GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE CENTRALE (GABAC)

LES NOUVEAUX MOYENS DE PAIEMENT

FACE AUX DEFIS DE LA LUTTE ANTI BLANCHIMENT ET CONTRE LE FINANCEMENT DU TERRORISME DANS LA ZONE CEMAC

AOÛT 2017

Immeuble de la BVM AC - place de l'Indépendance
B.P. : 764 Libreville - Gabon - Tél. : +241 01 76 39 54
Couriel : secretariat@spgabac.org - www.spgabac.org

GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE CENTRALE

Le Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC) est un Organe Spécialisé de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) ayant pour missions :

- La lutte contre le blanchiment d'argent et des produits du crime ;
- La mise en place harmonieuse et concertée des mesures appropriées à cette lutte dans la CEMAC ;
- L'évaluation de l'action et de l'efficacité des mesures adoptées ;
- L'assistance des Etats Membres dans leur politique anti blanchiment ;
- La collaboration avec les structures existant en Afrique et au niveau international.

Le GABAC est membre associé du Groupe d'Action Financière (GAFI) depuis Octobre 2015.

VUE D'ENSEMBLE

Dans la CEMAC (Communauté Economique et Monétaire de l'Afrique Centrale), les banques, les établissements de microfinance (EMF) et les opérateurs de téléphonie mobile ont introduit, au cours de la dernière décennie, des innovations sur les plans technologique et organisationnel afin de renforcer l'inclusion financière des populations n'ayant pas accès aux produits financiers dans la Sous-région. L'une des avancées majeures en la matière a été l'arrivée de la monnaie électronique, matérialisée par les nouveaux moyens de paiement (NMP), comme instruments de règlement.

Toutefois, si les transactions financières qu'ils permettent d'effectuer ne sont pas parfaitement tracées, la large diffusion des NMP peut favoriser la réalisation d'opérations de blanchiment d'argent et de financement du terrorisme.

Il ressort du présent exercice de typologies, qui porte sur les cartes prépayées, les paiements faits au moyen d'un téléphone mobile (mobile money) ainsi que ceux réalisés en ligne sur des sites internet, que le volume des transactions effectuées au moyen des NMP, connaît une forte croissance dans la CEMAC. Le développement étant plus marqué dans certains de ses Etats membres que dans d'autres. Par ailleurs, le manque de traçabilité des paiements réalisés au moyen de NMP, les défaillances des dispositifs réglementaires et de surveillance, et l'anonymat des auteurs de certaines transactions constituent les principaux facteurs de risques de blanchiment d'argent et de financement du terrorisme.

Deux cas avérés de blanchiment d'argent liés à l'utilisation des NMP dans la CEMAC ont été identifiés : l'un se rattache à du blanchiment d'argent au moyen de cartes prépayées et l'autre à travers l'utilisation du mobile money.

La Banque des Etats de l'Afrique Centrale ne disposant pas d'un dispositif de suivi des transactions effectuées au moyen des NMP, le groupe de travail, en charge de la réalisation de cette étude, a rencontré d'importantes difficultés d'accès aux informations dont il avait besoin, tant auprès des banques, des opérateurs de téléphonie mobile que des organes de supervision et des autorités en charge du contrôle et de la lutte contre le blanchiment d'argent et du financement du terrorisme ■

SOMMAIRE

INTRODUCTION

Si un nombre considérable de transactions financières est réalisé dans les systèmes financiers informels, le taux de bancarisation dans la zone CEMAC, 11% en moyenne, constitue un frein au développement des échanges commerciaux (Mayoukou, 2000, Lelart, 2002). La faible proportion de la population active ayant accès aux services bancaires ne favorise pas une forte inclusion financière, facteur de croissance économique socialement et politiquement soutenable sur le long terme (Levine, 2003, Adrianaivo et Kpodar, 2012, Babajide, 2015).

En d'autres termes, dans les pays de la CEMAC, une frange importante des populations exclue du système financier, mais économiquement actives, vit en dehors de l'économie formelle, en particulier dans les zones péri-urbaines et rurales, dans lesquelles la densité des agences bancaires est très faible. Bien plus, celle de la population qui y a accès ne fait pas toujours un usage systématique des services financiers qui lui sont offerts.

C'est dans cet environnement que les banques, les établissements de micro finances (EMF) et les opérateurs de téléphonie mobile implantés dans la CEMAC ont introduit, au cours de la dernière décennie, des innovations sur le plan technologique et de l'organisation, afin de favoriser l'inclusion financière des populations vivant dans la Sous-région. L'une des initiatives majeures en la matière a été l'arrivée de la monnaie électronique, matérialisée par les NMP, comme instrument de règlement.

Le règlement n°01/11/CEMAC/UMAC/CM définit la monnaie électronique comme « une valeur monétaire incorporée sous forme électronique contre remise de fonds de valeur égale, qui peut être utilisée pour effectuer des paiements à des personnes autres que l'émetteur, sans faire intervenir des comptes bancaires dans la transaction ». Les instruments de la monnaie électronique qui font l'objet de cette étude sont constitués des cartes prépayées, des paiements par internet et de ceux effectués au moyen d'un téléphone portable, dits « mobile money ». Ils sont généralement regroupés sous l'appellation de nouveaux moyens de paiement (NMP).

Malgré leur adoption relativement tardive dans la CEMAC, comparativement d'autres sous-régions africaines[1] , ces instruments connaissent depuis leur introduction, une évolution significative tant en nombre d'instruments émis qu'en volume des transactions effectuées.

1 L'exemple du Kenya est souvent présenté. Ce pays de l'Afrique de l'Est connait un des plus importants développements en matière de mobile money en Afrique.

L'adoption de stratégies nationales d'inclusion financière élaborées par plusieurs Etats membres de la CEMAC, ainsi que l'adoption et la mise en vigueur de textes réglementaires favorisant le développement de l'offre et de la demande en NMP contribuent à la diffusion de ces instruments financiers dans la CEMAC. Toutefois, il est apparu que les défaillances des systèmes financiers à maîtriser les transactions financières effectuées au moyen des NMP peuvent favoriser le blanchiment d'argent et le financement du terrorisme. Deux phénomènes qui constituent une menace pour la stabilité financière et la prospérité économique des Etats (Lawack, 2013). En ce qu'ils peuvent compromettre l'intégrité du système financier, fausser l'allocation des ressources financières, notamment en donnant une mauvaise orientation des investissements dans l'économie d'une part, et un vecteur d'insécurité dont certains pays de la sous région paient un lourd tribut. Il serait donc indispensable de mieux encadrer et de maîtriser l'utilisation des NMP, afin de réduire les risques de blanchiment de capitaux et de financement du terrorisme dans un contexte d'instabilité préoccupant.

Le blanchiment des capitaux est défini à l'article 1er du règlement N°01/CEMAC/UMAC/CM portant prévention et répression du blanchiment des capitaux et du financement du terrorisme en Afrique Centrale comme: *« a) la conversion ou le transfert de biens provenant d'un crime ou d'un délit au sens des textes applicables dans l'Etat membre ou du présent Règlement, dans le but de dissimuler ou de déguiser l'origine illicite desdits biens et d'aider toute personne qui est impliquée dans la commission de ce crime ou délit à échapper aux conséquences juridiques de ses actes... [2] ».* Ouverte à une large clientèle, les nouveaux moyens de paiement pourraient être un instrument au service de délinquants et des personnes coupables d'activités de blanchiment de capitaux ou de financement du terrorisme.

Tout comme le blanchiment des capitaux, le financement du terrorisme est défini dans le même Règlement comme le « *fait pour toute personne de fournir ou de réunir par quelque moyen que ce soit, directement ou indirectement, illicitement et délibérément, des fonds dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés en tout ou partie, en vue de commettre : a) un acte qui constitue une infraction de terrorisme selon la définition de l'un des traités internationaux pertinents régulièrement ratifié par l'Etat membre ;... ».* A la lumière de cette précision, les NMP pourraient constituer un moyen de stockage, de transport, de règlement et de transfert de fonds destinés à des activités terroristes. La conjoncture des Etats de la CEMAC, notamment celle du Cameroun, de la RCA et de la République du Tchad avec les mouvements insurrectionnels et terroristes tels Boko Haram, Seleka, Anti Balaka, impose certainement un encadrement efficace de l'utilisation des NMP.

2 Règlement N°01/CEMAC/UMAC/CM portant prévention et répression du blanchiment des capitaux et du financement du terrorisme et de la prolifération en Afrique Centrale du 16 avril 2016, article 8 a)

OBJECTIFS

Entre autres, et conformément à ses termes de référence, l'objectif de cet exercice de typologies est de rendre compte des développements des NMP dans la sous région, faire une analyse comparative de différentes approches réglementaires susceptibles de réguler et de superviser le phénomène des NMP et qui maintiennent un équilibre entre la nécessité de promouvoir l'inclusion des couches de populations qui n'ont pas accès au système financier et la lutte contre le blanchiment d'argent et le financement du terrorisme ; identifier les risques et les vulnérabilités spécifiques inhérents aux NMP suivants : cartes de débit prépayés, les systèmes de paiements en ligne (y compris la monnaie virtuelle) et les Services de paiement via les téléphones mobiles ; et enfin, sur la base d'études de cas effectuées autant que possible dans la sous région, dresser les modes opératoires et les tendances de l'utilisation abusive des NMP à des fins de blanchiment d'argent et de financement du terrorisme en Afrique Centrale.

MÉTHODOLOGIE

C'est au regard des développements qui précèdent que, à la suite d'un séminaire atelier organisé sur le thème, le Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC), a institué un groupe de travail, auquel a été confiée la tâche de mener un exercice de typologies couvrant cinq des six Etats de la CEMAC[3] et visant à détecter et endiguer les vulnérabilités au blanchiment d'argent et au financement du terrorisme inhérentes à l'utilisation des NMP.

Ce groupe était composé de quarante membres issus des autorités nationales en charge de la régulation et de la supervision du secteur financier, des poursuites pénales et des enquêtes de police judiciaire (Finances, Justice et Sécurité), des établissements de crédit, des sociétés de téléphonie mobile offrant les NMP dans les Etats de la Sous-Région, des cellules de renseignement financier ainsi que, des autorités régionales en charge de la supervision et du contrôle du système financier en Afrique Centrale (Banque des Etats de l'Afrique Centrale et Commission Bancaire de l'Afrique Centrale).

Les informations ont été recueillies auprès des organismes sous régionaux de régulation et de supervision, des cellules de renseignement financier, des autorités nationales de supervision et de contrôle du secteur financier, des autorités de poursuites, des établissements de crédit et des opérateurs de téléphonie mobile.

3 La Guinée Equatoriale n'a pas contribué aux travaux

Le groupe de travail a élaboré des questionnaires, qu'il a adressés aux administrations et entités ci-dessus évoquées. Les retours des enquêtes révèlent que trois (03) questionnaires ont été respectivement renseignés par les agents des autorités en charge du contrôle et de la lutte contre le blanchiment d'argent et par les autorités de contrôle et de supervision. Par ailleurs, dix (10) questionnaires ont été renseignés par les agents de banque et de société de téléphonie mobile. Les données tirées des questionnaires ont été complétées par la conduite d'entretiens semi-directifs auprès des acteurs du système financier. Treize (13) entretiens ont été menés auprès des autorités de régulation et de contrôle, et onze (11) autres auprès des agents de banque et de société de téléphonie mobile. Le traitement de ces données a conduit à la formulation de propositions.

Le présent rapport d'étude est constitué de cinq chapitres : le premier donne une brève revue des écrits sur les NMP; le deuxième est consacré à l'état des lieux des NMP dans la CEMAC; le troisième propose une cartographie des risques liés aux NMP; le quatrième est consacré à l'étude des cas de typologies, le cinquième enfin, est consacré aux recommandations ■

CHAPITRE I

Revue de la littérature en matière d'inclusion financière.

Plus d'un milliard de personnes vivent avec moins de 500 FCFA[4] par jour, et plus de trois milliards avec moins de 1000 FCFA. 825millions de personnes, dont 200 millions d'enfants, souffrent de faim dans le monde, principalement dans les pays du sud (Attali, 2006). L'essentiel de ces personnes vivent en marge des systèmes financiers classiques. Cependant, l'inclusion financière peut constituer une solution au problème de financement de ces individus et une voie d'amélioration de leurs conditions de vie (Mosley et Hulme, 1996, Helms, 2006).

Depuis longtemps, la microfinance est présentée comme le principal instrument de lutte contre la pauvreté et d'inclusion financière des personnes exclues dans les pays sous-développés. En accédant aux services de la microfinance et particulièrement au microcrédit, leurs bénéficiaires, en grande majorité les pauvres, peuvent réaliser des activités génératrices de revenus (Armandariz de Aghion et Morduch, 2005, Lelart, 2005). Avec les revenus ainsi dégagés, ils peuvent satisfaire leurs besoins élémentaires, comme se vêtir, se nourrir, se soigner, assurer les frais de scolarité des enfants, entre autres.

Toutefois, l'accès difficile à la microfinance pour des personnes démunies, qui dérive de la quête du profit pour certaines EMF, remet en question le ciblage des pauvres par ces institutions (CGAP, 2001). Il réduit les possibilités de la microfinance de servir les plus pauvres et d'assurer une inclusion financière des indigents (Helms, 2006). La microfinance en Afrique Centrale, étant davantage commerciale, présente des limites pour contribuer à l'inclusion financière de la totalité des populations (Servet et fall, 2010).

Selon l'étude[5] qu'elle a menée, l'Association GSM estime que « dans de nombreux pays en développement, les opérateurs mobiles ont mieux réussi à atteindre les consommateurs non bancarisés que les banques. Les services d'argent mobile fournissent une occasion unique de faire passer les clients disposant d'un téléphone mobile mais ne disposant pas d'un compte bancaire, d'un système de paiement en argent liquide à un système financier formel qui leur donne accès à une variété de services financiers,

4 Un euro = 655,96 FCFA
5 L'argent mobile au service des personnes non bancarisées (Maria solin, Andrew Zerzan, 2009)

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

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

Depuis leur apparition, le mobile money et les autres NMP ont facilité l'accès aux services financiers à des personnes se trouvant en marge des systèmes financiers classiques (Klein et Mayer, 2011, Donovan, 2012, Lal et Sachdev, 2015). Avec ces nouveaux instruments, des milliards de personnes effectuent des transactions financières dans le monde (Châtain et al, 2008). Dû en partie au dynamisme de la microfinance, le taux de bancarisation se situe autour de 20 % (supérieur au taux moyen dans la zone CEMAC) au Cameroun. Concernant l'utilisation du téléphone mobile, dans ce même pays, le taux de pénétration de ce dernier est passé de 9,8 % en 2004 à 71 % en 2014, avec un nombre d'abonnés de l'ordre de 18,6 millions et un marché potentiel de près de 15 millions pour le mobile money[6] . Au Gabon le nombre d'abonnés avoisine trois millions en 2014[7] , alors qu'il est de 4,59 millions en République du Congo en 2015[8] . Au Tchad, le taux de pénétration du téléphone mobile est passé de 0,07% en 2000 à 39,75% en 2014. Les NMP, et en particulier le mobile money, favorisent dans ces pays, un accès facile aux services financiers à une large catégorie de la population ne disposant pas d'un compte bancaire.

Toutefois, il faudrait reconnaître que l'utilisation des NMP expose le système financier à d'importants risques de blanchiment d'argent et de financement du terrorisme. Ceux-ci sont fortement tributaires de plusieurs facteurs qui déterminent leur occurrence (Di Castri, 2013). L'un des facteurs majeurs de

6 Ces statistiques sont tirées du Journal Investir au Cameroun no38 de juin 2015. Plusieurs articles de ce numéro sont consacrés à l'utilisation du mobile money dans le pays.

7 http://www.lenouveaugabon.com/telecom/1006-9149-gabon-1-million-d-internautes-3-millions-d-abonnes-au-mobile

8 http://www.afrique-it.com/web-tech/analyse-comparative-de-la-telephonie-mobile-au-congo-brazzaville-arpce/

ces risques est la défaillance de la technologie qui conduit les organisations à mettre en place des processus automatisés. Ces processus sont alors peu efficaces à endiguer les risques évoqués, étant donné que les phénomènes étudiés sont très complexes et évolutifs. L'utilisation de ces moyens de mobilisation de la monnaie électronique, qui n'est pas toujours connectée à une institution financière, et peut rapidement passer d'un acteur à un autre, rend difficile la connaissance des identités des multiples personnes impliquées (Demetis, 2010, P09). La fausse identité des utilisateurs, le caractère fragmenté des transactions, et la rapidité de celles-ci, qui peuvent être réalisées en tout lieu et à tout moment, sont autant de facteurs qui favorisent la survenance de ces risques (Chatain et al, 2008).

La combinaison de ces différents facteurs de risque dans des contextes variés, a donné lieu à des cas typologiques de blanchiment d'argent et de financement du terrorisme. Une étude du contexte français[9] a permis de dégager plusieurs cas de blanchiment d'argent par le biais des NMP. Ces cas ont porté sur (1) l'exercice illégal de la profession de banquier au moyen d'une monnaie virtuelle qui n'a pas cours légal (bitcoin), (2) la complexité de la détection de l'origine des fonds et la distribution de cartes prépayées par un acteur opaque, (3) l'utilisation des cartes prépayées dans un schéma frauduleux.

Par ailleurs, une étude du contexte coréen portant exclusivement sur le mobile money a conduit à l'identification d'une typologie de cas de blanchiment d'argent. L'un des cas est relatif au jeu cybernétique. Il consiste à ce qu'une personne utilisant une fausse identité, participe à des jeux illégaux d'argent sur internet. Pour ce faire, elle engage des employés étrangers et des complices, pour lui permettre de déposer ses gains, tirés du jeu, auprès de banques coréennes. Un autre cas porte sur des transferts d'argent transfrontaliers : une personne, utilisant également de fausses identités, ouvre plusieurs comptes dans des banques. Ces comptes lui servent par la suite à recevoir d'importantes sommes d'argent sur une courte période. Les fonds qui lui sont envoyées par de multiples personnes dont les identités sont fausses, sont ensuite utilisées pour la réalisation de transactions sous forme de mobile money. Un dernier cas concerne l'escroquerie par le canal d'un fond d'investissement, créé à des fins frauduleuses. Les investisseurs attirés par la promesse d'un retour sur investissement élevé, envoient des montants considérables d'argent au fond d'investissement au moyen du mobile money (Chatain et al, 2008, p15).

9 TRACFIN, Monnaies électronique, monnaies virtuelles et nouveaux risques

Les études menées en Europe et en Asie montrent que les typologies de blanchiment d'argent et de financement du terrorisme sont tributaires de la zone dans laquelle les transactions sont réalisées. Cette approche contingente du phénomène exige donc une analyse particulière dans le cas de la CEMAC pour mieux cerner la forme que peuvent y prendre le blanchiment d'argent et le financement du terrorisme par le biais des NMP ■

CHAPITRE 2

Etat des lieux sur les nouveaux moyens de paiement dans la CEMAC

Avant d'appréhender les phénomènes de blanchiment d'argent et de financement du terrorisme liés aux NMP dans la CEMAC, il est apparu nécessaire de procéder à un état des lieux de leur émission et de leur diffusion dans la Sous-région afin d'en connaître les intervenants, ceux qui y ont recours, le type de transactions financières qu'ils permettent de réaliser et le dispositif réglementaire et de supervision qui s'applique à ces moyens de paiement.

2.1 Dispositif réglementaire relatif aux nouveaux moyens de paiement.

Le dispositif réglementaire qui régit les NMP dans la CEMAC s'inscrit dans le cadre du projet de modernisation des systèmes et moyens de paiement mis en place par la Banque des Etats de l'Afrique Centrale (BEAC) en 1999, en vue de moderniser ces systèmes et de limiter l'utilisation des espèces dans la Sous-région. Dans le cadre de ce projet, un dispositif réglementaire a été constitué sous forme de des règlements et instructions suivants :

- Règlement N°01/CEMAC/UMAC/CM du 11 avril 2016 portant prévention et répression du blanchiment d'argent et du financement du terrorisme et de la prolifération en Afrique Centrale.
- Règlement nº 02/03/CEMAC/UMAC/CM du 04 avril 2003 relatif aux systèmes et moyens de paiement ;
- Règlement COBAC R-2005/01 relatif aux diligences des établissements assujettis en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme en Afrique Centrale ;
- Règlement COBAC R-2005/02 relatif aux établissements de monnaie électronique ;
- Règlement nº01/11/CEMAC/UMAC/CM du 18 septembre 2011 fixant les conditions d'exercice de l'activité d'émission de monnaie électronique, ainsi que les rôles des autorités de régulation ;
- Instruction nº01-GR du 31 octobre 2011 du Gouverneur de la BEAC, relative à la surveillance des systèmes de paiement par monnaie électronique, avec en annexe un cadre référentiel recensant les éléments permettant à la BEAC d'assurer sa mission de surveillance de l'activité ;
- Instruction nº 02/GR/UMAC du 07 mai 2014 du Gouverneur de la BEAC,

relative à la mise en place du multibanking dans le cadre de l'activité d'émission de la monnaie électronique.

2.2 Evolution de la réglementation relative aux nouveaux moyens de paiement.

La modernisation progressive des systèmes et moyens de paiement dans la sous-région Afrique centrale, a conduit à l'adoption de la monnaie électronique, dont les différents supports sont regroupés sous l'appellation NMP, comprenant, comme indiqué, les cartes prépayées, la téléphonie mobile (mobile money), et les paiements par internet.

La réglementation régissant la monnaie électronique porte d'abord sur les textes communautaires relatifs aux moyens de paiement. Elle est par la suite complétée par le règlement n° 01/11/CEMAC/UMAC/CM, l'instruction n° 01/GR du Gouverneur de la BEAC, ainsi que par l'instruction n° 02/GR/UMAC du 07 mai 2014. Ces textes traitent :

- des définitions ;
- de l'objet et du champ d'application;
- des conditions d'exercice de l'activité d'émission de monnaie électronique;
- du régime d'émission de la monnaie électronique et de sa conversion en monnaie fiduciaire ou scripturale ;
- de la régulation, du contrôle et de la surveillance de l'activité d'émission de la monnaie électronique ;
- de la cessation de l'activité d'émission de monnaie électronique ;
- des dispositions transitoires et finales.

Ils définissent la monnaie électronique comme une valeur monétaire incorporée sous forme électronique contre remise de fonds de valeur égale, qui peut être utilisée pour effectuer des paiements à des personnes autres que l'émetteur, sans faire intervenir des comptes bancaires dans la transaction. La monnaie électronique est ainsi principalement caractérisée comme étant :

- une créance dont le détenteur dispose à l'égard de l'émetteur, et dont il peut à tout moment réclamer le remboursement du solde ou de la valeur détenue non utilisée ;
- un instrument électronique, car des dispositifs électroniques (cartes prépayées, mobile money, serveur d'ordinateur) en facilitent le stockage et

la gestion à distance, ainsi que son utilisation dans les transactions financières et commerciales ;

- un moyen d'échange qui peut être utilisé à des fins de paiement auprès des tiers autres que l'émetteur de monnaie électronique, ou de transfert de fonds entre particuliers, ou encore de retrait d'espèces à un distributeur automatique de billets.

Ils octroient l'exclusivité de l'exercice de l'activité d'émission de monnaie électronique aux seuls établissements de crédits. Par ailleurs, ils déterminent le contenu des contrats conclus entre les établissements émetteurs et les porteurs, les accepteurs, et assignent la régulation et le contrôle de cette activité à la COBAC et la BEAC. Aussi, ils introduisent pour ces établissements de crédit une obligation d'information et de renseignement et étendent le contrôle de cette activité aux partenaires techniques et commerciaux. (Ndjimba[10], 2016).

Ce dispositif réglementaire décrit le rôle des intervenants dans l'activité de monnaie électronique et les conditions de son exercice. Il a été complété par des dispositions sur le multibanking, qui visent à garantir l'interopérabilité dans les transactions par monnaie électronique dans la CEMAC. Le cadre juridique CEMAC relatif aux NMP est, dans les grandes lignes, proche de celui de la UEMOA. Cela, notamment, en ce qui concerne les conditions d'obtention de l'autorisation d'exercer et les conditions d'exercice elles-mêmes (Ndjimba, 2016). Toutefois, l'utilisation des NMP véhicule des risques de plusieurs natures, parmi lesquels ceux de blanchiment de capitaux et de financement du terrorisme, que la réglementation en vigueur, avec l'apport supplémentaire des règlements adoptés par la COBAC, tente d'encadrer.

2.3 Dispositions réglementaires en matière de lutte anti blanchiment et contre le financement du terrorisme liés aux nouveaux moyens de paiement

Le dispositif règlementaire préconise la mise en place de procédés et de diligences de lutte anti-blanchiment d'argent et contre le financement du terrorisme pour pallier les vulnérabilités liées à l'utilisation des NMP. Ainsi, le règlement n° 01/CEMAC/UMAC/CM du 16 avril 2016 portant sur la prévention et la répression du blanchiment des capitaux et du financement du terrorisme en Afrique centrale, et les règlements de la COBAC, prévoient l'adoption des diligences telles que :

10 Le document cité a été rédigé par le Docteur NDJIMBA, dans le cadre de sa collaboration avec le GABAC. Il est répertorié en annexe du présent rapport.

- la connaissance de la clientèle (Know Your Customer, ou le sigle «KYC»): à ce titre, tout établissement assujetti doit, avant l'établissement d'une relation d'affaires, prendre des mesures de vigilance (« due diligence ») à l'égard de ses nouveaux clients. Elles consistent dans la vérification de l'identité du client, par l'exigence de la présentation d'un document officiel original en cours de validité, ainsi que dans la vigilance sur la provenance des fonds, et l'identification des bénéficiaires et des personnes qui contrôlent ces fonds ;
- la connaissance des relations d'affaires du client : elle vise à estimer le nombre de ses relations commerciales. Cette diligence doit être effectuée chaque fois que surviennent des changements importants dans l'activité du client. Ce faisant, l'assujetti peut apprécier la légitimité des opérations effectuées et détecter celles suspectes, le cas échéant ;
- le contrôle des transactions : les établissements assujettis doivent exercer une vigilance constante sur leurs relations d'affaires, et assurer un examen attentif de leurs transactions pendant toute la durée de la relation. La cohérence des transactions effectuées par les clients avec la connaissance actualisée de ces derniers, que les établissements assujettis sont tenus de mettre en œuvre, est ainsi assurée. Cette diligence est facilitée par la mise en place de systèmes informatisés permettant la détection d'opérations atypiques, compte tenu du profil du client ;
- La déclaration de soupçon : les établissements assujettis ont l'obligation de désigner au moins un correspondant ANIF (Agence Nationale d'Investigation Financière) et COBAC, dont l'identité est leur communiquée ; ils doivent également déclarer par écrit, ou, si nécessaire, verbalement, avant ou après exécution, toute opération objet de soupçon. Tout dirigeant ou agent non officiellement désigné d'un assujetti est autorisé à déclarer les soupçons de blanchiment de capitaux et de financement du terrorisme en cas d'urgence ;
- La centralisation des informations sur l'identité des clients, donneurs d'ordre, bénéficiaires et sur les transactions. A travers cette diligence, il a été prévu la création dans chaque Etat membre de la CEMAC, de fichiers nationaux composés entre autres, du fichier des incidents de paiement par chèque et par carte de paiement, ainsi que celui des chèques et cartes irréguliers. Les informations contenues dans ces fichiers sont réservées aux établissements assujettis à des fins de profilage de leur clientèle, aux officiers de police judiciaire, aux magistrats dans le cadre d'une procédure judiciaire, aux cellules de renseignement financier et aux autorités sous régionales et nationales de supervision et de contrôle ;
- La communication des informations: la BEAC et les autres assujettis doivent communiquer toute information utile à la répression de la criminalité financière aux cellules de renseignement financier aux autorités de poursuite habilitées et aux parquets.

Une analyse comparée plus fine des cadres juridiques de la CEMAC et de la UEMOA, permet de déceler ses nombreuses faiblesses. Celles-ci se rattachent à l'encadrement juridique de l'activité d'émission de la monnaie électronique et aux mesures relatives à la lutte contre le blanchiment des capitaux par le biais des NMP (Ndjimba, 2016).

Sur l'encadrement juridique de l'activité d'offre de NMP, l'essentiel des dispositions dans la CEMAC tendent à poser des principes génériques sans formuler de réelles obligations contraignantes. Aussi, il est observé une absence de dispositions portant sur les rapports entre les établissements de crédit et leurs partenaires, une absence d'obligation de contrôle interne et le défaut de précision de la responsabilité des établissements émetteurs quant aux activités de leurs partenaires. Par ailleurs, le caractère limité de l'obligation de traçabilité qui n'est que de trois (03) ans dans la CEMAC, alors qu'elle est de dix (10) ans dans la UEMOA constitue une insuffisance.

Le cadre juridique CEMAC se caractérise par une certaine vacuité sur la lutte contre le blanchiment des capitaux et le financement du terrorisme via les NMP. Contrairement à celui de la UEMOA, il n'indique pas clairement l'assujettissement des différents acteurs aux règles communautaires relatives à ces phénomènes.

Il ressort de ce qui précède que si le dispositif juridique de la CEMAC vise à encadrer l'utilisation de la monnaie électronique dans la sous région, il ne prend pas en compte de façon adéquate les objectifs de lutte contre le blanchiment des capitaux et le financement du terrorisme tels qu'ils sont prévus par le Règlement 01/CEMAC/UMAC/CM du 16 avril 2016 portant prévention et répression du blanchiment des capitaux et du financement du terrorisme et de la prolifération en Afrique Centrale.

Ceci dit, la maîtrise des risques de blanchiment de capitaux et de financement du terrorisme inhérents à l'utilisation des NMP exige, outre un cadre réglementaire adéquat, une connaissance approfondie de l'offre et de la demande de ces instruments dans la Sous-région CEMAC.

2.4 Le marché des nouveaux moyens de paiement dans la CEMAC

Depuis quelques années, les NMP font l'objet d'une utilisation croissante dans la CEMAC. Ce marché, bien que comportant plusieurs acteurs, demeure toutefois embryonnaire, à l'image de celui des cartes bancaires traditionnelles, encore peu développé.

2.4.1 Les cartes prépayées

Dans le système bancaire de la Sous-région, deux types de cartes bancaires circulent : les cartes de débit, rattachées à un compte bancaire, et les cartes prépayées. Seules les cartes prépayées feront l'objet de cette étude.

Les cartes de débit sont adossées à un compte bancaire. Elles permettent à leurs porteurs de retirer des espèces dans des distributeurs automatiques de billets (DAB) et d'effectuer des paiements, soit chez des commerçants équipés de terminaux de paiement électronique (TPE), soit en ligne auprès de fournisseurs et de banques proposant ce type de règlement. Ces cartes, qui se présentent sous la forme d'un support plastique muni d'une puce, sont personnalisées et fonctionnent généralement par la saisie d'un code confidentiel. L'utilisation de certaines cartes bancaires peut être limitée à un pays ou à un réseau bancaire. Cependant, les cartes se rattachant aux circuits de paiement internationaux tels que VISA ou MASTERCARD, peuvent être utilisées partout dans le monde, dès lors que la fonctionnalité le permettant a été activée.

N'ayant pas encore adopté les cartes prépayées dans les produits qu'elles proposent à leur clientèle, la grande majorité des banques de la sous-région CEMAC continue d'offrir uniquement des cartes de débit dont la croissance est proportionnelle au taux de bancarisation des bénéficiaires.

Le cas de la banque Crédit du Congo est illustratif de cette tendance.

Sur les dix dernières années cette banque émet en moyenne 26.729 cartes de débit par an. Entre 2004 et 2013, le nombre annuel de cartes émis est quasi-stable. Avec un pic en 2014 où l'mission des cartes prépayées connaît une augmentation de près de 25%, le nombre de cartes émis cette année-là est de 33.397.

Contrairement aux cartes de débit, les cartes prépayées, quant à elles, ne sont pas rattachées à un compte bancaire.

La carte prépayée en zone CEMAC est un instrument de paiement électronique au sens du règlement N°01/11-CEMAC/UMAC/CM du 18 septembre 2011. Il s'agit d'un ensemble de *« signaux enregistrés dans une mémoire informatique incorporée dans une carte nominative fournie par un émetteur à un porteur[11] ».* L'essor des Technologies de l'Information et de la Communication (TIC) –principalement de la téléphonie- et la volonté affirmée des pays en voie de développement de réduire le phénomène d'exclusion financière, ont favorisé le développement et l'expansion de l'offre de cartes prépayées.

11 Règlement N° 01/11-CEMAC/UMAC/CM relatif à l'exercice de l'activité d'émission de monnaie électronique, article 1er.

La carte prépayée fonctionne comme une carte de débit traditionnelle. En effet, le porteur ne peut effectuer des paiements et/ou des retraits qu'à concurrence de la valeur monétaire qui y est stockée. Seulement, contrairement à la carte de débit, la possession d'une carte prépayée n'est pas subordonnée à la détention d'un compte bancaire. Elle reste toutefois rattachée à un compte de monnaie électronique ou porte monnaie électronique et ne peut être émise que par un établissement expressément habilité. En Afrique Centrale, seuls les établissements de crédit sont autorisés à émettre la monnaie électronique.

Comme avec un porte-monnaie électronique, le porteur de la carte doit la charger à hauteur d'un certain montant. Chaque fois qu'il réalise une opération d'achat ou de retrait, les montants et les frais associés sont soustraits du solde. Et lorsque le solde est épuisé, le porteur doit recharger la carte pour effectuer de nouvelles transactions. L'usage de la carte prépayée s'étend quasiment à tous : les personnes dépourvues de compte bancaire, les interdits bancaires, les jeunes non majeurs, les voyageurs et même les titulaires de comptes bancaires qui ne souhaitent pas fournir leurs coordonnées bancaires.

En outre, d'autres fonctionnalités peuvent être associées à une carte prépayée selon les émetteurs. C'est le cas des services tels que le transfert d'argent (carte à carte et mise à disposition), le paiement de factures ou encore l'achat de crédit de communication. Sur le marché bancaire camerounais, certaines banques émettrices de monnaie électronique offrent même à des entreprises l'occasion de régler les salaires de leurs employés dépourvus de compte bancaire, directement dans une carte prépayée créée à cet effet. Toutes ces fonctionnalités ne sont disponibles qu'à l'intérieur d'une plateforme dédiée, utilisant des technologies spécifiques et pour la plupart affiliées aux réseaux internationaux Visa et MasterCard. Les infrastructures logicielles et matérielles varient selon la solution prépayée retenue par un établissement émetteur.

Offrant plusieurs avantages, la carte prépayée est tout d'abord une alternative au compte bancaire. Elle permet à son titulaire de bénéficier de services financiers de base (retraits, paiements, consultation de solde) et de jouir de la possibilité de stocker ses liquidités sous une forme plus sûre. Ensuite, elle est un facteur d'inclusion financière puisqu'elle permet aux exclus du système financier formel d'avoir accès à certains produits ou services financiers. Enfin, elle améliore la célérité et la sécurité des transactions financières et commerciales.

Si les avantages et les bienfaits de ce produit ne sont pas à contester, son utilisation peut favoriser certains comportements répréhensibles au sens des lois et règlements édictés par les Etats membres de la CEMAC.

2.4.1.1 La distribution des cartes bancaires prépayées

Un grand nombre de banques dans la sous-région n'offrent pas de cartes prépayées. Au Cameroun par exemple, sur les treize banques qui y sont présentes, seules Ecobank Cameroun, Afriland First Bank, Atlantique Bank et UBA Cameroun émettent ce type de NMP.

A partir des résultats des entretiens semi-directifs en profondeur, il ressort que la distribution des cartes fait intervenir le fabricant du support de la carte, un personnalisateur de la carte, un prestataire, la banque et le client. Des banques et parfois des EMF sont des émetteurs et des acquéreurs de cartes. Ils effectuent le routage des données et la connectivité de ces instruments aux DAB et aux TPE. Par ailleurs, ils assurent le « clearing » des opérations et l'archivage.

Dans le principe[12] , l'acquisition d'une carte bancaire prépayée se fait aux guichets de banque. Pour en obtenir une, le client doit remplir une fiche de souscription et être identifié. La personnalisation de la carte se fait après la confirmation de la non identification du client sur la « black list » de la banque et la signature du contrat de souscription par le gestionnaire.

Dans les banques étudiées, les flux monétiques relatifs à l'utilisation des cartes prépayées convergent vers une plateforme localisée chez le prestataire (exemple : Atos Cardamone). Ce prestataire joue le rôle d'intermédiaire entre les émetteurs de cartes et la banque en matière de flux monétiques. Par ailleurs, le fonctionnement des guichets automatiques de banque est rattaché à la plateforme monétique du prestataire et ce dernier effectue la compensation des flux monétiques.

2.4.1.2 La demande de cartes bancaires prépayées en zone CEMAC

Pour pouvoir utiliser les cartes prépayées, leurs porteurs doivent disposer d'une provision d'unités monétaires. Le montant des retraits en espèces et des règlements pouvant être effectués est plafonné par la réglementation. La synthèse des plafonds règlementaires est présentée dans le tableau ci-dessous :

12 Certains établissements de crédit autorisent leurs distributeurs à émettre des cartes prépayées

Tableau 1 : Plafonds des transactions via les NMP

REFERENCE	ELEMENTS D'APPRECIATION	NORME OU STANDARD (En FCFA)[13]
REM CP1	Plafond de l'instrument électronique	5.000.000 FCFA
REM CP2	Plafond de chargement journalier (en espèces)	2.000.000 FCFA
REM CP12	Plafond de chargement journalier (par transfert bancaire)	5.000.000 FCFA
REM CP3	Plafond par opération de retrait (cash out manuel ou sur automate)	500.000 FCFA
REM CP4	Plafond par opération de transfert	1.000.000 FCFA
REM CP5	Plafond par opération de paiement	1.000.000 FCFA
REM CP6	Plafond de retraits journaliers	750.000 FCFA
REM CP7	Plafond de transferts journaliers	1.500.000 FCFA
REM CP8	Plafond de paiements journaliers	2.500.000 FCFA
REM CP9	Plafond des transactions journalières (Retrait + Transfert + Paiement)	3.000.000 FCFA
REM CP10	Plafond des transactions hebdomadaires (Retrait + Transfert + Paiement)	5.000.000 FCFA
REM CP11	Plafond des transactions mensuelles (Retrait + Transfert + Paiement)	10.000.000 FCFA

Source : BEAC

Des enquêtes, il ressort que dans la CEMAC, les personnes physiques sont les principaux demandeurs des cartes prépayées. Ces dernières servent principalement à effectuer des retraits d'argent auprès des guichets automatiques de banque et des paiements à partir des TPE dont sont équipés les commerçants. Dans les banques, la recharge des cartes prépayées se fait, soit par la remise d'espèces en agences, soit par débit d'un compte bancaire. Elle peut aussi se faire sur le site web de la banque, par débit au compte bancaire du client.

Les informations disponibles sur les cartes prépayées ont été collectées auprès de[14] :

- UBA, Afriland First Bank Cameroun;
- UBA au Gabon;
- UBA au Congo

13 Un euro = 655,96 FCFA

14 Toutes les banques de la zone CEMAC offrant les cartes prépayées n'ont pas mis les informations relatives à cette activité à la disposition du Groupe de travail. En outre, la BEAC ne disposant pas d'informations agrégées et détaillées sur ce sujet, les statistiques présentées dans ce rapport sont partiellement représentatives de la situation réelle du marché des cartes prépayées dans la zone CEMAC.

Toutefois, seules les banques exerçant leur activité au Cameroun ont fourni des données suffisamment détaillées.

Ainsi en glissement annuel, le nombre de cartes prépayées émises par la banque Afriland First Bank est passé de 12.773 en 2013 à 16.326 en 2014 (soit une augmentation de 27,81%), à 20.322 en 2015. Sur la même période à UBA Cameroun, ce nombre est passé 2.555 à 50.050 (soit une progression de 1859% entre 2013 et 2014) et à 145.850 en 2015. Pour ce qui concerne Ecobank Cameroun, il est resté quasi stable.

Toujours en glissement annuel, chez Afriland First Bank, le nombre de cartes prépayées actives représentent en moyenne 96,9% le nombre total de cartes. Et le volume des transactions en valeur via ces cartes est passé de 4.385.700.062 FCFA (6.685.926€) à 4.718.154.598 FCFA (7.192.750€) entre 2013 et 2014, soit une augmentation de 7,58%. Et, FCFA 5.752.463.745 (8.769.534€) Entre 2014 et 2015 soit, 21,9% en valeur relative.

Pour ce qui concerne UBA Cameroun, le volume de transaction en valeur via les cartes prépayées est passé de 56.387.500.000 FCFA (85.961.796€) en 2013 à 125.125.000.000 FCFA (190.750.960€) en 2014, soit une hausse de 121,9%. Entre 2014 et 2015, ce volume de transaction a connu une croissance de 45,7% passant à FCFA 182.312.500.000 (277.932.343€).

A Ecobank, entre 2013 et 2014, ce volume de transaction est passé de 105.132.292.000 FCFA (160.272.412€) à 178.006.239.000 FCFA (271.367.520€), soit une hausse de 69,31%. Entre 2014 et 2015, ce montant a augmenté de 7,15% passant à FCFA 190.735.811.000 (290.773.540€). Pour l'ensemble de ces banques, il ressort que le volume d'activités liées aux cartes prépayées augmente au fil du temps.

Tableau 2 : Offre de cartes prépayées par quelques banques en Afrique centrale

Source : données d'enquête

Statistiques sur les cartes prépayées – Afriland First Bank Cameroun

Indicateurs	2013	2014	2015	2016 (au 30/06/16)
nombre de cartes prépayées enregistrées	12 773	16 236	20 322	21970
Nombre de cartes prépayées actives	12 339	15737	19 750	21390
Nombre DAB/GAB	61	78	85	102
Nombre TPE	195	208	219	266
Nombre de transactions effectuées	371 074	385 498	407 347	204 219
Valeur des transactions effectuées	4 385 700 052	4 718 154 598	5 752 463 745	3 067 926 896
Solde en cours des cartes prépayées	489 977 408	522 919 184	687 069 366	700 021 527

Statistiques sur les cartes prépayées- UBA Cameroun

Indicateurs	2012	2013	2014	2015
nombre de cartes prépayées enregistrées	2 555	2 555	50 050	145 850
Nombre de cartes prépayées actives				
Nombre DAB/GAB				
Nombre TPE				
Nombre de transactions effectuées				
Valeur des transactions effectuées	12 775 000 000	56 387 500 000	125 125 000 000	182 312 500 000
Solde en cours des cartes prépayées				

Statistiques sur les cartes prépayées - EcobankCameroun

Indicateurs	2012	2013	2014	2015
nombre de cartes prépayées enregistrées	1	7 422	7 321	8 158
Nombre de cartes prépayées actives				
Nombre DAB/GAB				
Nombre TPE				
Nombre de transactions effectuées				
Valeur des transactions effectuées	3013 000	105 132 292 000	178 006 239 000	190 7 35 811 000
Solde en cours des cartes prépayées				

Ainsi entre 2012 et juin 2016, les seules banques camerounaises qui ont accepté de fournir les informations, sur insistance de l'autorité monétaire du Cameroun, assortie de menace de sanctions en cas de non collaboration il faut le dire, ont émis des cartes bancaires prépayées pour une valeur globale des transactions de FCFA 868.401.600.301 (1.323.863.650€). Outre le fait que leurs projections à partir des chiffres au 30 juin 2016 laissent entrevoir une progression des valeurs de transaction équivalent au double de celles de 2015, deux des institutions bancaires ne font apparaître aucun solde en cours des cartes prépayées au 31 décembre de chacune des années.

Dans la sous-région, l'absence d'un dispositif qui donne une vue globale du système de paiement par les cartes prépayées a été un handicap et non des moindres, pour la collecte des données. En effet il n'existe pas une entité comme au Portugal qui gère l'ensemble des DAG. Par ailleurs, Il n'y a pas un référentiel centralisateur des cartes qui mentionne les noms des utilisateurs des cartes et les numéros des cartes, etc. Des entretiens avec les différents acteurs, il ressort que la maitrise des flux lors des opérations via les cartes prépayées n'est pas un objectif des autorités sous régionales de régulation et de supervision dont, il faut le rappeler, l'une des missions est de veiller à la stabilité financière et monétaire sous régionale.

2.4.2 Le mobile money

Pour l'essentiel des institutions engagées dans l'offre de mobile money, ce moyen de paiement a été introduit dans la Sous-région après 2010. Il permet de réaliser des transactions grâce à un système d'unités monétaires via le téléphone mobile. Les transactions par mobile money sont liées à l'ouverture d'un compte électronique. L'agrément pour offrir un produit de mobile money par un opérateur de téléphonie mobile est obtenu par une banque partenaire qui constitue un fonds de garantie permettant de couvrir l'ensemble des volumes d'argent électronique en circulation. Les émetteurs de mobile money sont donc les banques. Dans la CEMAC, les produits de mobile money suivants sont offerts :

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

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

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

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

Tableau 3 : Liste des établissements de crédit de la CEMAC autorisés à émettre du mobile money

Pays	**Emetteur**	**Opérateur technique**		**Type de produit**	**Date d'autorisation**
Cameroun	BICEC	Orange		Mobile Money	29/07/2011
	ECOBANK	MTN		Mobile Money	29/07/2011
	Afriland First Bank	MTN		Mobile Money	29/07/2011
	SGC			Mobile Money	02/12/2011
TOTAL			4		
Congo	ECOBANK	MTN		Mobile Money	29/07/2011
	BGFI BANK	Airtel		Mobile Money	03/10/2011
TOTAL			2		
Gabon	BGFI BANK	Airtel		Mobile Money	29/07/2011
	BICIG			Mobile Money	11/07/2012
	ORABANK	Atlantique Télecoms (Moov)		Mobile Money	
	UGB	Gabon Telecom		Mobile Money	20/01/2014
TOTAL			4		
Tchad	ECOBANK	Airtel		Mobile Money	05/03/2012
	ORABANK	TIGO		Mobile Money	11/07/2012
TOTAL			2		
TOTAL GLOBAL			12		

Source : BEAC

A la lecture de ce tableau, on peut constater que sur la cinquantaine de banques exerçant dans la sous région, seules douze d'entre elles possèdent des agréments pour l'émission du mobile money. Parmi les banques disposant d'un agrément, certaines à l'instar de la Société Générale ou encore Ecobank au Cameroun n'émettent pas encore de mobile money.

2.4.2.1 La distribution du mobile money

Mobile Money est un service qui permet aux clients de faire leurs transactions financières en utilisant leur téléphone mobile.

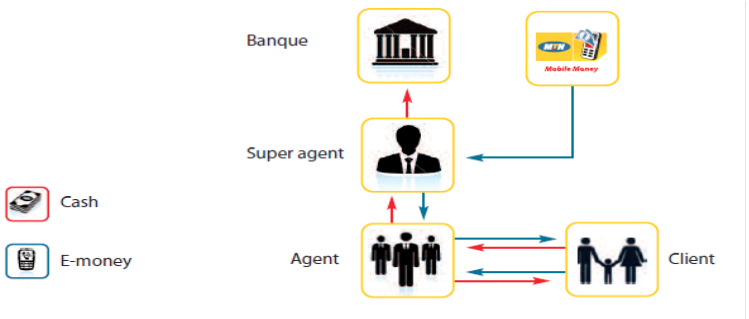
Ce service est un outil important pour l'inclusion financière. Il permet d'insérer dans le circuit bancaire une tranche importante de la population qui est non bancarisée.

La Banque Centrale a réglementé le Mobile Money en instituant un partenariat entre les banques, qui seules ont autorisation d'émettre la monnaie électronique, et les opérateurs de téléphonie mobile pour rendre le service accessible à leurs clients.

L'utilisation du mobile money met en jeu plusieurs intervenants :

- la banque, dépositaire de tous les fonds virtuel circulant sur la plate-forme Mobile Money ;
- l'opérateur de téléphonie mobile, chargé de développer le réseau Mobile Money, fournir les Sims aux clients, et généralement gérer la plate-forme Mobile Money ;
- l'agent mobile money, Il obtient de l'argent virtuel par le dépôt d'un équivalent de trésorerie physique à la banque ;
- le marchand qui reçoit les paiements des clients mobile money ;
- le client, utilisateurs final qui crédite et débite les comptes Mobile Money dans le réseau de distributeurs, et est en mesure d'effectuer des transactions Mobile Money.

La banque partenaire gère l'argent équivalent aux flottes virtuelles qui circulent dans les comptes « mobile money ». Elle contrôle et garantit l'émission de la monnaie électronique, assure la conformité des opérations avec les lois en vigueur relatives au blanchiment d'argent et au financement du terrorisme. Les banques n'ont pas toujours une plateforme. On observe plutôt des prestataires avec des plateformes multi-banques.



Le régulateur n'a pas accès aux plateformes en temps réel. Mais les plateformes sont certifiées, ce qui du point de vue du régulateur garantit la fiabilité de la gestion des comptes.

Toutefois, les banques ont accès en temps réel aux informations sur les plateformes. Les entreprises de téléphonie mobile gèrent la plateforme des transactions y compris la flotte virtuelle. Les distributeurs reçoivent la monnaie créée et effectuent la distribution. Ils font des dépôts dans le compte de garantie à des fins de mise à disposition du mobile money auprès des revendeurs et agents de distribution. Les agents de distribution sont rattachés aux distributeurs et effectuent des opérations de retraits et de dépôts dans les comptes des clients. Les accepteurs sont des commerçants qui acceptent les paiements par mobile money.

Pour s'approvisionner en mobile money, les distributeurs achètent des unités de monnaie électronique auprès des opérateurs de téléphonie mobile. Les revendeurs à leur tour ont recours aux distributeurs. Les clients finaux eux-mêmes s'approvisionnent en unités de monnaie électroniques contre remise d'espèces dans les points de vente des revendeurs et des détaillants.

Pour qu'un marchand reçoive des paiements par mobile money, il doit remplir un ensemble de conditions, formalisées par l'établissement d'un dossier juridique qui est objet d'étude de son dossier par un agent de la société de téléphonie mobile, et le cas échéant, de la signature d'un contrat, préalablement validé par une banque partenaire, entre lui et l'opérateur de téléphonie mobile. Un compte marchand lui est ensuite ouvert dans la plateforme de gestion de l'opérateur de téléphonie et une copie du contrat est transmise à la banque pour ouverture du compte du marchand dans la plateforme.

Pour les distributeurs et les accepteurs, le dossier comprend la carte de contribuable, l'inscription au registre du commerce, le plan de localisation, une photo du dirigeant et des justificatifs de domicile, comme des factures d'eau ou d'électricité. Sur la plateforme, la banque a une liste des distributeurs et autres intermédiaires, mais pas celle des clients finaux. Elle n'a donc pas une trace des transactions réalisées par les clients finaux. Elle contrôle davantage le stock de monnaie électronique disponible.

La distribution de mobile money requiert la communication, par les opérateurs de téléphonie mobile à leurs banques partenaires, d'un certain nombre d'informations. Elles portent en particulier sur les volumes des transactions, la fraude, les activités des distributeurs, le respect de la réglementation sur les montants et les seuils des transactions.

2.4.2.2 La demande de mobile money dans la CEMAC

Les utilisateurs de mobile money sont principalement des personnes, physiques et morales, disposant ou non d'un compte bancaire, abonnées des opérateurs de téléphonie mobile. Parmi elles, on trouve des personnes résidant dans des zones péri-urbaines et rurales, des commerçants et des salariés non bancarisés.

Le mobile money permet d'effectuer des retraits en espèces ainsi que des paiements de factures auprès de commerçants, le règlement des impôts et taxes, les paiements en ligne, les achats d'articles, des crédits de communication et des transferts d'argent. Il s'agit essentiellement des transferts d'argent peer to peer (P2P)[15] , peer to cash (P2C). En outre, le mobile money favorise la collecte d'épargne auprès des populations non bancarisées ou résidant dans les zones rurales, contribuant ainsi à l'inclusion financière. Pour pouvoir utiliser le mobile money, le client doit disposer d'une ligne téléphonique et renseigner un formulaire de souscription, en y joignant une copie de sa carte nationale d'identité. Le tableau ci-après présente des statistiques sur l'activité de mobile money en zone CEMAC; seuls Airtel au Gabon, MTN et Orange (et leurs banques partenaires respectives Afriland First Bank et BICEC) au Cameroun, ont fourni une information abondante.

Comme illustré dans les tableaux ci-dessous et sur la base des informations recueillies auprès des seuls opérateurs du Cameroun et du Gabon, près de FCFA 868.702.238.000 (€1.324.321.000) ont transité par le mode de paiement du mobile money entre 2011 et fin juin 2016 ■

15 Modèle de réseau informatique où chaque client est aussi un serveur

Tableau 4&5 : Offre de Mobile Money en Afrique centrale (source : données d'enquêtes)

Statistiques sur le mobile money – MTN & Orange – Cameroun

Indicateurs	**2011***	**2012***	**2013**	**2014**	**2015**	**2016 (au 30/06/2016)**
Nombre de comptes monnaie mobile enregistrés	42 996	628 378	2 738 901	3 589 086	3 796 051	6 284 061
Nombre de comptes de monnaie mobile actifs	3 589	68 799	1 442 692	1 738 976	2 172 792	2 808 249
Nombre d'agents enregistrés	659	264	6 849	5 991	17 219	11 952
Nombre d'agents actifs	206	400	1 969	4 461	4 943	6 379
Valeur des transactions bancaires mobiles effectuées (en milliers)	**372 581**	**7 563 478**	**30 789 734**	**71 993 361**	**201 397 836**	**315 685 248**
Nombre des transactions bancaires mobiles effectuées	35 475	998 277	3 273 148	8 951 175	25 096 057	28 907 949
Soldes en cours des comptes bancaires (en milliers)	20 499	172 039	1 840 056	8 790 596	9 845 234	10 159 347

**statistiques ne concernant que l'opérateur Orange Cameroun*

Statistiques sur le mobile money – AIRTEL - GABON

Indicateurs	2 012	2 013	2 014
Nombre de comptes mobile money	294 428	2 687 540	6 261 740
Valeur des transactions	12 600 000	76 100 000	152 200 000

Dans la CEMAC et au Cameroun notamment, l'on peut constater que l'utilisation du mobile money commence à se répandre à partir de 2013. Cette année-là, le nombre de comptes mobile money enregistrés auprès des opérateurs techniques franchit la barre de deux millions sept cent mille et les comptes actifs connaissent leur progression annuelle la plus élevée sur la période 2011-fin juin 2016 soit près de 2000%. Comme attendu, le nombre d'agents participant à la distribution augmente dans un même ordre de grandeur que celui du nombre des comptes mobile money avec un pic en 2013.

En 2016, le nombre total des comptes va au–delà de six millions deux cent mille. Seulement, un compte sur trois n'est pas actif.

S'agissant des flux financiers mobilisés à travers les transactions par mobile money, leur valeur annuelle augmente en moyenne de 170 % chaque année depuis 2013. En fin juin 2016 (1er semestre), cette valeur est estimée à plus de 315 milliards de FCFA (57% de plus que la valeur totale de l'année précédente). Le ralentissement de la croissance du stock (des soldes) en cours des comptes

mobile money confirme le rôle majeur de transfert d'argent « instantané » que joue cet instrument auprès de ses utilisateurs et l'augmentation de la vitesse de circulation des flux financiers mobilisés. Pour cela, on peut observer que les soldes en cours auprès des banques camerounaises, concernant cet outil, ont progressé en glissement annuel de 970% en 2013 mais seulement de 12 % en 2015 (voire 3% au premier semestre 2016. Ce qui veut dire que les transferts par mobile money sont effectués dans des délais de plus en plus brefs.

Au Gabon, la valeur totale des transactions mobile money de l'opérateur Airtel a doublé en deux ans et se situe à plus de 150 milliards de FCFA en 2014 et comme au Cameroun, 2013 est une année charnière avec plus de 813 % d'augmentation du nombre de comptes mobile money ouverts auprès de AIRTEL GABON. En 2014, le nombre de comptes avoisine six millions trois cent mille

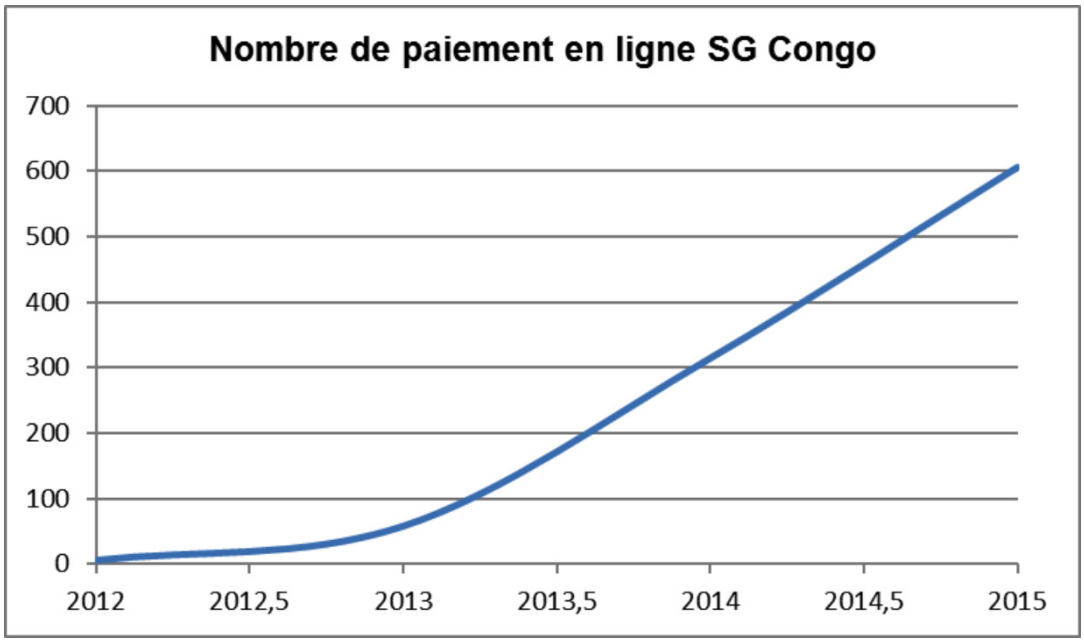
En résumé, s'appuyant sur les cas d'institutions étudiés, on peut dire que la demande de mobile money dans la zone CEMAC a connu une très forte augmentation au cours des trois dernières années. Dans la même lancée, le volume des transactions via le mobile money a connu une progression fulgurante.

2.4.3 Les paiements en ligne

Les paiements en ligne ont commencé dans la CEMAC au début des années 2000. Les principaux acteurs engagés dans l'offre de paiement en ligne sont la passerelle de paiement en ligne, les sites web et les banques.

La passerelle de paiement en ligne constitue le fournisseur de produits de paiement en ligne. Pour effectuer une opération de paiement en ligne, la création d'un espace affecté au client est effectuée dans le site web où sont réalisés les achats. Par ailleurs, une authentification de l'espace affecté au client est faite par le fournisseur d'accès internet à chaque tentative d'utilisation du site par le client pour effectuer un achat.

Dans une structure telle la Société Générale du Congo, le nombre de transactions par paiements en ligne connait certes une évolution à la hausse d'une année sur l'autre, tout en demeurant faible : 605 paiements en ligne en 2015. Cette évolution est représentée par le graphique suivant :



Pour pouvoir réaliser des paiements en ligne, les clients ont l'obligation de s'inscrire sur un site marchand, de souscription d'un contrat, de possession d'un identifiant et d'un mot de passe. En outre, le client doit accéder à un espace qui lui est réservé et disposer d'un portemonnaie électronique ou d'une carte affiliée à un système de paiement international. Les paiements en ligne portent principalement sur les achats de biens et de services mais certaines banques proposent un service de virements en ligne. Les utilisateurs des paiements en ligne sont principalement les entreprises et les personnes physiques ayant en majorité déjà séjourné à l'étranger.

L'offre de NMP dans la sous-région pose de multiples problèmes qui sont à la fois technique, de contrôle et de régulation. Les problèmes techniques sont relatifs à l'instabilité du réseau. Les problèmes de contrôle portent sur le faible contrôle de la banque sur les activités d'offre de NMP par leurs partenaires. Les informations sur les activités des partenaires des banques ne sont pas toujours complètes et/ou disponibles en temps réel. Le contrôle de l'identité des utilisateurs, de l'origine des fonds et des seuils réglementaires n'est pas toujours assuré. Par ailleurs, la régulation et la supervision des autorités monétaires sur les activités d'offre de NMP n'est pas effective ■

CHAPITRE III

Les risques de blanchiment d'argent et de financement du terrorisme via les nouveaux moyens de paiement dans la CEMAC

L'essor des Technologies de l'Information et de la Communication (TIC) – principalement de la téléphonie- et la volonté affirmée des pays de la sous région de réduire le phénomène d'exclusion financière, ont favorisé le développement et l'expansion de l'offre de nouveaux instruments de paiements tels que les cartes prépayées et le mobile money. Si les avantages et les bienfaits de ce produit ne sont pas à contester, son utilisation peut favoriser certains comportements répréhensibles au sens des lois et règlements édictés par les Etats membres de la CEMAC

L'équipe de recherche a toutefois noté que les risques de blanchiment d'argent et de financement du terrorisme découlant de l'utilisation des nouveaux moyens de paiement sont mal appréhendé par les différents acteurs de la chaîne qui, bien que formés et sensibilisés aux diligences auxquelles ils sont astreints vis-à-vis de leur clientèle au moment de l'exécution de leurs opérations courantes, ne sont pas avertis de l'utilisation frauduleuse que pourraient en faire les malfaiteurs de toutes sortes.

Le séminaire organisé par le GABAC au moment de lancer le présent exercice de typologies et cours duquel, plusieurs spécialistes venus d'horizons et de métiers divers du domaine ont eu à faire des présentations thématiques sur les NMP et, les entretiens et séances de travail que le groupe de travail a eu à organiser tout le long de l'exercice ont permis d'identifier quelques unes des vulnérabilités au blanchiment d'argent et de financement du terrorisme inhérentes aux nouveaux moyens de paiement en Afrique Centrale.

Les habitudes de consommation dans la sous région étant telles que le commerce en ligne des produits est très limitée, nous ne présenterons que les risques ou vulnérabilités au blanchiment d'argent et au financement du terrorisme, liés à l'utilisation des cartes prépayées et du mobile money.

3.1 Risques communs aux nouveaux moyens de paiement

3.1.1 Risques relatifs aux défaillances du dispositif réglementaire

Bien que d'introduction relativement récente, la réglementation sur le fonc-

tionnement de l'activité d'émission de la monnaie électronique et sur l'utilisation des NMP semble prendre en compte les possibles dérapages pouvant conduire au blanchiment des capitaux et au financement du terrorisme. Toutefois, il subsiste encore des vides réglementaires qui pourraient favoriser l'occurrence de ces phénomènes. En effet, le dispositif régissant l'utilisation des NMP dans la zone CEMAC présente une certaine vacuité sur les aspects relatifs à la lutte anti blanchiment d'argent et contre le financement du terrorisme (Ndjimba, 2016), notamment sur les aspects ci-après :

- l'absence d'un dispositif réglementaire spécifique aux NMP et à la régulation des risques que leur utilisation peut engendrer ;
- le contrôle sur l'origine des fonds déposés en contrepartie de l'émission de monnaie électronique, sur l'objet des transactions, ainsi que sur la destination des fonds. Des dispositions dans ce sens contribueraient à une meilleure traçabilité des opérations ;
- le contrôle des transactions en temps réel dans le but de réduire les risques liés au caractère rapide de la circulation de la monnaie électronique via les NMP ;
- Le niveau des seuils sur les volumes de transaction qui restent trop élevés et semblent avoir été fixés sans tenir compte du possible caractère fragmentaire de ces opérations, et d'un recours possible au smurfing. La supervision des nouveaux acteurs du marché, notamment les intervenants dans le circuit de distribution du mobile money. Ce dernier peut en effet présenter de nombreuses vulnérabilités liées à la faible formation des agents ou distributeurs, souvent non professionnels du secteur financier, au fonctionnement des NMP ainsi qu'aux dispositifs et autres mécanismes de lutte contre les risques de BC/FT liés à l'utilisation de ces derniers.

A ces défaillances réglementaires quant à l'utilisation des NMP à des fins de blanchiment ou de financement du terrorisme, s'ajoutent les limites reconductibles aux facteurs de risque relatifs à la conduite de l'activité d'émission de la monnaie électronique, et des NMP qui la véhiculent.

3.1.2 Risques liés à La variété des acteurs et à la rapidité des évolutions technologiques

Le groupe de travail a fait sien le développement général suivant[16] :« Les risques propres à la monnaie électronique proviennent de ceux liés aux différents intervenants dans l'émission, la gestion et la distribution des produits, ainsi qu'aux évolutions rapides de technologie qui devancent le plus souvent l'adaptation nécessaire des pouvoirs publics.

16 Source : Etude de TRACFIN, monnaie électronique, monnaies virtuelles et nouveaux risques

A titre d'exemple, cinq catégories d'acteurs interviennent dans la chaîne de valeur de la carte prépayée :

- L'émetteur de la carte, qui est agréé auprès d'une autorité de contrôle et endosse la responsabilité vis à vis de cette autorité. Il est également responsable du bon fonctionnement de la carte vis à vis des utilisateurs. La carte prépayée est le support de la monnaie électronique ;
- Le réseau (MASTERCARD, VISA, AMERICAN EXPRESS, JCB-CUP, ..), qui gère les autorisations de transactions. L'appartenance de la carte à un réseau permet à celle-ci d'être acceptée dans les points de vente affiliés au dit réseau ;
- Le processeur, qui gère les aspects technologiques et informatiques de la carte
- Le « program manager », qui porte tous les aspects non technologiques: marketing, packaging, conformité, logistique, gestion pratique du produit, services à la clientèle. Il peut s'agir de banques, d'acteurs sur des marchés spécialisés, de bureaux de change, de petites sociétés, etc. ;
- Le distributeur, qui commercialise la carte et est en contact direct avec la clientèle (buralistes, enseigne de distribution, commerces de proximité).

L'identification des opérations est réalisée par le réseau, le processeur et l'émetteur. L'émetteur de la carte conserve également dans ses systèmes (serveurs d'autorisation) les numéros de carte à des fins de recherche ultérieure. Ces trois opérateurs peuvent distinguer les opérations réalisées par une carte prépayée d'une carte bancaire classique. En effet, à l'émission, la carte est associée à un numéro BIN qui est un numéro d'identification lequel comporte une clé qui permet de définir s'il s'agit d'une carte prépayée, d'une carte d'entreprise ou une carte individuelle. Il apparaît que si l'émetteur est responsable juridiquement de la vigilance en matière de blanchiment, les éléments constitutifs de la connaissance-client ne peuvent être collectés que par le biais du « program manager» et du distributeur.

Par ailleurs, les acteurs du secteur de la monnaie électronique, en tout cas pour ce qui concerne essentiellement les distributeurs, sont issus d'une culture non-bancaire dont l'expertise et l'expérience («know how») en matière de connaissance-client est plus limitée que dans le secteur financier traditionnel.

En effet, les réseaux de distribution de ces nouvelles méthodes de paiement sont le plus souvent des opérateurs non-financiers, peu férus en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, voire réfractaires à la mise en place de vigilances, qui peuvent être perçues comme étant un frein coûteux à la distribution de ces produits.

C'est ainsi qu'il est revenu au groupe de travail qu'Orange Cameroun, bien que sous le contrôle de la BICEC, émet de la monnaie électronique via son produit « carte visa orange money » sans que les autorités de la BEAC ou du GIMAC n'en aient été informées et sans probablement que les risques de blanchiment d'argent et de financement du terrorisme inhérents au dit produit n'aient préalablement été évalués par les deux parties.

Un autre facteur vient accroître le risque de défaillance ; le marché est en plein développement et peu stabilisé. En conséquence, les établissements sont en forte concurrence les uns avec les autres et rivalisent d'inventivité pour augmenter le chiffre d'affaires.

S'agissant des risques liés aux évolutions technologiques, il convient de souligner que la recommandation 15 du GAFI prévoit que : *« Les pays et les institutions financières devraient identifier et évaluer les risques de blanchiment de capitaux ou de financement du terrorisme pouvant résulter (a) du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution, et (b) de l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants. Dans le cas des institutions financières, cette évaluation du risque devrait avoir lieu avant le lancement des nouveaux produits ou des nouvelles pratiques commerciales ou avant l'utilisation de technologies nouvelles ou en développement. Les institutions financières devraient prendre les mesures appropriées pour gérer et atténuer ces risques».* En conséquence, les émetteurs de monnaie électronique, qui entrent dans le champ des institutions financières, devraient être en mesure de proposer des produits et des procédures de contrôle permettant d'atténuer le risque. Cette obligation n'est cependant pas respectée compte tenu du caractère particulièrement concurrentiel de ce secteur.

[Il est constant qu'en Afrique Centrale, aucune démarche tendant à une évaluation des risques de blanchiment d'argent et de financement du terrorisme liés à l'offre des nouveaux moyens de paiement n'a été entreprise préalablement à leur mise sur le marché]. Or, les évolutions technologiques vont, dans le sens de transactions de plus en plus rapides et le plus souvent plus véloces que les réseaux plus traditionnels, que ce soit la rapidité de chargement ou de déchargement de ces nouveaux moyens de paiement, mais aussi pour ce qui concerne la distinction entre achat de cartes/création d'un compte et la possibilité de chargement ultérieur/de virement des fonds/etc. par simple transmission d'un SMS ou d'un clic via Internet. En outre, cette rapidité des flux complique considérablement le contrôle et peut empêcher la saisie et le gel des fonds délictuels. La chaîne d'informations est plus complexe que dans un circuit bancaire classique : pour la même opération financière, l'analyse du

flux nécessite de faire appel à davantage d'interlocuteurs dont certains hors de la juridiction de la CEMAC. En conséquence, le processus d'investigation s'en trouve de facto ralenti ».

Les attaques cybercriminelles répétées dont a été victime une banque gabonaise et l'une de ses succursales au Congo viennent conforter ce qui précède à souhait.

3.2 Risques liés aux cartes prépayées

3.2.1 Opacité des banques

Tous les établissements bancaires de la sous région ont été conviés à participer à l'exercice de typologies objet du présent rapport. Cependant, seuls ceux représentant les grands groupes internationaux et une banque à capitaux camerounais ont accepté de jouer le jeu. Or, d'une part, les concernés ne proposent pas de service de cartes prépayées pour les premiers et la valeur des transactions du second ne représente que 1,72% de l'échantillon étudié et d'autre part, il est revenu aux membres du groupe de travail que les établissements de crédit qui n'ont pas accepté de collaborer à l'exercice seraient impliqués dans des enquêtes relatives aux transferts de fonds à grande échelle à destination de pays d'Afrique de l'Ouest touchés par le terrorisme et au change manuel au profit de personnes concernées par le blanchiment d'argent dans les pays où ils sont implantés. Et enfin, font de la surenchère aux plafonds de chargement des cartes prépayées.

3.2.2 Anonymat des porteurs

Les cartes prépayées peuvent être nominatives ou anonymes selon les options. Généralement, la carte est vendue à une clientèle occasionnelle[17] qui n'est pas systématiquement identifiée et qui règle son achat ou ses recharges en espèces. L'achat de la carte pouvant se faire auprès d'un établissement assujetti[18] ou chez un distributeur de monnaie électronique[19].

Les fonctionnalités de la carte étant universellement partagées, les porteurs anonymes jouiraient en principe des mêmes services que les porteurs régulièrement identifiés. Sans identification formelle par contre, l'établissement assujetti ou le distributeur ne sont pas capables de déterminer l'identité du porteur et l'origine des fonds qui servent à l'achat de la carte et à son charge-

17 « Personne physique ou morale n'ayant pas de compte dans l'établissement assujetti auquel elle s'adresse », Règlement COBAC R-2005/01 relatif aux diligences des établissements assujettis en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme en Afrique Centrale.

18 Etablissement habilité à émettre de la monnaie électronique.

19 Etablissement offrant au porteur de l'instrument électronique, en exécution d'un contrat conclu avec un établissement assujetti, un service de chargement, de rechargement ou d'encaissement de monnaie électronique.

ment. En d'autres termes, un client en possession d'argent d'origine douteuse ou provenant d'activités illicites peut très bien insérer le produit de son délit dans le système financier formel via une ou plusieurs cartes prépayées. Ainsi, l'anonymat de la carte est une brèche dans laquelle les délinquants et mafieux de tout genre pourraient aisément s'engouffrer.

3.2.3 Non respect des plafonds prescrits par la Banque Centrale

Les plafonds en chargement, retrait, paiement, transfert ou par transaction, qui laissent croire que la mise à disposition des cartes prépayée s'est détourné de son objectif d'inclusion financière, peuvent entrainer des abus de toutes sortes au regard des statistiques présentées plus haut.

Notamment, lorsque ceux-ci sont très larges et susceptibles de bénéficier à des porteurs anonymes. Aujourd'hui, les plafonds en chargement peuvent aller jusqu'à FCFA 10 millions (€15.245) par mois au Cameroun[20] et FCFA 25 millions (€38.115) hebdomadaires offert par une banque du Gabon pour les cartes prépayées. Les mêmes plafonds sont pratiqués pour les retraits GAB et les paiements.

Même si les établissements assujettis définissent ces plafonds à l'intérieur de plusieurs segments, ils restent pour la plupart très élevés. Surtout pour le cas des opérations de retrait. Sans compter que, faute d'un dispositif de centralisation des informations sur les transactions par les cartes prépayées, un client titulaire ou non de comptes bancaires peut, tout en respectant les plafonds réglementaires définis par chacune d'elles, contourner les plafonds et procéder à des rechargements itératifs dans autant de banques de son choix dans son pays de résidence et dans la sous région.

3.2.4 Risques de blanchiment des produits de la fraude fiscalo douanière

Dans la sous région, les cartes prépayées sont majoritairement utilisées par des opérateurs en lien avec le commerce international. C'est-à-dire les importateurs dont il faut le dire, le civisme fiscal n'est pas une préoccupation majeure. A cet effet, comme en ce qui concerne les cartes de débit, les cartes prépayées leur donnent la faculté non seulement de contourner la réglementation communautaire en matière de change, mais également, de procéder à la minoration des valeurs déclarées en douane et donc des droits et taxes y afférents. De même que la base taxable des impôts intérieurs dont ils sont redevables. Les profits frauduleusement acquis étant investis dans divers secteurs (immobilier, projet agricole de grande envergure, distribution des produits pétroliers…).

20 Veille concurrentielle

Bien que cet aspect ne fasse pas l'objet de la présente étude, nous voulons attirez l'attention des autorités monétaires sur le fait qu'au-delà des pertes en recettes budgétaires qu'elle occasionne et du déficit de la balance commerciale dont elle participe largement, l'utilisation des cartes prépayées dans le commerce extérieur pourrait être l'une des causes inexpliquée et non des moindres de la baisse de la couverture de change au niveau du compte des opérations sans compter, la déperdition des taxes qui pourraient être perçues sur les commissions prélevées par les banques sur les transactions opérées par leurs clientèles hors zone FCFA.

3.2.5 Blanchiment par le contournement des seuils de déclarations automatiques

La plupart des pays de la sous région ont pris des actes réglementaires qui, sous certaines conditions, obligent les établissements financiers à systématiquement déclarer aux cellules de renseignement financier toutes les opérations de dépôts en espèces de FCFA 5.000.000 (€7.625 environ). Dans le cadre de la première étape du blanchiment (placement), des opérateurs pourraient recharger leurs cartes prépayées de manière itératives avec des montants chaque fois inférieurs aux seuils de déclarations automatiques. Introduisant ainsi dans le circuit financier, l'argent qui pourraient provenir par exemple, de la corruption et/ou des détournement de fonds, de la vente de drogue, de la vente illicite des pierres et métaux précieux ou de tout autre produit du crime.

3.2.6 Les risques liés à la réalisation des opérations

La maîtrise des flux monétiques constitue le principal facteur de risque lié à la réalisation des transactions par l'entremise des NMP. Dans la Sous-région, les banques n'ont pas la maîtrise de leurs plateformes monétiques, qui sont localisées hors de leurs juridictions d'activités. Ceci peut encourager une manipulation des informations relatives aux transactions effectuées au moyen de cartes prépayées depuis les services du prestataire et favoriser la réalisation d'opérations douteuses. Par ailleurs, la qualité de la connexion internet peut encourager la réalisation d'opérations sans qu'elles fassent l'objet d'une analyse en temps réel.

En outre, l'insuffisance ou le défaut de formation du personnel des banques sur les systèmes d'informations en charge des cartes prépayées et sur la réglementation et les techniques de blanchiment d'argent, peut favoriser la réalisation de transactions douteuses du fait des erreurs humaines. Ainsi, en présence d'indices d'une opération de blanchiment d'argent ou de financement de terrorisme, un agent pas ou insuffisamment formé sur le sujet ne sera pas en mesure d'identifier le caractère douteux d'opérations et par voie de

conséquence, la déclaration de soupçon requise par la législation ne sera pas effectuée, sauf s'il existe un système de supervision centralisé, capable de détecter les opérations douteuses qui ne l'auraient pas été au premier niveau de vigilance.

Il s'agit là d'un risque opérationnel élevé, surtout lorsque les organes de supervision n'effectuent pas des contrôles réguliers des opérations. Ce risque est renforcé par le fait que dans ces institutions il n'existe pas de dispositif électronique d'alerte qui identifie les indices de soupçon de blanchiment d'argent et de financement du terrorisme. Le contrôle des transactions par un système manuel de pointage des indices s'avère très limité. Une telle manière de faire est encline aux erreurs et à l'incapacité des agents à systématiquement détecter des indices, étant donné la masse considérable d'opérations à analyser.

L'absence d'un dispositif informatique d'analyse des indices peut constituer une défaillance du système de gestion des transactions à identifier celles de nature douteuse.

Face à ces multiples facteurs de risques, d'ordre organisationnel et systémique, il est indispensable de développer un dispositif systémique de prévention des risques de blanchiment et de financement du terrorisme.

3.2.7 Le blanchiment des produits de la cybercriminalité et le financement du terrorisme avec les produits de la cybercriminalité

Les produits des fraudes suivantes peuvent servir au blanchiment et/ou au financement du terrorisme.

Il s'agit de :

La fraude physique. De manière non exhaustive, il est question de :

- fraude se rapportant à la contrefaçon des cartes prépayées imitant de vraies cartes aussi bien le visuel que le contenu, au **« yes card »**, contrefaçon de cartes à puce qui répond OK à tous les codes secrets saisis ;
- La contrefaçon des terminaux en utilisant des techniques de collectes de données telles que la modification des données des terminaux pour extorquer les données sensibles.

La fraude en ligne. Elle consiste en :

- La redirection de l'adresse IP à l'insu de l'internaute ;
- L'hameçonnage du site web
- Le vol des données dans les systèmes d'informations des banques, des processeurs ou des commerçants ;
- Attaque de la base d'informations de l'émetteur par l'interception au niveau des nœuds, l'accès aux serveurs, le décryptage des messages, ...

3.3 Risques liés au paiement par le mobile money

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

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

Les risques de blanchiment d'argent et de financement du terrorisme attachés à l'exécution d'opérations via le mobile money portent principalement sur les défaillances des systèmes de gestion de ces instruments par les institutions financières et leurs partenaires respectifs. Ces risques peuvent être classés en deux groupes : ceux liés à l'identification de la clientèle et ceux afférents à la réalisation des opérations à chacun des maillons de la chaîne des acteurs.

3.3.1 Risques liés à l'identification de la clientèle

3.3.1.1 Risques liés à l'authenticité des pièces d'identité

Le risque de blanchiment d'argent et de financement du terrorisme se trouve accru dans la Sous-région, dans la mesure où les personnes physiques peuvent plus facilement recourir à des pièces d'identification fausses. L'absence d'un dispositif efficace de vérification de l'authenticité des pièces d'identité par les opérateurs de téléphonie mobile constitue une forte limite à la prévention de ces risques, d'autant que chez plusieurs opérateurs de téléphonie mobile, l'utilisation du mobile money est possible dès l'identification du client et non

après vérification de l'authenticité de sa pièce d'identité. Dans ces structures, c'est même souvent la copie de cette pièce qui est présentée et la vérification de l'authenticité du document d'identité d'origine est alors impossible à réaliser. Aussi, les possibilités qu'ont les acteurs de passer d'un pays à un autre, en l'absence d'une base de données sous régionale d'identification des personnes physiques, peut favoriser la survenance de ces risques. Ainsi, la libre circulation des personnes entre les pays de la Sous-région constituerait un facteur de risque.

3.3.1.2 Les risques de blanchiment d'argent et de financement du terrorisme liés à la clientèle

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

3.3.2 Risques liés à la réalisation des opérations

3.3.2.1 Risques liés aux commerçants

Ces personnes peuvent recevoir des montants substantiels de paiements et les faire apparaître comme le produit légitime de leur activité (cela pouvant comprendre l'intégration de fonds). Les commerçants peuvent être des criminels eux-mêmes, escroquant leur clientèle, ou servant de façade pour le blanchiment du produit des activités de leurs complices, se faisant passer eux-mêmes pour des clients

3.2.2.2 Risques liés aux agents, intermédiaires et partenaires de détail

Ils se situent à un emplacement stratégique dans le cycle de paiement des services d'argent mobile: le chargement de sommes en espèces, le point de rachat ou retrait, et également la vente des appareils téléphoniques susceptibles d'être utilisés pour les opérations. Ces personnes ont donc la possibilité

de falsifier leurs registres, d'ignorer des soupçons qui devraient sinon être signalés, ou simplement de constituer un point de faiblesse en n'exerçant pas leur fonction avec toute la vigilance nécessaire.

3.2.2.3 Risques par le biais des paiements transfrontaliers

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

3.2.2.4 Risques de contournement de blanchiment d'argent et de financement du terrorisme via les transferts internationaux

L'évolution des activités des opérateurs de la téléphonie mobile vers l'émission de la monnaie électronique au travers des cartes de paiement type « VISA », pour régler des transactions et pour retirer des espèces dans les guichets automatiques des banques, pourrait ouvrir la porte aux transferts internationaux à des fins de blanchiment d'argent de financement du terrorisme. Sans compter que lesdits transferts internationaux ne manqueraient pas d'avoir un impact sur les réserve de change des Etats de la sous région ■

CHAPITRE IV

Typologies des risques de blanchiment d'argent et de financement du terrorisme liés aux nouveaux moyens de paiement

La conjugaison des risques de blanchiment d'argent et de financement du terrorisme, précédemment évoqués, a encouragé l'observation de plusieurs cas typologiques avérés de blanchiment d'argent et de financement du terrorisme par le canal des nouveaux moyens de paiement. Après en avoir fait la présentation, des propositions pour réduire le risque de BT/FCT sont émises.

4.1 Cas de blanchiment d'argent et de financement du terrorisme au moyen de nouveaux moyens de paiement dans la CEMAC

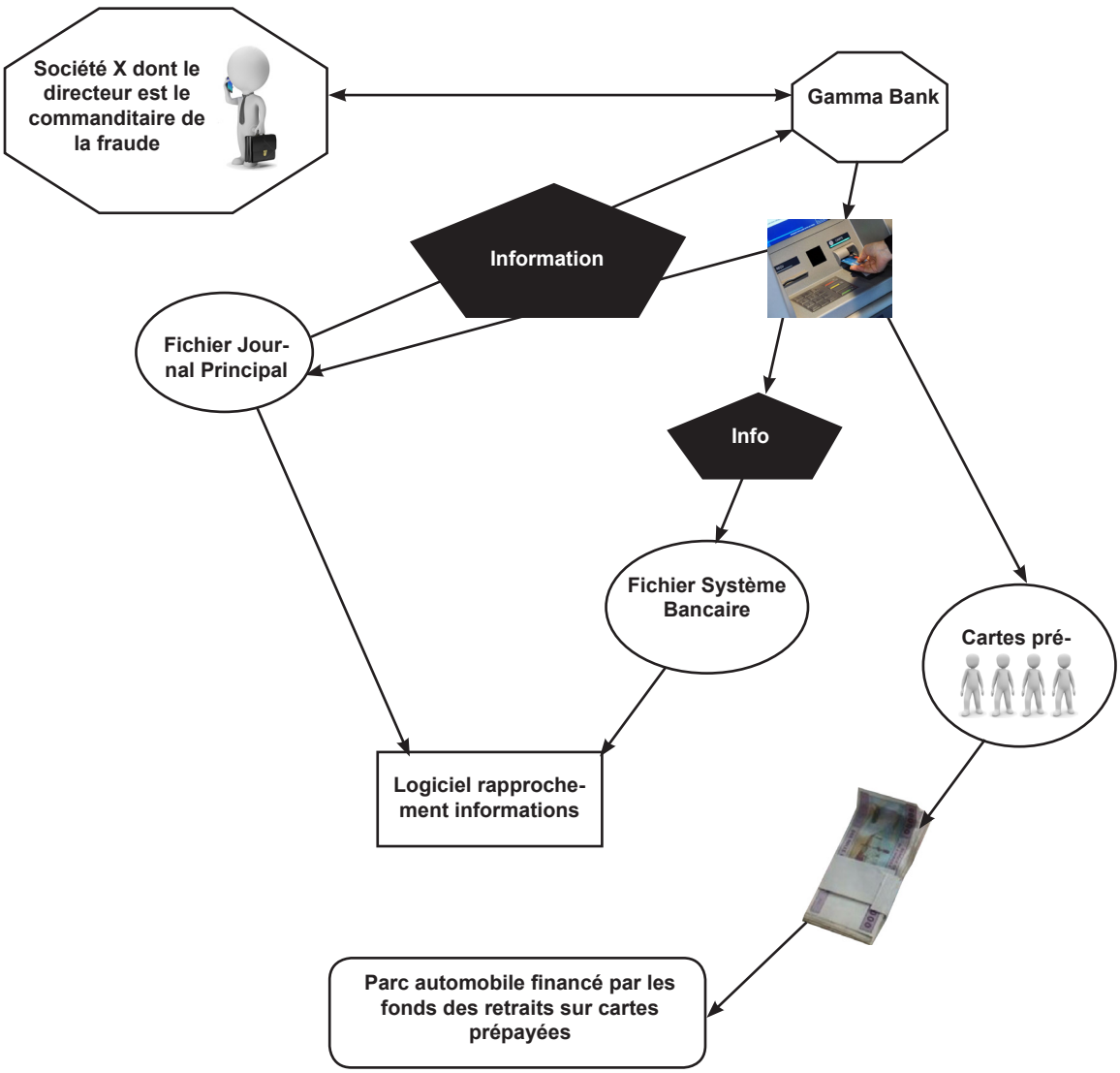
Des enquêtes auprès des ANIF, il a été identifié deux cas typologiques avérés de blanchiment d'argent . Le premier cas porte sur une fraude informatique sur les cartes prépayées qui conduit à un blanchiment d'argent[21].

CAS 1 : Fraude informatique sur cartes prépayées et blanchiment d'argent

La société X, spécialisée dans les solutions monétiques et dont le directeur général est le nommé Pippo, est en charge de la gestion de la monétique à Gamma Bank. A ce titre, elle héberge et administre les serveurs monétiques de Gamma Bank. Le 12 janvier 2015, M. Pippo est saisi par les dirigeants de Gamma Bank du fait que des opérations seraient comptabilisées dans leur système bancaire mais pas dans le système monétique. Une séance de travail conjointe entre les informaticiens de la société X et de Gamma Bank va révéler l'existence de retraits d'espèces aux guichets automatiques de Gamma Bank par le biais de 12 cartes magnétiques prépayées appartenant à 12 individus. En effet, ces 12 individus détenteurs chacun d'une carte de crédit prépayée à Gamma Bank, vont à maintes reprises effectuer des retraits d'argent sur des guichets automatiques. Après chaque opération, le chef du département technique de X, M. Gando, va se connecter au fichier journal principal en augmentant ses privilèges pour modifier et effacer les traces des transactions concernant le rapport de toutes les activités effectuées sur un distributeur automatique sur lequel les 12 personnes en cause ont opéré. Connaissant les délais requis pour les mises à jour entre le système monétique et le système bancaire, il va procéder à la suppression des informations relatives aux retraits d'argent effectué par ses commissionnaires à l'aide de ces 12 cartes bancaires pour empêcher le système bancaire de débiter les comptes concernés du montant d'argent par lui retiré. Une des personnes effectuant des retraits va répéter cette opération au point de spolier Gamma Bank de la somme de 39.000.000 FCFA au cours des années 2014 et 2015.

21 Des cas typologiques relatifs au blanchiment de capitaux via les NMP, fortement probables dans la zone CEMAC au regard des facteurs de risque identifiés en amont du présent rapport, ont été identifiés dans le contexte français (rapport Tracfin 2011, cas 5 et 6, PP 18-23).

Toutefois, Gamma Bank a implémenté une solution informatique chargée d'effectuer, à un moment précis, des rapprochements entre les informations contenues dans le fichier journal du système bancaire et les informations contenues dans le fichier journal du système monétique. Ladite application va produire un rapport d'erreur signalant une incapacité à rapprocher les informations du fait de la suppression de certaines données dans la table principale du système monétique. Exploitation faite du rapport d'erreur, il est constaté que 12 comptes « crédit prépayés » ne sont pas régulièrement débités bien que des retraits aient eu lieu. Gamma Bank saisit alors le Directeur Général de la société X, qui saisit à son tour le nommé Alexander basé en Inde, fournisseur et responsable technique Zone Afrique de la solution monétique que X distribue au Cameroun. Ce dernier va vérifier le système monétique de X et va confirmer à Sieur PIPPO que les opérations de suppression des informations dans la table principale du système monétique ont été effectuées à l'intérieur de son entreprise. Au cours de l'enquête judiciaire, Sieur Gando va finalement reconnaitre les faits avant de déclarer un parc de vente de véhicules d'occasion dont l'activité était financée par l'argent détourné.

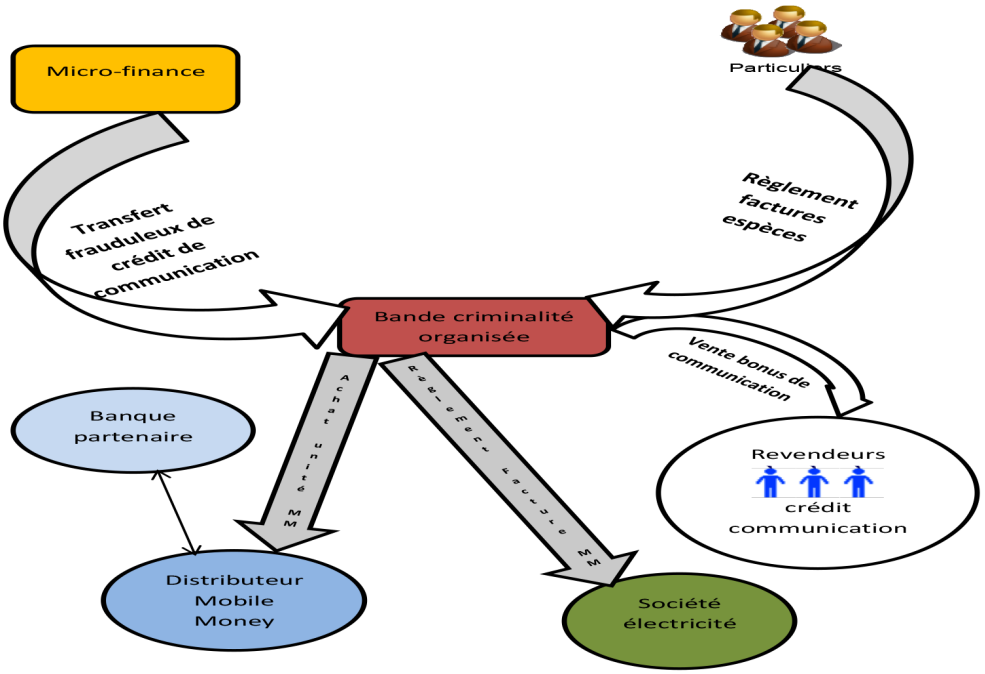


Le deuxième cas est relatif à une opération de blanchiment d'argent via le mobile money.

Cas 2 : Blanchiment d'argent via le mobile money

Après avoir été condamné pour escroquerie, la bande dont le chef est le nommé Ahomo va s'illustrer en prison dans une autre forme d'arnaque. Le 30 mai 2014, M. Bodo, employé dans un établissement de micro finance, saisit le Parquet pour dénoncer une escroquerie, dont il a été victime. En effet, ses bourreaux ont imité la voix de son patron pour l'emmener à faire des transferts de crédit d'une valeur de 900 000 FCFA. Après réalisation des transferts effectués vers des numéros de téléphone précis, les usurpateurs ont cessé toute communication avec leur victime. La traçabilité des transactions a permis d'établir que ces crédits avaient permis le paiement, par mobile money, de la facture d'électricité de plusieurs personnes, service offert par un opérateur de téléphonie mobile de la place. Après interpellation et audition de Monsieur Abondo, il ressort que dans son quartier à Bantoma, deux jeunes prétendument employé à la société d'électricité, ont offert à la population la possibilité de régler désormais leur factures d'électricité sans qu'elle ne soit obliger de faire la queue devant les agences agrées.

Plusieurs habitants ont ainsi plusieurs fois remis à ces faux agents, leur quittance, l'argent en espèce correspondant au montant à payer ainsi que les frais de taxi. Il a précisé qu'après chaque opération, les reçus de paiement de leurs factures leur sont remis en bonne et due forme. Par ailleurs, après chaque règlement de facture par mobile money, l'opérateur de téléphonie mobile octroi à l'abonné un bonus en crédits d'appel. Ces faux agents revendaient alors ces crédits à plusieurs revendeurs de crédit de communication, connu sous l'appellation de « call boxeurs », à des prix alléchants. A la fin, l'argent perçu en espèce chez la population et chez les call boxeurs était retourné à la bande à Ahomo toujours détenus à la prison centrale.



Cas 3 : Une affaire de cyberattaque : l'expérience du Bangladesh[22]

Cas 3 : De récentes cyberattaques révèlent une tendance des pirates informatiques à ne pas se limiter à un seul pays, mais à plutôt choisir des cibles affectant le système financier mondial.
Lors d'un récent acte frauduleux utilisant le portail sécurisé SWIFT, des pirates informatiques ont réussi à obtenir illégalement des identifiants valides d'opérateurs SWIFT et à détourner USD 81 millions provenant des réserves de devises étrangères de la Banque centrale du Bangladesh (BB) stockées à la Réserve fédérale de la banque de New York (FRBNY).

Qu'ont fait les intrus ?

- Désactivation de l'imprimante liée au serveur de production
- Émission réussie de 70 transactions via le réseau SWIFT
- (5 virements effectifs)
- Suppression de plusieurs fichiers, dont les enregistrements des messages
- Effacement de 116 messages en tout : 70 ordres de virement et 46 récépissés
- Suppression de l'historique Windows et écrasement d'autres fichiers remplacés par des fichiers contenant des données falsifiées
- Réinitialisation des mesures de sécurité : retour au paramétrage par défaut des règles de « pare-feu »

Initiatives prises par la Banque du Bangladesh

- Correspondance avec des banques intermédiaires telles que Wells Fargo, Bank of New York, Mellon, Citi NA, DBTCO et PABC ;
- Engagement d'une équipe de deux informaticiens chargés du rapport des incidents internes (8 févr. 2016) ;
- World Informatix Cyber Security chargé d'établir un rapport d'incident détaillé ainsi qu'une évaluation des vulnérabilités dans le cadre de l'investigation (28 févr. 2016) ;
- Mandiant (FireEye) chargé de mener une enquête scientifique (6 mars 2016) ;
- Demande d'assistance auprès de la Banque mondiale dans le cadre de son programme de recouvrement de l'argent volé ;
- CRF de Bangladesh alertée et impliquée dans la procédure de recouvrement des fonds.

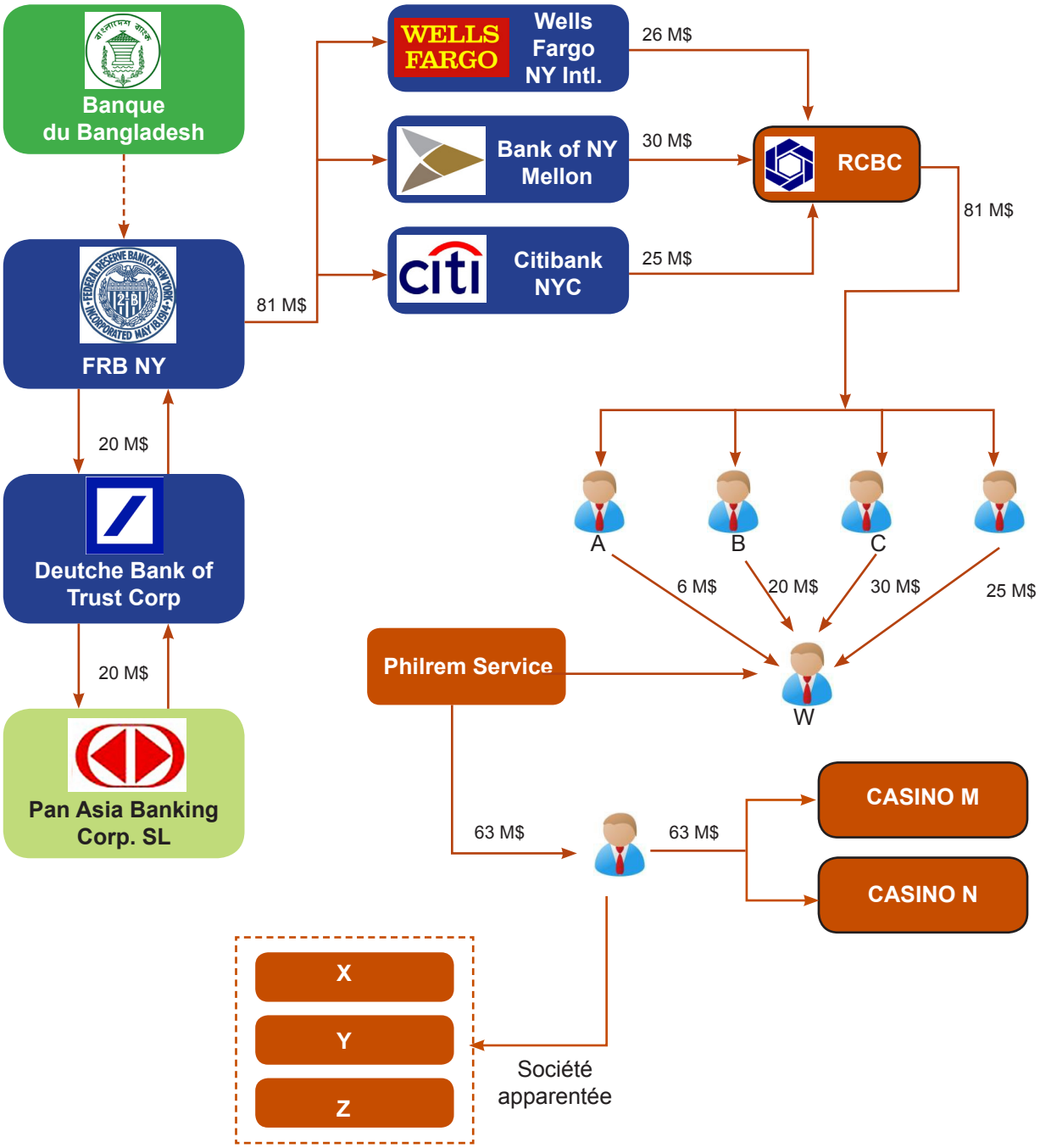
Rôle de la CRF

- Rôle central de la CRF dans le renforcement de la coopération nationale et internationale
- Faciliter la formation d'un groupe spécial dédié à la coordination des efforts réalisés pour récupérer l'argent volé
- Préparation de la demande d'assistance judiciaire mutuelle par le bureau du procureur général en accord avec la CRF et envoi au ministère de la Justice des Philippines conformément à la convention de Palerme
- La BFIU a recherché des informations concernant des individus et des entités aux Philippines auprès des membres du groupe Egmont et a reçu des réponses positives dans certains cas.
- La CRF a maintenue le contact avec l'AMLC des Philippines.
- L'AMLC a obtenu un ordre de la cour pour saisir les comptes suspects identifiés et pour lancer une enquête officielle.
- La CRF a maintenu la communication avec le GAFI et le GAP ;
- Des représentants de la CRF se sont physiquement impliqués dans la procédure aux Philippines et ont également assisté à l'audition de la commission Ruban bleu du sénat ;
- Réunion et téléconférence tripartites (BB, FRB NY et SWIFT) ;
- Réunion concernant la coordination du dossier organisée par Interpol et le Bureau national de lutte contre le terrorisme au Bangladesh.

Toutes ces actions ont permis de recouvrer USD 35 millions

22 Avec l'aimable autorisation de la CRF de Bangladesh

Piste de l'argent



CHAPITRE V

Recommandations visant à la réduction des risques de blanchiment d'argent et de financement du terrorisme liés aux nouveaux moyens de paiement

Les recommandations visant une amélioration du dispositif de gestion des NMP dans la sous-région peuvent porter sur des propositions relatives au contrôle et la régulation de l'activité d'offre de ces instruments financiers et au système technique de gestion des transactions via ceux-ci.

Ces propositions concernent principalement :

- les améliorations du dispositif réglementaire et de supervision de l'offre des NMP;
- la coordination des activités entre les acteurs impliqués dans la conduite de cette activité par la mise en place de systèmes de partage automatique des informations relatives aux transactions, qui se font par la monnaie électronique, entre les sociétés d'émission de manière à faciliter la collecte des informations nécessaires aux enquêtes, la détection des opérations suspectes et leurs déclarations aux cellules de renseignement financier et les reportings aux autorités sous régionales et nationales de supervision et de contrôle ;
- le renforcement des capacités des différents acteurs sur la problématique du blanchiment d'argent et du financement du terrorisme et général, mais sur les risques de blanchiment d'argent et du financement du terrorisme liés à cette branche d'activité.

5.1 Améliorer le dispositif réglementaire de régulation et de supervision de l'activité d'offre des NMP

Les différents risques répertoriés dans ce rapport, notamment, ceux liés à l'anonymat des porteurs, aux plafonds des cartes prépayées, au blanchiment des produits de la fraude fiscalo douanière et à l'opacité des banques d'une part et la difficulté à obtenir des statistiques agrégées, malgré les dispositions de l'instruction N°GR/01 relative à la surveillance par la BEAC des systèmes de paiement par monnaie électronique d'autre part, sont dus pour l'essentiel, à des carences réglementaires et à un défaut de mise en œuvre effective de l'encadrement et de la surveillance des activités se rapportant aux nouveaux moyens de paiement par les autorités de régulation, de supervision et de contrôle tant au niveau régional qu'au niveau national.

Outre que de manière générale, dans un environnement où le règlement des transactions se dématérialise inexorablement, ces carences ne permettent pas d'établir de

manière affinée les agrégats de la masse monétaire et donc de prendre des mesures appropriées de stabilité monétaire et financière, elle n'autorise pas non plus une lutte anti blanchiment et contre le financement du terrorisme efficace.

Des défaillances réglementaires ont été évoquées plus haut. A celles là, il faudrait ajouter que si, pour ce qui concerne les nouveaux moyens de paiement, édicter les règles anti blanchiment et contre le financement du terrorisme à l'intention des établissements de crédit incombe à la COBAC comme le prévoit l'instruction N°GR/01, cette dernière n'a à ce jour, mis à disposition aucune ligne directrice ou autre acte édictant les diligences propres aux nouveaux moyens de paiement que les acteurs devraient mettre en œuvre dans leur relation avec les partenaires technique et avec la clientèle.

Dans tous les cas, nous pensons que, faute d'avoir au préalable mis en œuvre la recommandation 15 du GAFI évoquée ci-dessus (voir &3-1-2), les autorités compétentes devraient améliorer l'encadrement juridique des nouveaux moyens de paiement de manière à minimiser les vulnérabilités au blanchiment des capitaux et au financement du terrorisme qui leur sont inhérentes.

Le nouveau cadre juridique comporterait des dispositions tendant à :

1. définir le rôle et les responsabilités opérationnelles de chacun des acteurs du déploiement des activités de la monnaie électronique (autorités de régulation, émetteurs, distributeurs…) pris individuellement et dans leurs relations d'affaires ;
2. énoncer les responsabilités des différents intervenants en matière de lutte anti blanchiment et contre le financement du terrorisme ;
3. exiger la mise en place d'un dispositif technique comportant entre autres, une piste d'audit spécifique de manière à s'assurer d'une traçabilité des opérations depuis l'origine des ordres de paiement jusqu'à leur dénouement. En facilitant leur collecte, les informations contenues dans une telle piste serait une source complémentaire pour l'enrichissement des recherches faisant suite aux déclarations de soupçon et plus généralement, pour les enquêtes menées par les autorités de poursuite ;
4. Faire respecter la réglementation des changes de la sous région pour les transactions effectuées avec la monnaie électronique dans le cadre du commerce extérieur avec les pays non membres de la zone CEMAC ;
5. Plafonner les avoirs en monnaie électronique à un montant compatible avec les politiques d'inclusion financière et les risques de blanchiment d'argent et de financement du terrorisme qui leur sont propres. En Afrique de l'Ouest par

exemple, sous réserve d'une autorisation spéciale de la Banque Centrale, les avoirs en monnaie électronique ne peuvent excéder FCFA 2.000.000 (€3.000 environ) de même, lorsque le porteur dispose de plusieurs instruments auprès d'un même établissement, le cumul mensuel de rechargement ne peut excéder FCFA 10.000.000 (€15.250 environ). A titre illustratif, le cumul hebdomadaire autorisé par une banque Gabonaise est de FCFA 25.000.000 (€38.000 environ). Toujours en Afrique de l'Ouest, le montant maximum en monnaie électronique pouvant être mis à la disposition d'un client non identifié est de FCFA 200.000 (€305 environ) au cours d'un même mois ;

6. Prescrire un reporting systématique et effectif non seulement à la BEAC mais également aux autorités monétaires nationales et aux autorités douanières et fiscales (pour ce qui concerne les transactions commerciales effectuées en dehors de chacune de leurs juridictions respectives), selon une périodicité et un canevas que la première aura défini et dont les données pourraient être affinées en fonction des requêtes des autorités chargées des enquêtes ;

7. Prévoir des sanctions en cas de non respect des dispositions réglementaires ;

   Pour ce qui concerne particulièrement le mobile money, les dispositions de la réglementation pourraient contribuer à minimiser les risques identifiés en prévoyant les mesures suivantes :

8. Pour les risques liés à la clientèle : pour autant qu'il s'agirait de transactions de personne à personne, développer des mécanismes en vue d'une meilleure identification des émetteurs et des destinataires des transactions électroniques, mettre en place de limites sur le nombre de comptes, la fréquence des opérations, les volumes et les montants de virement pouvant être réalisés sur une certaine période de temps ; la surveillance au niveau du système des flux d'opérations visant à signaler au prestataire d'argent mobile toute séquence d'opérations suspecte (de manière similaire aux systèmes de LAB/CFT utilisés par les banques et les systèmes de détection des fraudes utilisés par les opérateurs de téléphonie mobile) les limites imposées obligeraient les criminels et terroristes à fractionner leurs opérations, les rendant ainsi plus susceptibles d'être détectés par le système ;

9. Pour les risques liés aux commerçants : prescrire des procédures de vérification approfondies au début et en cours de relation dans le but de réduire le risque jusqu'à un niveau faible ;

10. Pour les risques liés aux agents, intermédiaires et partenaires de détail : mettre en place des procédures de vérification approfondies au début et en cours de relation ainsi qu'une surveillance continue du respect des obligations.

5.2. Maîtriser les risques de fraude cybercriminelle

Les attaques ci-dessus évoquées dont a été une banque de la sous région devraient amener le régulateur du marché de la monétique et les différents acteurs du secteur de même le cas de typologie sur la cybercriminalité, à veiller à la mise en place des architectures de sécurité robustes, anticiper sur les évolutions des systèmes qui permettent de détecter au plus tôt les fraudes et les attaques ou, au pire des cas, réagir promptement à celles-ci.

5.3 Veiller à la mise en œuvre de la recommandation 15 du GAFI

Avant le lancement des nouveaux produits ou des nouvelles pratiques commerciales ou avant l'utilisation de technologies nouvelles ou en développement, les institutions financières, mais plus particulièrement les organes et autorités de supervision et de contrôle sous régionaux et nationaux devraient, chacun en ce qui le concerne, prendre les mesures appropriées pour gérer et atténuer les risques pouvant résulter du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution, et (b) de l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants. Notamment, ceux liés à l'évolution des activités des opérateurs de la téléphonie mobile vers l'émission de la monnaie électronique via les cartes de type « VISA ».

5.4. Coordination des activités des acteurs impliqués dans la gestion des NMP

Quel que soient les améliorations que l'on pourrait apporter au cadre juridique relatif aux nouveaux moyens de paiement, elles seraient inopérantes en l'absence d'instruments permettant le contrôle de leur mise en œuvre effective. Pour cela, les possibilités qu'offrent les nouvelles technologies d'information pourraient être d'un apport plus qu'appréciable.

Il s'agirait de mettre en place un dispositif qui assurerait une meilleure coordination et un contrôle rigoureux des activités des acteurs impliqués dans l'offre des NMP à des fins de lutte anti blanchiment et contre le financement du terrorisme en permettant aux acteurs d'avoir une vue systématique des transactions financières via les NMP dans la CEMAC. Il assurerait dans la même lancée une centralisation des informations (volume, destination des fonds, …etc) et une détection rapide des opérations de blanchiment d'argent et de financement du terrorisme liées aux NMP afin de permettre aux établissements de crédit, aux autorités de poursuite habilitées et à l'ANIF d'accéder et de partager les informations relatives aux incidents de paiement déclarés.

Un tel dispositif de nature informatique et télématique, devrait être connecté aux serveurs, aux DAB, aux TPE et aux plateformes monétiques des différents acteurs qui assurent l'émission de monnaie électronique dans la sous région.

A titre d'exemple, la mise en place des plafonds peut se montrer inefficace s'il n'y a pas d'interopérabilité du déploiement de la monnaie électronique entre les plateformes des émetteurs de la sous région. Plateformes dotées de systèmes bloquant chaque fois qu'il y'aurait tentative de dépassement de plafonds. On pourrait imaginer le déploiement d'une solution technique de partage instantané d'informations par le biais d'un identifiant unique attribué à chacun des clients et qui serait géré par un fichier central des détenteurs de monnaie électronique. Toute chose qui devrait être l'une des préoccupations du Groupement Interbancaire Monétique de l'Afrique Centrale (GIMAC) dans le cadre du développement de ses produits en particulier, mais également dans le cadre de l'exécution de ses missions statutaires.

Pour la lutte contre le blanchiment d'argent et le financement du terrorisme, ce dispositif favoriserait un tracking des utilisateurs suspects dans la CEMAC. En effet, il pourra signaler les points d'utilisation des NMP et encourager par voie de conséquence la reconstitution des itinéraires des flux de monnaie électronique, voire des criminels financiers. En lui intégrant des modules de fraude et des programmes de détection des opérations douteuses (smurfing,….), ce dispositif peut beaucoup plus rapidement que les individus, aider à initier des déclarations de soupçon de blanchiment d'argent et de financement du terrorisme. Une opération frauduleuse qui implique plusieurs banques, et qui du point de vue de chaque banque individuelle ne laisse entrevoir rien d'anormal, peut être détecter d'un point de vue global par cette mécanique.

Toutefois, son fonctionnement efficace requiert l'implémentation des différentes recommandations évoquées plus haut. Il necessite aussi l'adhésion et la participation des acteurs impliqués dans l'offre des NMP, et surtout la volonté des décideurs politiques. Moins utopique qu'on peut l'imaginer, la mise sur pied d'un tel dispositif est envisageable et contribuerait fortement à la maitrise des flux monétaires liés aux NMP et à la mitigation des risques de blanchiment d'argent et de financement du terrorisme associés à leur utilisation.

5.5 Le renforcement des capacités des acteurs opérationnels

Une application efficace des mesures de lutte anti blanchiment et contre le financement suppose non seulement une maîtrise de la réglementation qui l'encadre pour mieux en appréhender la problématique mais également, des risques de déstabilisation auxquels l'utilisation abusive des instruments de

paiement, notamment les NMP, peut exposer les secteurs financiers, les économies et fragiliser la sécurité des Etats.

Il faudrait donc assurer une bonne formation continue des acteurs concernés par les NMP. Cette formation doit porter sur la connaissance du cadre juridique de la lutte anti blanchiment et contre le financement du terrorisme, et sur les techniques de détection rapide des opérations atypiques associées aux nouveaux moyens de paiement.

A cet effet, la COBAC devrait, comme c'est le cas de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) en France, par voie de lignes directrices (instructions), en relation avec le GABAC et/ou les cellules de renseignement financier, indiquer aux acteurs de la monnaie électronique les diligences spécifiques aux nouveaux moyens de paiement pour se prémunir des risques de blanchiment des capitaux et du financement du terrorisme et outre le Règlement portant prévention et répression du blanchiment des capitaux et du financement du terrorisme et de la prolifération en Afrique Centrale d'avril 2016, pour servir de supports supplémentaires pour le renforcement des capacités des différents acteurs de la chaîne des NMP ■

CONCLUSION

Conformément à ses termes de référence, l'objectif de exercice de typologies était de rendre compte des développements des NMP dans la sous région, faire une analyse comparative de différentes approches réglementaires susceptibles de réguler et de superviser le phénomène des NMP et qui maintiennent un équilibre entre la nécessité de promouvoir l'inclusion des couches de populations qui n'y ont pas accès au système financier et la lutte contre le blanchiment d'argent et le financement du terrorisme ; identifier les risques et les vulnérabilités spécifiques inhérents aux cartes prépayés, aux systèmes de paiements en ligne (y compris la monnaie virtuelle) et aux services de paiement via les téléphones mobiles ; et enfin, sur la base d'études de cas effectuées autant que possible dans la sous région, dresser les modes opératoires et les tendances de l'utilisation abusive des NMP à des fins de blanchiment d'argent et de financement du terrorisme en Afrique Centrale.

Sur la base des données collectées, notamment des flux financiers qui s'en dégagent, il ressort de la présente étude que le volume des transactions effectuées au moyen des NMP, tels que définis ci-dessus, connaît une forte augmentation dans la CEMAC, démontrant ainsi que la frange de populations qui autrement n'y auraient pas eu accès, s'est saisi de l'offre de services financiers qui leur sont proposés par les nouveaux moyens de paiement. Notamment par le mobile money.

Cependant, un certain nombre de vulnérabilités au blanchiment d'argent et au financement du terrorisme pourraient être inhérentes aux nouveaux moyens de paiement.

Il s'agit des vulnérabilités liées :

- A la carence du dispositif réglementaire et à la variété des acteurs et la rapidité des évolutions technologiques, pour celles qui sont communes aux NMP étudiés ;
- A l'opacité des banques ; à l'anonymat des porteurs ; au non respect des plafonds prescrits par la Banque Centrale ; au blanchiment des produits de la fraude fiscalo douanière, le contournement des seuils de déclaration, automatiques et à la réalisation des opérations pour ce qui concerne les cartes prépayées.

A la clientèle ; à l'identification de la clientèle ; aux commerçants; aux agents, intermédiaires et partenaires de détail et aux paiements transfrontaliers pour ce qui concerne le mobile money.

Deux cas avérés de blanchiment d'argent et de financement du terrorisme liés à l'utilisation des NMP dans la CEMAC ont été identifiés : le premier cas porte sur une fraude informatique sur les cartes prépayées qui conduit à un blanchiment d'argent, et le deuxième cas est relatif à une opération de blanchiment d'argent via le mobile money.

Ces différents cas typologiques font suite, comme repris ci-dessus, à la conjugaison de plusieurs facteurs de risque de blanchiment d'argent et de financement du terrorisme. Parmi ces facteurs de risque, on peut identifier ceux relatifs aux défaillances du dispositif réglementaire. Il s'agit principalement d'une vacuité cadre juridique des NMP à traiter des aspects liés au blanchiment d'argent et du financement du terrorisme, une absence de textes sur l'origine des fonds, l'identité des utilisateurs… et sur le contrôle associé à la conduite des activités par l'entremise des nouveaux moyens de paiement, et des plafonds de transactions jugés trop élevés. On identifie aussi des facteurs de risque liés à l'alimentation des nouveaux moyens de paiement et à la réalisation des opérations.

Pour corriger ces facteurs de risque de manière à endiguer les risques de blanchiment d'argent et de financement du terrorisme, un ensemble de recommandations est défini. Ces recommandations portent sur le renforcement du dispositif réglementaire qui encadre l'offre des NMP, sur la proposition des mecanismes assurant une meilleure coordination des activités des acteurs impliqués dans l'offrre de NMP, sur le développement d'un dispositif de collecte de l'information en temps réel sur les transactions via les NMP. La mise en œuvre de cette batterie de propositions mûe par une volonté politique et la participation concertée des différents acteurs du système financier peut fortement contribuer une meilleure maitrise des transactions via les NMP et à une prémunition contre les risques de blanchiment de capitaux et de financement du terrorisme liés à leurs utilisations ■

ANNEXE 1

Liste des sigles utilisés dans le rapport

ANIF : Agence Nationale d'Investigation Financière

AMLC : Comité de lutte anti blanchiment

BC : Blanchiment de Capitaux

BEAC : Banque des Etats de l'Afrique Centrale

BICEC : Banque Internationale du Cameroun pour l'Epargne et le Crédit

CEMAC : Communauté Economique et Monétaire des Etats de l'Afrique Centrale

COBAC : Commission Bancaire de l'Afrique Centrale

CRF : Cellule de renseignement financier

EME : Etablissement de Monnaie Electronique

FT : Financement du Terrorisme

GABAC : Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale

GIMAC : Groupe Interbancaire Monétique de l'Afrique Centrale

LAB/FT : Lutte Anti Blanchiment et contre le Financement du Terrorisme

NMP : Nouveaux Moyens de Paiement

UEMOA : Union Économique et Monétaire Ouest Africaine

UMAC : Union Monétaire de l'Afrique Centrale

ANNEXE 2

Bibliographie

1- Adrianaivo, M, Kpodar, K, 2012, Mobile phones, financial inclusion and growth, Review of Economics and Institutions, Vol 3, No2.

2- Armendariz de Aghion, B., Morduch, J., 2005, "The economics of microfinance", The Mit Press Cambridge, Massachusetts London.

3- L'argent mobile au service des personnes non bancarisées (Maria Solin, Andrew Zerzan).

4- Attali, J., 2006, "La microfinance aujourd'hui", Planetfinance, télécharger à www.pointsdactu.org/article_print.php3?id_article=664.

5- Babajide, A, 2015, Financial inclusion and economic growth in Nigeria, International Journal of Economics and Financial Issues, Vol 5, No3.

6- CENAFE, 2010, Typologies et tendances en matière de blanchiment d'argent et de financement du terrorisme au sein des entreprises de services monétaires canadiennes - Rapport de typologies et de tendances de CENAFE.

7- CGAP, 2001, Commercialisation et dérive de la mission des IMF, la transformation de la microfinance en Amérique Latine, Etude Spéciale.

8- Chatain, P-L ., Hernandez-Coss, R., Borowik, K., Zerzan., 2008, Integrity in mobile phone financial services : Measures for mitigating risks from money laundering and terrorist financing, World Bank Working - Paper No 146.

9- Demetis, D., 2010, Technology and anti-money laundering : A systems theory and risks-based approach, Edgard Egar Publising Limited.

10- Di Castri, S, Mobile money: Enabling regulatory solutions, www.gsma.com/.../2013/.../MMU-Enabling-Regulato..

11- Donovan, K, 2012, Mobile money for financial inclusion, siteresources.worldbank.org/.../IC4D-2012-Chapter-4.

12- Helms, B., 2006, “La finance pour tous: construire des systèmes financiers inclusifs”, Les éditions Saint-Martin.

13- Hulme, D., Mosley, P., 1996, “Finance against poverty”, Volume 1, Routledge, London.

14- Investir au Cameroun, 2005, le Mobile money prend ses marques au Cameroun, N°38

15- Klein, M, Mayer, C, 2011, Mobile money and financial inclusion: The regulatory lessons, Policy research working paper 5664, World Bank.

16- Lal, R, Sachdev, I, 2015, Mobile money services, design and development for financial inclusion, Harvard Business School, Working paper 15-83

17- Lawack, V, 2013, Mobile money, financial inclusion and financial integrity: The South African Case, Washington Journal of Law, Technology and Art, Vol 8, No 3, p 317-346.

18- Lelart, M., 2002, L’évolution de la finance informelle et ses conséquences sur l’évolution des systèmes financiers, Réseau Entrepreneuriat, Cotonou 16-18 Avril.

19- Lelart, M., 2005, “De la finance informelle à la microfinance”, Editions des Archives Contemporaines, AUF.

20- Levine, R, 2003, More on finance and growth: More finance, more growth ?, Federal Reserve Bank of St Louis Review, Vol 84, No 4, P31-46.

21- Mayoukou, C, 2000, La microfinance en Afrique centrale : Etat des lieux et perspectives de développement, TFD, 59-60, Juillet

22- Etude de TRACFIN, monnaie électronique, monnaies virtuelles et nouveaux risques.

23- Maria solin, Andrew Zerzan, L’argent mobile au service des personnes non bancarisées-2009.

ANNEXE 3

Liste des textes réglementaires relatifs à la monnaie électronique

1. Règlement nº 01/02/CEMAC/UMAC/COBAC du 13 avril 2002 relatif aux conditions d'exercice et de contrôle de l'activité de micro finance dans les Etats de la CEMAC
2. Règlement nº 01/03/CEMAC/UMAC du 04 Avril 2003 portant prévention et répression du blanchiment des capitaux et du financement du terrorisme en Afrique Centrale.
3. Règlement nº 02/03/CEMAC/UMAC/CM du 04 avril 2003 relatif aux systèmes, moyens et incidents de paiement.
4. Règlement nº 01/11/CEMAC/UMAC/CM du 18 septembre 2011 relatif à l'exercice de l'activité d'émission de monnaie électronique.
5. Règlement de la COBAC R-2005/01 du 1er avril 2005 relatif aux diligences des établissements assujettis en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme en Afrique Centrale.
6. Règlement de la COBAC R-2005/02 relatif aux établissement de monnaie électronique.
7. Instructionde la COBAC I-2006/01 du 31 juillet 2006 relative aux informations sur le dispositif de prévention du blanchiment des capitaux et du financement du terrorisme.
8. Instruction nº 01/GR du 31 octobre 2011 du Gouverneur de la BEAC, relative à la surveillance des systèmes de paiement par monnaie électronique, avec en annexe un cadre référentiel recensant les éléments permettant à la BEAC d'assurer sa mission de surveillance de l'activité
9. Instruction nº 02/GR/UMAC du 07 mai 2014 du Gouverneur de la BEAC, relative à la mise en place du multibanking dans le cadre de l'activité d'émission de la monnaie électronique


GROUPE D'ACTION CONTRE LE BLANCHIMENT D'ARGENT
EN AFRIQUE CENTRALE
G.A.B.A.C

Immeuble de la BVM AC - place de l'Indépendance
B.P. : 764 Libreville - Gabon - Tél. : +241 01 76 39 54
Couriel : secretariat@spgabac.org - www.spgabac.org