Banque de la République d'Haïti
CIRCULAIRE

CIR. : BRH/IF/2026/129-1

AUX INSTITUTIONS FINANCIÈRES

La présente circulaire établit les mesures préventives que les institutions financières doivent prendre aux fins de lutter contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive, ci-après « la prolifération ». Elle s'applique aux :

a) banques ;
b) sociétés financières de développement ;
c) sociétés de crédit-bail ;
d) sociétés de cartes de crédit ;
e) coopératives d'épargne et de crédit ;
f) institutions de microfinance ;
g) sociétés de promotion des investissements ;
h) maisons de transfert ;
i) bureaux de change ;
j) fournisseurs de services de paiement électronique ;
k) autres entités désignées par la Banque de la République d'Haïti (BRH).

1. Du programme de prévention

Les institutions financières doivent mettre en place un programme de prévention du blanchiment de capitaux, du financement du terrorisme et de la prolifération, conformément à l'article 31 du décret du 30 avril 2023 sanctionnant le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive.

Ledit programme doit refléter la nature, l'ampleur et la complexité des activités des institutions financières et comprendre les éléments suivants :

1. des politiques, des procédures et des contrôles internes, y compris des dispositifs de contrôle de la conformité, et des procédures appropriées lors du recrutement des employés, de façon à s'assurer qu'il s'effectue selon des critères exigeants ;
2. la centralisation des informations sur l'identité des clients, des donneurs d'ordre, des bénéficiaires effectifs, des bénéficiaires et titulaires de procuration, des mandataires et sur les transactions suspectes ;
3. la désignation d'un officier de conformité et la désignation de responsables de conformité au niveau de chaque succursale, agence ou point de services, le cas échéant ;

4. l'évaluation des risques de l'institution en matière de blanchiment de capitaux, de financement du terrorisme et de la prolifération, et une classification des risques en fonction des activités et du profil de la clientèle ;
5. l'élaboration d'un programme de formation continue à l'intention des employés et des sous-agents pour les maisons de transfert ;
6. un dispositif de contrôle interne pour vérifier la conformité, l'observance et l'efficacité des mesures adoptées ;
7. la mise en place d'un dispositif de tests indépendants du contrôle de la conformité ;
8. la procédure de traitement des opérations suspectes.

Le programme de prévention doit être approuvé par le Conseil d'administration de l'institution financière ou par le correspondant étranger si l'institution financière est un agent représentant pour des activités de transfert de fonds.

1.1 Politiques, procédures et méthodes

Les institutions financières sont tenues d'élaborer et de mettre en œuvre un programme de prévention comprenant des politiques, procédures et méthodes consignées par écrit et permettant d'identifier les facteurs de risques et d'évaluer les risques de blanchiment de capitaux, de financement du terrorisme ou de la prolifération que présentent leurs activités.
Les politiques, procédures et méthodes doivent être approuvées par le Conseil d'administration et régulièrement mises à jour. Elles doivent être clairement communiquées à tous les employés appelés à interagir avec des clients.

Ces politiques et procédures doivent couvrir l'ensemble des obligations applicables en matière de déclaration, de tenue de documents, de conservation de documents, d'identification des clients et de connaissance de la clientèle, ainsi que de contrôle, d'évaluation et d'atténuation des risques. Elles doivent être intégrées à la stratégie globale de gestion des risques de l'institution financière et comporter des étapes appropriées pour prévenir, détecter, évaluer, surveiller, gérer, atténuer en permanence les risques de blanchiment de capitaux et/ou de financement du terrorisme liés notamment aux clients, pays ou zones géographiques, ou encore aux produits, services, nouvelles technologies, opérations et canaux de distribution.

Les politiques et procédures doivent également couvrir le traitement des sanctions internationales (liste de l'Organisation des Nations Unies ou autres), les modalités de gel des avoirs dans le cadre de la lutte contre le financement du terrorisme et de la prolifération.

Les politiques, procédures et méthodes doivent s'appliquer à l'ensemble des succursales, agences, points de services et filiales, lorsqu'il s'agit d'un groupe tel que défini à l'article 13 de la loi du 14 mai 2012 sur les banques et autres institutions financières. Dans ce cas, les institutions financières sont tenues d'intégrer des politiques et des procédures de partage des informations au sein du groupe aux fins de l'exercice du devoir de vigilance à l'égard de la clientèle et de gestion du risque de blanchiment de capitaux, du financement du terrorisme et de la prolifération. Des garanties appropriées doivent être mises en place afin d'assurer la confidentialité et l'utilisation adéquate des informations échangées.

Les institutions financières doivent également s'assurer que les informations relatives aux clients, aux comptes et aux opérations provenant de leurs succursales et de leurs filiales soient mises à la disposition des fonctions de conformité, d'audit et/ou de la lutte contre le blanchiment de capitaux et le financement du terrorisme au niveau du groupe.

En outre, les institutions financières doivent veiller à ce que leurs filiales à l'étranger, le cas échéant, exerçant des activités similaires, mettent en œuvre le programme de prévention du groupe y compris les politiques et procédures de partage des informations au sein du groupe. Lorsque le pays d'accueil de la filiale ne permet pas la mise en œuvre effective des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme conformes aux mesures nationales, le groupe est tenu d'appliquer des mesures supplémentaires appropriées pour gérer ces risques et d'en informer la BRH.

Par ailleurs, les maisons de transfert qui jouent le rôle d'agent doivent veiller à ce que leurs sous-agents appliquent effectivement leur programme de prévention. Il en est de même pour les bureaux de change en ce qui concerne tout réseau constitué par des sous-agents de change, le cas échéant.

Les politiques et procédures doivent prendre en compte les relations avec les banques correspondantes et couvrir les questions relatives à la collecte d'informations sur lesdites banques correspondantes (nature de leurs activités, leur clientèle, le contrôle exercé par les autorités compétentes, etc.) ainsi que la suspension et le non-établissement de relations de correspondance avec :

a) des banques étrangères qui ne disposent pas de procédures suffisantes de contrôle à l'égard des activités criminelles, ou
b) des banques étrangères qui ne sont pas assujetties à une surveillance efficace de la part des autorités compétentes, ou
c) des banques fictives.

Les institutions financières sont également tenues d'élaborer des procédures appropriées de sélection garantissant le recrutement des employés selon des critères exigeants.

1.2 Centralisation des informations

Les institutions financières doivent se doter d'un système informatique permettant la centralisation des données sur l'identité des clients, des donneurs d'ordre, des bénéficiaires effectifs, des mandataires, des titulaires de procuration et sur les transactions suspectes.

1.3 Nomination d'un officier de conformité

Toute institution financière doit procéder à la nomination d'un officier de conformité. Cet officier doit être un cadre supérieur de l'institution, choisi en fonction de sa compétence, de son expérience, de sa probité et de son éthique professionnelle. Il doit connaitre les fonctions et la structure de l'institution, et être au fait des risques et des vulnérabilités liées au blanchiment de capitaux et au financement du terrorisme dans son secteur d'activités ainsi que des tendances et des typologies qui caractérisent ces menaces.

L'officier de conformité doit relever directement du Conseil d'administration pour toutes les questions liées à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération.

L'officier de conformité a notamment pour attributions de (d') :

a) assurer l'application de la législation et de la réglementation ;
b) faire respecter les procédures et méthodes internes de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ;
c) identifier les failles et faire les recommandations qui s'imposent ;
d) proposer des programmes de formation sur une base périodique ;
e) assurer la liaison avec les sous-agents (maisons de transfert ou bureaux de change) ;
f) assurer la liaison avec l'Unité Centrale de Renseignements Financiers (UCREF) ;
g) préparer et acheminer les déclarations de soupçons à l'UCREF ;
h) s'assurer que les déclarations de transactions sont complétées et acheminées à l'UCREF dans les délais requis ;
i) recevoir et donner suite aux demandes d'informations de l'UCREF et de toute autre autorité agissant dans le cadre de la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération.

Les institutions financières doivent désigner, dans chaque succursale, agence ou point de services, un cadre chargé de faire respecter les lois et réglementations anti-blanchiment et d'assurer la coordination avec l'officier de conformité. Pour assurer l'application du programme de prévention, l'officier de conformité peut déléguer certaines fonctions à d'autres employés. En aucun cas, la désignation de ces cadres ne dispense l'officier de conformité de ses responsabilités par rapport à la loi.

1.4 Évaluation des risques

Le programme de prévention et de conformité doit comprendre un volet relatif à l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme.

L'évaluation des risques est une analyse des menaces et faiblesses en matière de blanchiment de capitaux et de financement du terrorisme que présentent les activités de l'institution financière. Cette évaluation varie notamment selon la taille de l'institution financière, son emplacement géographique et selon les activités exercées. Une classification des risques doit être effectuée en fonction des services offerts, des conditions des transactions proposées, des canaux de distribution utilisés, des caractéristiques des clients, du pays ou du territoire d'origine ou de destination des fonds, des régions géographiques d'activités.

L'évaluation des risques implique que les employés soient bien imbus des activités de l'institution et qu'ils fassent preuve de jugement afin d'évaluer les risques. Cette évaluation ne doit pas être statique et devra être mise à jour au moins tous les douze (12) mois.

1.5 Formation continue

Le programme de prévention doit inclure une composante de formation. Tous les employés qui sont en contact avec les clients, qui ont connaissance d'opérations effectuées par des clients ou qui manipulent des espèces ou des fonds de quelque façon que ce soit ou qui sont responsables de la mise en œuvre ou de la surveillance du régime de conformité doivent comprendre notamment les obligations de déclaration, d'identification des clients et de tenue de documents.

Tous les sous-agents appartenant au réseau d'une maison de transfert ou d'une banque doivent également comprendre les obligations de déclaration, d'identification des clients et de tenue de documents. Il en est de même des agents de distribution des fournisseurs de services de paiement électronique.

Le programme de formation doit être consigné par écrit et tenu à jour. Les modalités entourant la fréquence et la méthode de formation doivent être établies. On doit y indiquer notamment les catégories de participants, les sujets qui seront couverts et la fréquence des séances de formation. Chaque nouvel employé ou nouveau sous-agent ou nouveau agent de distribution doit être formé avant de commencer à travailler avec des clients.

Des mises à jour du programme doivent avoir lieu périodiquement afin de tenir toutes les parties intéressées au courant des modifications législatives et règlementaires.

Le programme et le plan de formation continue doivent être adaptés à la taille, à la structure de l'institution, à la complexité de ses activités et à son niveau d'exposition au risque de blanchiment de capitaux et de financement du terrorisme.

1.6 Dispositif de contrôle interne

Les institutions financières doivent faire preuve d'une vigilance constante et se doter d'une organisation ainsi que de procédures internes propres à assurer le respect des dispositions légales en vigueur. Ces mesures doivent permettre aux responsables des opérations de prévenir et de détecter toute tentative de blanchiment de capitaux ou de financement du terrorisme. L'un des objectifs essentiels de ce contrôle est de prévenir l'utilisation du système financier à des fins de blanchiment de capitaux, de financement du terrorisme ou de financement de la prolifération, tout en minimisant les risques auxquels les institutions financières sont exposées.

Ce système de contrôle interne doit contenir, entre autres :

a) un mécanisme de contrôle des politiques, procédures et méthodes internes de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ;
b) une structure garantissant la confidentialité du traitement des informations ;
c) des mesures d'identification des éléments à risques liés au blanchiment de capitaux, au financement du terrorisme et de la prolifération, et des systèmes d'évaluation de ces risques ;
d) un système de surveillance pouvant garantir la maîtrise des risques relatifs au blanchiment de capitaux, au financement du terrorisme et de la prolifération ;
e) un système centralisé de documentation et d'information ;

f) un système d'information sur les initiatives prises en matière de conformité, de déficience dans ce domaine et des mesures correctives prises.

Le système de contrôle en place doit s'étendre à toutes les composantes de l'institution. Les institutions financières sont donc tenues de prendre les mesures nécessaires pour garantir la stricte application des politiques, procédures et méthodes en vigueur spécialement celles relatives au blanchiment de capitaux, au financement du terrorisme et de la prolifération.

Les fournisseurs de services de paiement électronique sont tenus de mettre en place un système de surveillance fondé sur les risques, basé sur le volume et la valeur des transactions, afin de permettre la détection des violations des limites de transaction et de la taille des portefeuilles. Ledit système doit également permettre aux fournisseurs de services de paiement électronique de détecter et d'analyser les activités suspectes et/ou inhabituelles et, lorsque cela est jugé nécessaire, de produire une déclaration de soupçons auprès de l'UCREF, dans les meilleurs délais.

1.7 Dispositif de tests indépendants

Lors des tests indépendants périodiques portant sur le respect des procédures internes, ou la bonne surveillance des risques, une vérification spécifique sur le volet blanchiment de capitaux, financement du terrorisme et de la prolifération doit être effectuée par l'audit interne de l'institution.

Les vérifications peuvent notamment s'appliquer aux points suivants :

a) l'évaluation de la qualité de la gestion et du contrôle des risques pour toutes les opérations et dans toutes les succursales, agences et/ou points de services ;
b) des entrevues avec des employés chargés des opérations et de leurs superviseurs pour évaluer leur degré de connaissance et de respect des procédures de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération adoptées par l'institution ;
c) le respect des procédures d'ouverture et de fermeture de comptes ;
d) l'examen d'un échantillon de profil de clients, de filtrage de sanctions, de formulaires d'archivage des documents et de formulaires de renseignements sur les transactions financières douteuses ;
e) la vérification du système de tenue des documents ;
f) l'existence des justificatifs joints ou référencés aux pièces comptables ;
g) la connaissance de la clientèle par les succursales et les responsables des opérations, en tenant compte des éléments suivants : activité professionnelle, fonctionnement du compte, situation financière et documentation comptable et financière concordante avec les crédits consentis et les volumes d'affaires traitées. Une attention particulière doit être portée à la justification économique des opérations et leur adéquation avec la situation connue de la clientèle ;
h) des examens périodiques de toutes les relations de correspondants bancaires établies avec des banques étrangères afin de détecter les partenaires à haut risque ;
i) la connaissance des collaborateurs des règles internes anti-blanchiment.

Les résultats de toute vérification doivent être soumis au Conseil d'administration. Suivant la structure hiérarchique de l'institution, les questions relatives aux mesures prises ou à prendre et aux échéanciers prévus à cet égard doivent être connues et divulguées au personnel exécutant.

1.8 Traitement des opérations suspectes

Les institutions financières doivent élaborer et mettre en œuvre des politiques relatives à l'identification et au suivi des transactions inhabituelles ou suspectes. Ces politiques doivent préciser ce qui est considéré comme suspect ou inhabituel et fournir des exemples concrets à cet égard.

L'identification des transactions inhabituelles ou suspectes peut être effectuée par différents moyens notamment : la surveillance des opérations, les contacts avec le client (rencontres, visites, discussions, etc.), des informations en provenance de tiers (journaux, internet, etc.), et la connaissance qu'à l'institution financière de l'environnement et du profil du client.

Pour toute transaction qui parait complexe, inhabituelle, injustifiée ou dépourvue de justification économique ou d'objet licite, même lorsque le montant en jeu n'atteint pas le seuil règlementaire, les institutions financières doivent recueillir toutes les informations pertinentes concernant l'origine des fonds, l'objet de l'opération et l'identité des personnes impliquées. Un rapport confidentiel écrit doit être établi. Il doit comporter tous les renseignements utiles et requis par la loi, notamment les modalités de l'opération, l'identité du donneur d'ordre et, le cas échéant, celle des autres acteurs économiques impliqués.

Les déclarations de transactions et les déclarations de soupçons doivent être transmises à l'UCREF par voie de communication électronique, ou à défaut par tout moyen écrit, conformément aux délais fixés par la réglementation en vigueur.

2. Du devoir de vigilance relatif à la clientèle

Les institutions financières doivent accorder une importance particulière aux normes relatives à la connaissance du client pour préserver leur réputation et l'intégrité du système financier. Pour ne pas s'exposer au risque d'atteinte à la réputation, au risque opérationnel et au risque juridique, les institutions financières doivent disposer de politiques, méthodes et procédures appropriées en tenant compte entre autres des éléments suivants :

a) des conditions claires d'acceptation de nouveaux clients ;
b) des règles précises sur l'identification des clients permanents ou occasionnels et de leurs mandataires, des bénéficiaires effectifs, des donneurs d'ordre et des bénéficiaires ;
c) des règles relatives aux opérations occasionnelles de montant élevé ;
d) une surveillance constante des comptes à hauts risques ;
e) des procédures et moyens appropriés pour la gestion des risques et la surveillance constante de la clientèle ;
f) des conditions claires d'abandon d'une relation avec un client, si cela s'avère nécessaire ;
g) des mesures de vigilance pour la clientèle.

Les institutions financières doivent disposer de procédures de gestion des risques quant aux conditions dans lesquelles un client peut bénéficier de la relation d'affaires avant la vérification de son identification (opérations n'impliquant pas la présence physique du client).

Avant l'établissement d'une relation d'affaires avec un client, l'institution financière est tenue, en fonction de sa politique d'acceptation des clients, d'examiner les risques de réputation associés au profil du client et à la nature de la relation d'affaires.

Les institutions financières doivent adopter et appliquer des mesures de vigilance à l'égard de la clientèle lors :

1) de l'établissement de la relation d'affaires ;
2) des transactions occasionnelles supérieures à un million trois cent vingt mille gourdes (1,320,000.^{00} HTG) ou en cas de répétition d'opérations distinctes de montant individuel inférieur à un million trois cent vingt mille gourdes (1,320,000.^{00} HTG) ou lorsque la provenance licite des fonds n'est pas certaine ou s'il s'agit d'un transfert de fonds au niveau national ou international ;
3) des transactions sous forme de virements électroniques (transferts de fonds) ;
4) des transactions multiples en espèces, tant en gourdes qu'en devises étrangères, lorsque le total dépasse un million trois cent vingt mille gourdes (1,320,000.^{00} HTG) et lorsqu'elles sont réalisées par et pour le compte de la même personne en l'espace d'une journée ou dans une fréquence inhabituelle ;
5) de l'existence d'un soupçon de blanchiment de capitaux ;
6) de l'existence d'un soupçon de financement du terrorisme ;
7) des doutes quant à la véracité ou la pertinence des données d'identification du client précédemment obtenues.

La mise en œuvre des mesures de vigilance doit s'effectuer selon le risque identifié. À l'issue de l'évaluation des risques, un niveau de risque (faible, moyen ou élevé) doit être attribué à chaque client afin d'ajuster les mesures de vigilance appropriées.

2.1. Vigilance constante

Les institutions financières doivent exercer une vigilance constante pendant toute la durée de la relation d'affaires et examiner attentivement les opérations effectuées par la clientèle en vue de s'assurer qu'elles sont conformes à ce qu'elles savent de leurs clients, de leurs activités commerciales, de leur profil de risque et le cas échéant de la source de leurs fonds. Elles doivent recueillir, mettre à jour et analyser les éléments d'informations pouvant leur permettre d'avoir une connaissance appropriée de la clientèle. Elles doivent s'assurer que les documents ou informations obtenus dans l'exercice du devoir de vigilance sont à jour et pertinents.

2.2. Vigilance simplifiée

Sous réserve d'une évaluation des risques, les institutions de microfinance, les coopératives d'épargne et de crédit, les fournisseurs de services de paiement électronique et les banques peuvent, uniquement pendant l'établissement de la relation d'affaires, appliquer des mesures de

vigilance simplifiée et procéder à l'identification des clients, et le cas échéant du bénéficiaire effectif, si et seulement si :

a) le client présente un faible risque de blanchiment de capitaux ou de financement du terrorisme ;
b) les produits ou services financiers sont limités et bien définis à certains types de clients présentant un faible risque de blanchiment de capitaux ou de financement du terrorisme (cartes prépayées, comptes de fonds de paiement électronique, etc…) ;
c) le risque de blanchiment de capitaux ou de financement du terrorisme est évalué comme étant faible ;
d) le client est une institution financière établie en Haïti ou a son siège dans un autre pays imposant des obligations équivalentes de lutte contre le blanchiment de capitaux et de financement du terrorisme.

À ce titre, les institutions mentionnées dans la présente section doivent recueillir les informations justifiant que le client ou le produit présente un risque faible. Toutefois, elles sont tenues de mettre un dispositif de contrôle des transactions et de la clientèle pour être en mesure de détecter toute transaction inhabituelle ou suspecte.

Lorsque les institutions financières mentionnées dans la présente section choisissent de mettre en œuvre des mesures de vigilance simplifiées en application de l'article 62 du décret de 2023, elles doivent identifier et vérifier l'identité du client et, le cas échéant, du bénéficiaire effectif. Les fournisseurs de services de paiement électronique sont tenus de mettre en œuvre les mesures de vigilance simplifiées suivant les indications fournies à l'Annexe II de la présente circulaire.

Les institutions financières doivent être en mesure de justifier auprès de la BRH que l'étendue des mesures de vigilance qu'elles mettent en œuvre est adaptée aux risques qu'elles ont évalués.

2.3. Vigilance renforcée

Les institutions financières doivent appliquer, en fonction de leur appréciation du risque, des mesures de vigilance renforcées dans des situations qui, par leur nature, peuvent présenter un risque élevé de blanchiment de capitaux ou de financement du terrorisme et, à tout le moins, dans les cas suivants (liste non limitative) :

a) lorsque le client ou son bénéficiaire effectif n'est pas présent physiquement ;
b) le client ou son bénéficiaire effectif est une personne politiquement exposée résidant à l'étranger ;
c) lorsqu'il y a des relations de correspondants bancaires.

En outre, comme le prescrit l'article 28 du décret du 30 avril 2023, une attention particulière doit être exercée à l'égard des relations d'affaires et des opérations avec des personnes physiques ou morales, y compris les institutions financières, provenant de pays qui n'appliquent pas ou appliquent insuffisamment les normes internationales en matière de lutte contre le blanchiment de capitaux et contre le financement du terrorisme. Les institutions financières doivent leur appliquer

des mesures de vigilance renforcées, proportionnées aux risques, comme le requiert le Groupe d'Action Financière (GAFI).

Par ailleurs, les institutions financières sont tenues d'appliquer des mesures de vigilance renforcées à l'égard de la clientèle opérant dans des secteurs d'activités où l'utilisation des espèces est fortement constatée, et de celle évoluant dans des secteurs dont la réglementation est insuffisante et qui font partie de la catégorie dénommée « entreprises et professions non financières désignées (EPNFD) ».

3. De l'identification de la clientèle

En conformité avec les dispositions du décret du 30 avril 2023 sanctionnant le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive, les institutions financières sont tenues d'identifier leurs clients permanents ou occasionnels, les mandataires de leurs clients, les titulaires de procuration et les bénéficiaires effectifs. Les maisons de transfert doivent également s'assurer que leurs sous-agents appliquent des mesures préventives équivalentes.

Avant d'entrer en relation d'affaires avec un client, qu'il s'agisse d'une personne physique ou morale ou d'une construction juridique, les institutions financières doivent recueillir et analyser les éléments d'informations nécessaires à la connaissance du client ainsi que l'objet et la nature envisagée de la relation d'affaires. Pour les personnes morales ou les constructions juridiques, les institutions financières doivent comprendre leur structure de propriété et de contrôle.

Lorsque les clients n'agissent pas pour leur propre compte, les institutions financières sont tenues de se renseigner par tout moyen sur l'identité du véritable donneur d'ordre. Après vérification, si le doute persiste sur l'identité du véritable donneur d'ordre, il doit être mis fin à l'opération, sans préjudice de l'obligation d'effectuer une déclaration de soupçon. En outre, un avocat, un notaire, un comptable, un courtier en valeurs mobilières intervenant en tant qu'intermédiaire financier ne peut invoquer le secret professionnel pour refuser de divulguer l'identité du véritable donneur d'ordre, conformément à l'article 43 du décret du 30 avril 2023.

Lors de l'identification des clients, une copie de tous les documents doit être faite, classée et centralisée par l'institution financière. Des contrôles formels doivent être effectués quant à la signature, aux éventuelles anomalies sur la photographie et à l'apparence physique du client potentiel.

Les pièces, documents et renseignements requis pour l'identification des clients doivent être exigés lors des remises et transmissions de fonds pour un montant global égale ou supérieur à cent trente-deux mille gourdes (132,000.^{00} HTG) ou l'équivalent en monnaie étrangère, ainsi que pour toute opération occasionnelle d'un montant élevé ou toute transaction effectuée dans des conditions de complexité inhabituelles ou injustifiées.

Les maisons de transfert doivent s'assurer que les opérations de transferts contiennent toutes les informations requises relatives au donneur d'ordre et au bénéficiaire et prendre des mesures appropriées lorsque ces informations sont incomplètes ou manquantes, ce conformément aux

articles 47 à 54 du décret du 30 avril 2023. Le donneur d'ordre et le bénéficiaire peuvent être une seule et même personne. Le transfert peut être transfrontalier ou national.

Les institutions financières doivent prendre toutes les mesures particulières et suffisantes pour prévenir le blanchiment de capitaux et le financement du terrorisme lorsqu'elles entretiennent des relations d'affaires ou exécutent des opérations avec un client qui n'est pas physiquement présent aux fins d'identification, ce conformément à l'article 36 du décret du 30 avril 2023.

Si les institutions financières ne sont pas en mesure de se conformer aux dispositions prévues ci-dessus, elles ne peuvent ni nouer ou maintenir une relation d'affaires, ni effectuer une opération pour le client. Elles détermineront, dans ce cas, s'il y a lieu de produire une déclaration de soupçon à l'UCREF ou d'établir un rapport confidentiel interne conformément à l'article 46 du décret du 30 avril 2023.

Les institutions financières ne sont pas tenues de procéder de manière répétée à l'identification et à la vérification de l'identité d'un client à chaque opération effectuée par celui-ci. Elles peuvent s'en remettre aux mesures d'identification et de vérification déjà réalisées, à moins qu'elles aient des doutes quant à l'exactitude ou à la fiabilité des informations précédemment obtenues.

3.1 De l'identification des personnes physiques

L'identification d'une personne physique selon l'article 36 du décret du 30 avril 2023 implique « *l'obtention des nom et prénom complets, de la date et du lieu de naissance, et de l'adresse de son domicile principal* ». Les institutions financières sont tenues d'obtenir en ce sens les renseignements suivants :

a) patronyme légal et autres noms utilisés (par exemple nom de jeune fille) ;
b) date et lieu de naissance ;
c) nationalité ;
d) profession, charge publique et/ou nom de l'employeur ;
e) adresse (l'adresse complète doit être obtenue, un numéro de boite postale n'est pas suffisant) ;
f) pays de résidence ;
g) numéros de téléphone, courrier électronique.

Les personnes physiques non résidentes dans le pays doivent être identifiées de la même manière que les résidents. Les enfants mineurs doivent être représentés par un parent, client de l'institution financière, sinon des preuves documentaires sur l'identité de l'enfant et de son tuteur légal doivent être apportées.

3.2 De l'identification des personnes morales et des constructions juridiques

Lorsque le client est une personne morale ou une construction juridique, l'identification porte sur « *la dénomination sociale, la preuve de sa constitution légale, l'adresse du siège social, l'identité et les pouvoirs des administrateurs et dirigeants sociaux ou de leurs équivalents en droit étranger* », selon l'article 38 du décret du 30 avril 2023.

Les institutions financières sont tenues d'obtenir les renseignements suivants aux fins d'identifier les personnes morales :

a) adresse du siège principal de la société ou, si elle est différente, celle de l'un des principaux lieux d'activité (l'adresse complète doit être obtenue, un numéro de boite postale n'est pas suffisant) ;
b) numéros de téléphone, courrier électronique, site internet ;
c) nom(s) et prénom(s) des actionnaires, pays de résidence, catégorie d'actions détenues (nominative ou au porteur), pourcentage d'actions détenues (*pour les sociétés anonymes*) ;
d) nom(s) et prénom(s) des associés, des fondateurs, pays de résidence, pourcentage de parts sociales détenues (*suivant la forme juridique de la personne morale*) ;
e) nom(s) et prénom(s) des propriétaires, des membres du Conseil d'administration, des dirigeants (*suivant la forme juridique de la personne morale*) ;
f) nom(s) et prénom(s), profession, adresse des mandataires et des bénéficiaires effectifs, téléphone, courrier électronique, le cas échéant.

4. De la vérification de l'identité de la clientèle

Les institutions financières sont tenues de vérifier l'identité des clients au moyen de documents, de données ou d'informations provenant de sources fiables et indépendantes.

En ce qui a trait à la vérification des informations, l'article 36 du décret du 30 avril 2023 précise que : « l*a vérification de l'identité d'une personne physique requiert la présentation d'un (1) document officiel original en cours de validité et comportant une photographie, dont il en est pris copie. La vérification de son adresse est effectuée par la présentation d'un (1) document de nature à en rapporter la preuve ou par tout autre moyen* ».

Lorsque le client est une personne morale ou une construction juridique, la vérification porte sur « *la dénomination sociale, l'adresse du siège social, l'identité et les pouvoirs des administrateurs et dirigeants sociaux ou de leurs équivalents en droit étranger, la preuve de sa constitution légale à savoir l'original, voire l'expédition ou la copie certifiée conforme de tout acte ou extrait du registre du commerce attestant notamment de sa forme juridique* », selon l'article 38 du décret du 30 avril 2023.

La liste des pièces et documents d'identification exigibles figure à l'annexe de la présente circulaire.

5. Des bénéficiaires effectifs

Les institutions financières sont tenues d'identifier les bénéficiaires effectifs conformément aux dispositions des articles 40 à 42 du décret du 30 avril 2023. Elles doivent prendre des mesures appropriées afin de vérifier l'exactitude des informations recueillies et d'en assurer leur mise à jour lorsqu'il apparait que celles-ci ne sont plus actuelles.

Si les institutions financières ne peuvent pas obtenir ces informations ou si leurs clients restent en défaut de les communiquer, ou leur communiquent des informations non pertinentes ou invraisemblables, elles ne peuvent ni nouer ou maintenir une relation d'affaires, ni effectuer une opération pour le client. Elles détermineront, dans ce cas, s'il y a lieu d'en informer l'UCREF.

6. Les personnes politiquement exposées

Un devoir de vigilance renforcée doit être exercé à l'égard des personnes politiquement exposées (PPE) qui, en vertu de l'article 6 du décret du 30 avril 2023, sont définies comme des personnes qui exercent ou ont exercé d'importantes fonctions publiques dans un pays étranger ou en Haïti ou au sein de ou pour le compte d'une organisation internationale, ainsi que les membres de leur famille, ou toute autre personne qui leur est étroitement liée ou associée.

Les institutions financières doivent disposer de systèmes appropriés de gestion de risques leur permettant de déterminer si un client ou un bénéficiaire effectif est une personne politiquement exposée. Dès qu'un client est identifié comme personne politiquement exposée, il faut :

a) obtenir l'autorisation de la haute direction avant de nouer ou de continuer une relation d'affaires avec lui ;
b) prendre toutes les mesures appropriées pour établir l'origine du patrimoine et l'origine des fonds dudit client et de son ou ses bénéficiaires effectifs ;
c) assurer une surveillance continue renforcée de la relation d'affaires.

Lors du versement des prestations de contrats d'assurance vie, les institutions financières doivent prendre des mesures raisonnables afin de déterminer si les bénéficiaires d'un contrat d'assurance vie et/ou le bénéficiaire effectif du bénéficiaire du contrat sont des PPE.

Lors du versement des prestations, si des risques plus élevés sont identifiés, il faut que :

a) la haute direction soit informée avant le paiement du capital ;
b) soit entrepris un examen renforcé de l'ensemble de la relation d'affaires avec le titulaire du contrat ;
c) soit envisagée la rédaction d'une déclaration de soupçon, le cas échéant.

En sus des PPE, un contrôle rigoureux doit être appliqué envers toute personne ayant une fortune élevée d'origine incertaine ou douteuse.

7. Élaboration du profil de risque de la clientèle

Les institutions financières doivent établir le profil de risque des clients ou de catégorie de clients afin d'assurer une vigilance constante à l'égard de la clientèle.

Le profil de risque constitue une évaluation individualisée du niveau de risque présenté par chaque client. Il prend en compte des éléments permettant de caractériser ce risque, notamment : les

activités exercées (profession), les revenus ou la situation financière, tout élément permettant d'apprécier le patrimoine, l'objet et la nature intentionnels de la relation d'affaires ou de l'opération ponctuelle, le niveau d'activité attendu, la provenance des fonds, les opérations envisagées ou réalisées, le fonctionnement envisagé du compte, etc.

Le profil de risque doit être complet, exact et mis à jour selon une fréquence proportionnée au niveau de risque identifié.

8. Clients existants

Les institutions financières sont tenues d'appliquer à leurs clients existants, à la date d'entrée en vigueur de toutes nouvelles lois ou règlementations, les mesures de vigilance à la clientèle en tenant compte du moment où elles ont été mises en œuvre antérieurement ainsi que de la pertinence des informations obtenues, selon l'importance des risques qu'ils représentent.

9. Mise à jour des renseignements sur la clientèle

La fréquence des mises à jour des renseignements sur les clients, varie selon le contexte dans lequel les opérations se déroulent, donc d'une situation à l'autre. Les institutions financières sont responsables du choix de la fréquence qui ne peut dépasser trois (3) ans. Toutefois, pour les situations posant des risques élevés, les mises à jour doivent être effectuées au moins tous les deux (2) ans.

10. Correspondant bancaire transfrontalier

Toutes les institutions financières doivent disposer de politiques, procédures et mécanismes susceptibles de favoriser une bonne connaissance des activités légitimes de leurs correspondants bancaires transfrontaliers et autres relations similaires. Les institutions financières doivent s'assurer :

a) de vérifier l'identification des institutions clientes pour lesquelles elles jouent le rôle de correspondant bancaire ;
b) de recueillir des informations sur la nature des activités de l'institution cliente ;
c) d'évaluer, sur la base d'informations publiquement disponibles, la réputation de l'institution cliente et le degré de surveillance à laquelle elle est soumise et de déterminer si elle a fait l'objet d'une enquête ou de mesures de la part d'une autorité de contrôle en matière de blanchiment de capitaux ou de financement du terrorisme ;
d) d'évaluer les contrôles mis en place par l'institution cliente pour lutter contre le blanchiment de capitaux et le financement du terrorisme ;
e) pour les comptes de passage, que l'institution cliente a appliqué les mesures de vigilance aux clients ayant un accès direct à ses comptes et qu'elle est en mesure de fournir les données d'identification pertinentes sur demande ;
f) de comprendre les responsabilités respectives de chaque institution en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
g) d'obtenir l'autorisation de la haute direction avant d'établir de nouvelles relations de correspondance bancaire.

Les institutions financières ne peuvent en outre établir une fonction de correspondant bancaire avec une banque fictive. Elles doivent s'assurer que leur correspondant bancaire ne noue pas ou ne maintient pas des relations avec des banques fictives.

11. Virement électronique

On entend par virement électronique, toute transaction effectuée par voie électronique pour le compte d'un donneur d'ordre (personne physique ou morale) en vue de mettre à disposition d'un bénéficiaire une somme d'argent déterminée.

Dans le cadre d'opérations de virement électronique transfrontalier ou national, les institutions financières doivent identifier les donneurs d'ordre et les bénéficiaires effectifs conformément aux dispositions de l'article 47 du décret du 30 avril 2023. L'identification comprend les prénoms, le nom, l'adresse, le numéro de compte le cas échéant et tout autre renseignement qui accompagne le virement électronique ou le message qui s'y rapporte tout au long de la chaîne de paiement.

Les institutions financières doivent s'assurer que les virements électroniques contiennent toutes les informations requises sur le donneur d'ordre et/ou le bénéficiaire et prendre, le cas échéant, les mesures appropriées lorsque ces informations sont incomplètes ou absentes. À cet effet, elles sont tenues de mettre en œuvre toutes les dispositions relatives aux articles 48 à 53 du décret du 30 avril 2023.

Les institutions financières du bénéficiaire doivent élaborer et mettre en application des politiques et procédures fondées sur le risque afin d'être en mesure de décider quand exécuter, rejeter ou suspendre les virements électroniques qui ne comportent pas les informations requises relatives au donneur d'ordre ou au bénéficiaire. Ces politiques et procédures doivent également prévoir les mesures et actions consécutives appropriées aux situations susmentionnées.

Les dispositions de la présente section ne s'appliquent pas :

a) aux virements de fonds effectués au moyen d'une carte de crédit ou de débit ou par carte prépayée ou d'un téléphone portable pour l'achat de biens et de services tant que le numéro de ladite carte ou du téléphone accompagne l'ensemble des transferts découlant de l'opération ;
b) aux transferts effectués entre les institutions financières lorsque le donneur d'ordre et le bénéficiaire sont des institutions financières opérant pour leur propre compte ;
c) aux virements effectués au profit d'autorités publiques pour le paiement d'impôts, d'amendes ou d'autres prélèvements.

12. Recours à des tiers

Les institutions financières peuvent avoir recours à des intermédiaires ou autre tiers pour l'exécution de leurs obligations à l'entrée en relation d'affaires et de l'obligation de vigilance constante sur la clientèle et sur toutes les opérations de la clientèle. Les obligations de vigilance dont la mise en œuvre peut être confiée à un tiers comprennent entre autres : l'identification et la

vérification de l'identité du client et du bénéficiaire effectif, le cas échéant ; la connaissance de l'objet et de la nature de la relation d'affaires ; toute information pertinente sur le client.

Elles doivent s'assurer que :

a) le tiers est en mesure de fournir sur demande et sans retard des copies des données d'identification et autres documents qui ont trait à l'obligation de vigilance ;
b) le tiers est soumis à une réglementation, fait l'objet d'un contrôle ou d'une surveillance et a pris des mesures pour respecter les obligations de vigilance relatives à la clientèle et les obligations de conservation de documents, s'il s'agit d'une autre institution financière.

La responsabilité finale appartient aux institutions financières qui ont recours aux tiers.

Cette obligation ne s'applique pas aux relations de sous-traitance ou de mandat.

13. Des technologies nouvelles

Les institutions financières doivent identifier et évaluer les risques de blanchiment de capitaux et de financement du terrorisme pouvant résulter :

a) du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution ;
b) de l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants.

Cette évaluation de risques 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 doivent prendre des mesures appropriées pour gérer ces risques.

14. Conservation de documents

Les institutions financières sont tenues de conserver pendant une période de cinq (5) ans au moins, après la clôture des comptes ou la cessation des relations avec le client habituel ou occasionnel, les pièces et documents obtenus dans le cadre des mesures de vigilance relative à la clientèle. Elles conservent également les pièces et documents relatifs aux opérations nationales et internationales que les clients ont effectuées, les livres de comptes et les correspondances commerciales, les résultats de toute analyse réalisée pendant cinq (5) ans au moins après l'exécution de l'opération ou la fin de la relation. De même, une copie des déclarations faites auprès de l'UCREF doit être gardée et archivée par les institutions financières.

Les institutions financières doivent conserver pendant une période de cinq (5) ans au moins les informations collectées sur les donneurs d'ordre et les bénéficiaires lors des transferts internationaux et nationaux.

À cette fin, une formule d'archivage des documents sur les opérations doit être utilisée pour la conservation des documents.

Cette conservation des documents, se rapportant aux transactions nationales et/ou internationales effectuées, permettra de répondre rapidement aux demandes d'informations des autorités compétentes et de reconstituer les transactions individuelles (y compris les montants et les types d'espèces en cause, le cas échéant) de façon à fournir, le cas échéant, des preuves en cas de poursuite pour conduite criminelle.

Les institutions financières ont l'obligation de fournir toutes les informations requises avec célérité aux autorités judiciaires compétentes, aux autorités chargées de la détection et de la répression des infractions liées au blanchiment de capitaux et au financement du terrorisme, et aux autorités d'enquête.

15. Recours à des sous-agents

Les maisons de transfert sont tenues de veiller au respect par leurs sous-agents des lois et règlements relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Elles doivent s'assurer que les sous-agents sont en mesure de fournir sur demande et sans retard des copies des données d'identification et autres documents qui ont trait à l'obligation de vigilance.

16. Sanctions

En cas de non-respect des obligations définies dans la loi ou dans la présente circulaire, notamment :

a) grave défaut de vigilance ou non-respect des obligations d'identification de la clientèle,
b) non-production de déclarations de soupçons,
c) dénonciation, faite aux clients ou à des tiers, relative aux actions entreprises en matière de prévention et détection du blanchiment de capitaux et du financement du terrorisme,
d) violation des obligations contenues dans le décret du 30 avril 2023 et règlements de la BRH,

la BRH se réserve le droit d'engager toute procédure appropriée et/ou de prendre toutes mesures administratives conformément à la loi et à la règlementation en vigueur.

Les sanctions peuvent être :

a) soit des amendes : cinq cent mille gourdes (500,000.^{00} HTG) par violation constatée,
b) soit des sanctions administratives (avertissement, suspension d'activité, retrait d'agrément ou interdiction définitive dans les cas les plus graves) sans préjudice de celles prévues par la loi, et de celles résultant de la responsabilité civile ou pénale de l'institution financière qui peut être engagée en raison de la commission de l'infraction.

La BRH peut exiger d'une institution financière qu'elle apporte les corrections nécessaires quant aux violations relatives à la loi et à la présente circulaire. À défaut de se conformer aux actions de redressement requises par la BRH, l'institution financière est assujettie à une pénalité de trois cent

mille gourdes (300,000.^{00} HTG) par jour d'infraction à compter de la date à laquelle l'infraction lui est notifiée par la BRH, sans dépasser trente (30) jours.

Toute pénalité sera déduite du solde du compte de l'institution fautive à la BRH.

17. Abrogation et Entrée en vigueur

La présente circulaire abroge la circulaire 129 du 31 mars 2025 et entre en vigueur le 2 mars 2026.

Port-au-Prince, le 6 février 2026.

Ronald Gabriel
Gouverneur

Liste des annexes

Annexe I : Liste des pièces et documents
Annexe II : Exigences d'identification et de vérification pour les fournisseurs de services de paiement électronique

ANNEXE I

LISTE DES PIECES ET DOCUMENTS

Les pièces et documents suivants doivent être exigés lors de l'ouverture de comptes, l'émission de cartes de paiement, la location de coffres, l'exécution des transactions importantes en espèces c'est-à-dire pour une somme globalement égale ou supérieure au seuil établi par la BRH dans la présente circulaire ou l'équivalent en devise étrangère, pour une opération occasionnelle de montant globalement égal ou supérieur au seuil établi dans la présente circulaire ou l'équivalent en devise étrangère, pour toute transaction effectuée dans des conditions de complexité inhabituelles ou injustifiées, pour toute transaction qui parait ne pas avoir de justification économique ou d'objet licite, au moment de l'exécution de transactions sous forme de virement électronique, pour la garde des titres et d'autres avoirs, ou toutes autres transactions.

1. Personnes physiques

a) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) ;
b) un (1) document prouvant l'adresse : facture d'électricité, facture d'eau, facture d'internet, avis d'imposition ou relevé bancaire, preuve d'adresse émise par la mairie, géolocalisation par l'institution financière, etc.

2. Enfants mineurs

a) acte de naissance ou extrait d'archives ;
b) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou permis de conduire ou passeport) identifiant l'un des parents et un (1) document prouvant l'adresse du parent, ou
c) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou permis de conduire ou passeport) du tuteur légal et un (1) document prouvant l'adresse du tuteur ;
d) jugement homologuant le conseil de famille, le cas échéant.

3. Personnes morales

Société civile

a) contrat ou convention créant la société dûment enregistrée au Ministère du Commerce et de l'Industrie ;
b) copie de la carte d'immatriculation fiscale et du certificat de patente ;
c) un (1) document habilitant un ou plusieurs associés à effectuer des transactions et opérations financières ;

d) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les associés mandataires et les bénéficiaires effectifs ;
e) un (1) document prouvant l'adresse des associés mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, preuve d'adresse émise par la mairie, etc.).

Société en nom collectif et Société en commandite

a) acte constitutif de la société dûment enregistrée au Ministère du Commerce et de l'Industrie ;
b) statuts de la société dûment enregistrée au Ministère du Commerce et de l'Industrie ;
c) copie de la carte d'immatriculation fiscale et du certificat de patente ;
d) un (1) document habilitant un ou plusieurs associés à effectuer des transactions et opérations financières ;
e) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les associés mandataires et les bénéficiaires effectifs ;
f) un (1) document prouvant l'adresse des associés mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, preuve d'adresse émise par la mairie, etc.).

Société anonyme

a) autorisation de fonctionnement délivrée par le Ministère du Commerce et de l'Industrie ;
b) statuts de la société dûment enregistrée au Ministère du Commerce et de l'Industrie ;
c) copie de la carte d'immatriculation fiscale et du certificat de patente ;
d) un (1) document du Conseil d'administration habilitant une ou des personnes à effectuer des transactions et opérations financières ;
e) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les mandataires et les bénéficiaires effectifs ;
f) un (1) document prouvant l'adresse des mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, etc.).

Les sociétés anonymes de droit étranger doivent fournir toutes les pièces ci-dessus mentionnées. Les copies de documents doivent être certifiées conformes aux originaux par une autorité mandatée à cette fin (notaire, autorité consulaire, etc.) et traduits en français, le cas échéant.

Organisation Non Gouvernementale (ONG)

a) autorisation de fonctionnement délivrée par le Ministère de la Planification et de la Coopération Externe ;
b) statuts de l'ONG ;
c) copie de la carte d'immatriculation fiscale et du certificat de patente ;

d) un (1) document des membres du conseil de direction adressé aux personnes habilitées à faire des transactions et opérations financières ;
e) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les mandataires et les bénéficiaires effectifs ;
f) un (1) document prouvant l'adresse des mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, etc.).

Coopératives (épargne et crédit, agricole, de transport, etc.)

a) autorisation de fonctionnement délivrée par le Conseil National des Coopératives ou par la BRH, le cas échéant ;
b) statuts de la coopérative dûment enregistrés au Conseil National des Coopératives ;
c) copie de la carte d'immatriculation fiscale ;
d) un (1) document du Conseil d'administration aux personnes habilitées à faire des transactions et opérations financières ;
e) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les mandataires ;
f) un (1) document prouvant l'adresse des mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, etc.).

Fondation

a) inscription délivrée par la Mairie ;
b) statuts de la fondation ;
c) copie de la carte d'immatriculation fiscale ;
d) un (1) document du Conseil d'administration adressé aux personnes habilitées à faire des transactions et opérations financières ;
e) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou passeport ou permis de conduire) identifiant les mandataires et les bénéficiaires effectifs ;
f) un (1) document prouvant l'adresse des mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, etc.).

Autres entreprises commerciales

a) copies du certificat de patente, de la carte d'immatriculation fiscale et de la carte d'identité professionnelle ;
b) un (1) document du ou des propriétaires adressé aux personnes habilitées à faire des transactions et opérations financières;
c) un (1) document officiel original en cours de validité et comportant une photographie (carte d'identification nationale ou permis de conduire ou passeport) identifiant les mandataires et les bénéficiaires effectifs ;
d) un (1) document prouvant l'adresse des mandataires (facture d'électricité ou facture d'eau ou facture d'internet ou avis d'imposition ou relevé bancaire, géolocalisation par l'institution financière, photographie des lieux prises par l'institution financière, etc.).

Œuvres caritatives, clubs, associations, églises et partis politiques

Dans le cas de telles entités, les institutions financières doivent vérifier l'identité d'au moins deux (2) signataires, en sus de l'entité elle-même. Les responsables à identifier doivent être les personnes qui contrôlent totalement ou partiellement les actifs, c'est-à-dire les membres de l'organe ou comité exécutif, le président, un administrateur, le trésorier et tous les signataires autorisés.

En ce qui a trait aux partis politiques, la copie des pièces suivantes doit être réclamée :

a) l'enregistrement au Ministère de la Justice et de la Sécurité Publique ;
b) l'acte constitutif ;
c) les documents d'identification du représentant officiel ou de ceux mandatés par le Comité de direction.

Fonds de retraite

Le fiduciaire ou tout autre dirigeant en charge des relations avec l'institution financière (administrateur, gérant, signataire autorisé) doit être considéré comme le responsable et son identité doit être vérifiée par l'institution financière.

Autres

Pour tout autre type d'entités non mentionnées dans la présente circulaire, les institutions financières sont tenues de prendre les mesures adéquates aux fins d'établir l'identité du client et des bénéficiaires effectifs et à n'accepter de clients qu'à l'issue de cette procédure.

En ce qui a trait aux institutions financières non bancaires, les banques doivent s'assurer qu'elles sont agréées par la BRH (copie autorisation de la BRH ou vérification du site internet de la BRH).

4. *Sociétés en formation*

Pour les sociétés en formation (sociétés, fondations, ONG), les copies des documents notariés de constitution (acte de fondation, statut, assemblée constitutive) et tout document prouvant le processus d'enregistrement de la nouvelle entité (facture des Presses Nationales, correspondances, etc.) sont acceptables. Les institutions financières s'assurent, dans des délais raisonnables, de compléter le dossier d'ouverture de compte et s'efforcent de vérifier l'identité des mandataires de la société en formation.

5. *Des comptes ouverts à distance par les banques, les CEC et les IMF*

Lorsqu'un compte est ouvert par voie électronique, l'envoi de tous les documents doit être fait par courrier recommandé avec accusé de réception dans les cinq (5) jours ouvrables, suivant la date d'ouverture du compte. Cet accusé doit être signé en personne par le titulaire du compte. Les copies des documents d'identification doivent être certifiées conformes aux

originaux par une autorité mandatée à cette fin (notaire, autorité consulaire, etc.). Lorsqu'il s'agit d'une personne morale ou d'une construction juridique, tous les documents doivent être traduits en français et notariés, le cas échéant.

ANNEXE II

FOURNISSEURS DE SERVICES DE PAIEMENT ÉLECTRONIQUE

EXIGENCES D'IDENTIFICATION ET DE VÉRIFICATION DE LA CLIENTÈLE À FAIBLE RISQUE : Vigilance simplifiée

PERSONNES PHYSIQUES **Transactions de dépôts et retraits en espèces ou cash : 15 000 Gdes au maximum par mois**
1. Obtenir les informations suivantes concernant le client : • Patronyme légal et autres noms utilisés ; • Adresse ; • Date et lieu de naissance ; • Nationalité. • Données biométriques du client • Capture de photo 2. Vérifier les noms par rapport aux listes de personnes et d'entités désignées
MICRO-ENTREPRISES INFORMELLES
Transactions de dépôts et retraits en espèces ou cash : 50 000 Gdes au maximum par mois
1. Obtenir les informations suivantes concernant le client : • Nom de la microentreprise et/ou nom du (des) propriétaire(s) de la microentreprise ; • Adresse de la microenterprise ; • Nature de l'activité et chiffre d'affaires ; • Source des fonds. 2. Obtenir un (1) document d'identité national valide pour chaque personne physique /propriétaire/associé/ bénéficiaire effectif afin de vérifier la ressemblance physique, le nom légal, la signature, la date et le lieu de naissance. Si les personnes physiques propriétaires n'ont pas de pièces d'identité nationale valide, le FSP doit obtenir leurs données biométriques et leur capture de photo sur sa plateforme technologique. Si l'entreprise est détenue par un tiers, enregistrer les informations d'identité du ou des bénéficiaires effectifs. 3. Vérifier l'adresse de la microentreprise (géolocalisation, photos, ou tout autre moyen de vérification alternatif.)