropriés contre les risques de fraude, la perte de confidentialité et la non-disponibilité de services doivent être mis en place par les institutions financières pour protéger les clients.

Les exigences suivantes doivent être respectées en tout temps :

a) les institutions financières doivent mettre en place des mécanismes permettant à leurs clients d'identifier correctement leurs agents et les services fournis par ces derniers ;
b) les agents doivent émettre des reçus pour toutes les transactions qu'ils réalisent. Les institutions financières doivent fournir à leurs agents des équipements capables de générer ces reçus ;
c) un canal de communication pour traiter les plaintes des clients doit être mis en place par les institutions financières. Ces dernières doivent fournir des moyens pour enregistrer les plaintes de leurs clients. Les clients peuvent aussi utiliser ces mêmes moyens pour vérifier avec l'institution financière l'authenticité et l'identité de l'agent, sa localisation et la validité de sa relation d'affaires avec l'institution financière ;
d) les institutions financières doivent établir un mécanisme de traitement des plaintes et s'assurer que ce mécanisme soit communiqué aux clients ;
e) les plaintes des clients doivent être adressées dans un délai raisonnable ne dépassant pas trente (30) jours. Les institutions financières doivent garder l'historique des plaintes et la manière dont ces dernières ont été adressées ;
f) le client doit être sensibilisé sur le fait qu'il doit garder son NIP et toutes informations critiques de manière confidentielle et sur le fait de ne les partager avec personne incluant les agents.

9. SYSTÈME DE PAIEMENTS

Les principes régissant la compensation et le règlement sont applicables aux activités de banque à distance. Toutefois, vu certaines spécificités inhérentes à la banque à distance, une convention devra régir les relations entre les institutions financières et la BRH.

Les transactions sont traitées par le système de paiement de la BRH (Processeur de paiement universel, Règlement Brut en Temps Réel (SPIH), …) qui s'assure de:

a) la compensation et du règlement en temps réel de toutes les transactions ;
b) la sauvegarde de toutes les preuves des transactions ;
c) la réconciliation journalière de toutes les transactions.

10. INTEROPÉRABILITÉ

Tous les processeurs de paiements (Switch), les Guichets Automatiques Bancaires (GAB)[2], les points de vente (POS), les produits tels les cartes ou téléphones mobiles de paiements, déployés ou offerts par les institutions financières doivent être compatibles avec le processeur de paiements de la BRH et interfacés avec cette plateforme et approuvés par la BRH avant tout déploiement.

Pour assurer l'interopérabilité entre les institutions financières, elles devront adopter les formats de message édictés par la BRH.

Ces lignes directrices entrent en vigueur le 1er octobre 2010.

[2] GAB: communément appelé ATM

NOTE ADDITIONNELLE

AUX LIGNES DIRECTRICES SUR LA BANQUE À DISTANCE

INTRODUCTION

La Banque de la République d'Haïti (BRH) émet cette note additionnelle sur les activités de banque à distance en vue d'expliciter certains points traités dans les lignes directrices du 17 septembre 2010. Cette note constitue également un complément aux lignes directrices susmentionnées et fait partie intégrante desdites lignes.

MODÈLE POUR HAÏTI

Seul le modèle basé sur les institutions financières est permis dans le cadre des activités de banque à distance. Ce modèle fait intervenir des technologies, telles que les Terminaux de Paiements Électroniques (TPE), les Guichets Automatiques Bancaires (GAB), les téléphones mobiles, permettant l'identification des clients, l'autorisation des transactions et leur sauvegarde automatique. Ces technologies auxquelles viennent s'ajouter les agents, dans le cas des TPE, servent de canaux de distribution. Dans le cadre de ce modèle, chaque client effectue ses transactions par le biais d'un agent ou au moyen des technologies susmentionnées, et entretient une relation contractuelle directe avec l'institution financière. Ce modèle est implémenté en utilisant des arrangements non exclusifs avec des agents. Des accords peuvent intervenir entre l'institution financière et des compagnies de téléphonie mobile. Seul le modèle « many-to-many »[1] est permis en vertu de ce type de partenariat.

Chaque transaction effectuée par le client doit affecter son compte BAD et non une valeur monétaire stockée sur le moyen utilisé (téléphone mobile, carte de débit). Les balances qui apparaissent sur le téléphone mobile, par exemple, sont le reflet des balances du compte BAD. Conséquemment l'utilisation des termes « monnaie électronique » pour désigner les services décrits dans ces lignes directrices sur la banque à distance est techniquement incorrecte et est interdite.

ACTIVITÉS PERMISES

Le « compte banque à distance » tel que défini dans les lignes directrices est un compte de dépôt à vue domicilié dans une institution financière et qui est affecté au débit et au crédit par des transactions effectuées par son détenteur (le client) à travers des opérations réalisées chez un agent de l'institution financière, ou à travers les moyens de paiement autorisés. Ce compte

[1] Un opérateur de téléphonie mobile peut établir un partenariat avec plusieurs institutions financières et une institution financière avec plusieurs opérateurs de téléphonie mobile.

BAD, utilisé pour des transactions de faible valeur, constitue l'un des moyens de promouvoir l'inclusion financière et d'atteindre la population non encore bancarisée.

Le solde d'un compte BAD ne peut à aucun moment dépasser 10 mille gourdes. Le total des transactions de débit effectué journalièrement ne peut pas dépasser 10 mille gourdes et le cumul des transactions mensuelles ne peut excéder 60 mille gourdes.

Par ailleurs, du fait même que l'émission de monnaie électronique ne peut se faire que par les institutions financières, la BRH se réserve le droit d'émettre des lignes directrices à ce sujet.

MOYENS DE PAIEMENT

Les moyens de paiement liés aux comptes BAD tels que la carte de débit, le téléphone mobile sont utilisés pour autoriser les transactions en temps réel.

Lors des paiements par téléphone mobile, les données personnelles du client (notamment le numéro de téléphone) qui ne sont pas indispensables au déroulement de la transaction ne doivent pas être transmises à des tiers. Les données personnelles ne peuvent en aucun cas être utilisées pour des messages publicitaires.

Du point de vue de la protection des données, il faut que le trafic des paiements par téléphone mobile n'implique pas plus d'exigences en termes de données personnelles que les transactions effectuées avec d'autres moyens de paiement. Le système de paiement doit être conçu de manière à limiter au maximum le risque de perte financière pour le client en cas d'abus.

LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET CONTRE LE FINANCEMENT DU TERRORISME

Selon les recommandations du Groupe d'Action Financière (GAFI) adoptées par Haïti, comme membre du Groupe d'Action Financière de la Caraïbes (GAFIC), les institutions financières ont un devoir de vigilance (due diligence) qu'ils doivent prendre à l'égard de leur clientèle. La recommandation 5 est précise : « *les institutions financières devraient prendre les mesures de vigilance (« due diligence ») à l'égard de leur clientèle, notamment en identifiant et en vérifiant l'identité de leurs clients lorsqu'elles nouent des relations d'affaires* ». La recommandation 5 spécifie : « *Les mesures de vigilance à l'égard de la clientèle sont les suivantes : identifier le client et vérifier son identité au moyen de documents, données et informations de source fiable et indépendante* ».

La recommandation 8 indique que : « *les institutions financières devraient apporter une attention particulière aux menaces de blanchiment de capitaux inhérentes aux technologies nouvelles ou en développement qui risquent de favoriser l'anonymat, et prendre des mesures supplémentaires, si nécessaire, pour éviter l'utilisation de ces technologies dans les dispositifs de blanchiment de capitaux. Les institutions financières devraient notamment*

mettre en place des dispositifs de gestion des risques spécifiques liés aux relations d'affaires ou aux transactions qui n'impliquent pas la présence physique des parties. »

Les institutions financières sont donc tenues de mettre en place des systèmes de suivi permettant d'identifier :

- les transactions inhabituelles et suspectes ;
- les cas où le même compte est utilisé par plusieurs utilisateurs ;
- les cas où le même client ouvre plusieurs comptes.

La responsabilité finale de l'identification du client et de la vérification incombe à l'institution financière.

INTEROPÉRABILITÉ

Pour assurer l'interopérabilité, les institutions financières doivent adopter les formats de message des normes bancaires internationales. Le format standard de message pour les interfaces avec le Processeur National de Paiement est le ISO 8583.

Le client doit être en mesure d'effectuer une transaction de banque à distance sans se soucier de l'institution financière, de l'opérateur téléphonique, de l'agent ou des canaux de distribution utilisés. Ce processus requiert un accord formel entre les différentes parties appelées à intégrer cet environnement interopérable.

Port-au-Prince, le 21 février 2011