Tunis, le 19 septembre 2017

CIRCULAIRE AUX BANQUES ET AUX ETABLISSEMENTS FINANCIERS N°2017-08

Objet : Règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme.

Le Gouverneur de la Banque Centrale de Tunisie :

Vu la loi organique n°2015-26 du 7 août 2015 relative à la lutte contre le terrorisme et à la répression du blanchiment d'argent ; ci-après « la loi organique » ;

Vu la loi n° 2000-93 du 3 novembre 2000 telle que modifiée et complétée par les textes subséquents portant promulgation du code des sociétés commerciales notamment la loi n° 2009-16 du 16 mars 2009 ;

Vu la loi n°2005-51 du 27 juin 2005, relative au transfert électronique de fonds ;

Vu la loi n°2016-35 du 25 avril 2016 portant statut de la Banque Centrale de Tunisie ;

Vu la loi n°2016-48 du 11 juillet 2016 relative aux banques et aux établissements financiers;

Vu le décret-loi n°2011-87 du 24 septembre 2011 organisant les partis politiques ;

Vu le décret-loi n°2011-88 du 24 septembre 2011 relatif aux associations ;

Vu le décret n°2016-1098 du 15 août 2016 fixant l'organisation de la Commission Tunisienne des analyses financières ; ci-après CTAF;

Vu la circulaire n° 2006-01 du 28 mars 2006 relative à la réglementation des opérations d'externalisation ;

Vu la circulaire n°2006-19 du 28 novembre 2006 relative au contrôle interne dans les établissements de crédit ;

Vu la circulaire n°2011-06 du 20 mai 2011 portant renforcement des règles de bonne gouvernance dans les établissements de crédit ;

Vu la circulaire aux intermédiaires agréés n°2012-11 du 8 août 2012 relative à la déclaration à la Banque Centrale de Tunisie des opérations en billets de banque étrangers dont la valeur est égale ou supérieure à 5000 dinars tunisiens ;

Vu la circulaire n°2013-15 du 7 novembre 2013 portant mise en place des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme ;

Vu la décision de la Commission Tunisienne des Analyses Financières n° 2017-01 du 2 mars 2017 portant principes directeurs relatifs à la déclaration des opérations et transactions suspectes ;

Vu la décision de la Commission Tunisienne des Analyses Financières n°2017-02 du 2 mars 2017 portant principes directeurs aux professions financières sur la détection et la déclaration des opérations et transactions suspectes ;

Vu la décision de la Commission Tunisienne des Analyses Financières n° 2017-03 du 2 mars 2017 relative aux bénéficiaires effectifs ;

Vu l'avis n°2017-07 du Comité de Contrôle de la Conformité en date du 19 septembre 2017, tel que prévu par l'article 42 de la loi n°2016-35 du 25 avril 2016 portant statuts de la Banque centrale de Tunisie.

Décide :

Dispositions générales

Article 1er :

La présente circulaire s'applique aux banques et aux établissements financiers agréés dans le cadre de la loi n°2016-48 du 11 juillet 2016, Ci-après désignés par « les établissements assujettis».

Elle fixe les mesures à prendre et les procédures à mettre en place par les établissements assujettis en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

Article 2:

Au sens de la présente circulaire, on entend par:

- « actionnaire ou associé important » : l'actionnaire ou l'associé qui détient 10% ou plus du capital du client personne morale.
- « bénéficiaire effectif » : toute personne physique qui in fine possède ou contrôle de manière effective le client personne morale ou pour le compte de qui l'opération est effectuée sans qu'il soit nécessaire qu'il y ait un pouvoir écrit entre le client et le bénéficiaire effectif.
- « Personnes Politiquement Exposées » : les personnes physiques, qui exercent ou qui ont exercé, en Tunisie ou dans un pays étranger, au cours des deux dernières années précédant l'entrée en relation d'affaires, des hautes fonctions publiques ou des missions représentatives ou politiques et notamment :
  - Chef d'État, Chef du gouvernement ou membre d'un gouvernement,
  - gouverneurs,
  - membre d'un parlement, les élus nationaux et régionaux,
  - membre d'une cour constitutionnelle ou d'une haute juridiction,
  - membre d'une instance constitutionnelle,
  - officier militaire supérieur,
  - Ambassadeur, chargé d'affaires ou consul,
  - membre de collèges ou de conseils d'administration des autorités de contrôle et de régulation ainsi que les premiers responsables de ces autorités membre d'un organe d'administration, de direction ou de contrôle d'une entreprise publique,
  - membre des organes de direction d'une institution internationale créée par traité ou le premier responsable de sa représentation,
  - haut responsable d'un parti politique,
  - membre des organes de direction d'une organisation syndicale ou patronale.

- « banque intermédiaire » : toute banque qui, dans une série ou dans une chaîne de paiement de couverture, reçoit et transmet un virement électronique pour le compte de l'établissement du donneur d'ordre et de l'établissement du bénéficiaire ou une autre banque intermédiaire.
- « virement électronique de fonds » : toute opération effectuée par voie électronique pour le compte d'un donneur d'ordre via une institution financière nationale ou étrangère, y compris les prestataires de transfert de fonds, en vue de mettre des fonds à la disposition d'un bénéficiaire par l'intermédiaire d'une autre institution financière. Le donneur d'ordre et le bénéficiaire peuvent être ou non la même personne.
- «virement par lots» : un ensemble constitué de plusieurs virements de fonds individuels qui sont regroupés en vue de leur transmission.
- «numéro de référence unique d'opération», une combinaison de lettres, de chiffres ou de symboles qui est définie conformément aux protocoles des systèmes de paiement et de règlement ou des systèmes de messagerie utilisés pour effectuer le virement de fonds et qui assure la traçabilité de la transaction jusqu'au donneur d'ordre et au bénéficiaire.
- « donneur d'ordre» : toute personne qui autorise un virement de fonds à partir d'un compte ou, en l'absence de ce compte, donne un ordre de virement de fonds.
- «bénéficiaire» : la personne qui est le destinataire prévu du virement de fonds.
- « virement qualifié » : tout virement transfrontalier de fonds d'un montant supérieur à la contrevaleur de 1000 dinars.
- « banque fictive » : toute banque qui a été constituée et agréée dans un pays où elle n'a pas de présence physique et qui n'est pas affiliée à un groupe financier réglementé soumis à une surveillance consolidée et effective. L'expression « présence physique » désigne la présence d'une direction et d'un pouvoir de décision dans un pays. La simple présence d'un agent local ou de personnel subalterne ne constitue pas une présence physique.

Cette définition ne s'applique pas à la banque qui ne dispose pas de siège fixe dès lors qu'elle est rattachée à une banque dûment agréée qui dispose d'une présence physique et qui est soumise à un contrôle effectif.

- « opération ou transaction inhabituelle » : toute opération ou transaction qui revêt un caractère complexe ou qui porte sur un montant anormalement élevé.

- « Opération suspecte » : toute opération :

  - qui paraît sans rapport avec la nature de l'activité du client.
  - dont les documents ou informations faisant apparaître sa finalité n'ont pas été produits, et
  - qui ne revêt aucune justification économique ou licite apparente.

Titre I : Des mesures de vigilance et des diligences à l'égard des clients et des opérations

Chapitre I : Mesures de vigilance générale

Article 3:

Outre les diligences prévues par la décision de la CTAF n°2017-02, les établissements assujettis doivent accomplir les diligences et observer les mesures de vigilance prévues par la présente circulaire.

Article 4 :

Les établissements assujettis doivent prendre des mesures appropriées pour identifier, évaluer et comprendre les risques de blanchiment d'argent et de financement du terrorisme auxquels ils sont exposés, en tenant compte des facteurs de risques tels que le profil des clients, les pays ou les zones géographiques, les produits, les services, les transactions ou les canaux de distribution.

Les établissements assujettis doivent:

- documenter leurs évaluations des risques ;
- envisager tous les facteurs de risques pertinents avant de déterminer le niveau de risque global et le niveau et le type de mesures appropriées à appliquer pour atténuer

ces risques notamment le calibrage du niveau de vigilance par rapport au profil de risque ; et

- tenir à jour ces évaluations.

L'établissement assujetti peut, pour le besoin de l'identification des risques de blanchiment d'argent et de financement du terrorisme, s'appuyer sur des données précises relatives à son activité ainsi que sur des informations émanant de l'évaluation nationale des risques et des rapports publiés par les organisations internationales.

Les résultats de l'évaluation des risques doivent être consignés dans un rapport appelé « Rapport d'évaluation des risques de blanchiment d'argent et de financement du terrorisme de l'établissement assujetti ». Ce rapport doit décliner la matrice des risques par pays, par zone géographique, par type de client, par type de produits et par canal de distribution.

Article 5 :

Les établissements assujettis doivent, dès l'entrée en relation d'affaires avec un client et/ou, le cas échéant, son mandataire, vérifier son identité et le domaine de son activité ainsi que son environnement bancaire et financier.

Ils doivent procéder à un entretien lors du premier contact dont une fiche d'identification de client « KYC » visée par une personne habilitée doit être versée au dossier du client, permettant:

- d'identifier juridiquement la personne ;
- d'avoir une compréhension claire des activités, des revenus et du patrimoine du titulaire du compte ;
- d'obtenir, lorsque le client est une personne morale, toute indication sur son courant d'affaires, par la communication, entre autres, des états financiers récents ; et
- de comprendre et d'obtenir des informations sur l'objet et la nature envisagée de la relation.

À cet effet, les éléments d'information susceptibles d'être recueillis au titre de la connaissance de l'identité et de la situation juridique, professionnelle, économique et financière du client doivent être contenus dans la fiche d'identification de client « KYC » renfermant les informations minimales conformément à l'annexe 1 de la présente circulaire.

Les éléments d'identification ci-dessus doivent également être recueillis des personnes qui pourraient être amenées à faire fonctionner le compte d'un client en vertu d'une procuration.

Ces informations doivent être justifiées par des documents officiels dont copies doivent être conservées dans le dossier dudit client.

Article 6:

Les établissements assujettis doivent effectuer les diligences relatives à l'identification du client et éventuellement du bénéficiaire de l'opération ou de la transaction et la qualité de celui qui agit pour son compte notamment lorsque:

- le client souhaite ouvrir un compte, quelle que soit sa nature, ou louer un coffre-fort;
- le client effectue des transactions occasionnelles en espèces, dont la valeur est égale ou supérieure à 10.000 dinars ou la contre-valeur de 5.000 dinars en billets de banque étrangers et ce, conformément à la circulaire n°2012-11;
- le client effectue des opérations sous forme de virements électroniques de fonds ;
- il y a suspicion de blanchiment d'argent ou de financement du terrorisme ; et
- il y a des doutes quant à la véracité ou à la pertinence des données d'identification du client précédemment obtenues.

Article 7:

Les établissements assujettis doivent s'assurer de l'identité des associés et actionnaires importants de leurs clients personnes morales et des bénéficiaires effectifs.

Les diligences prévues ci-dessus sont simplifiées lorsque le client est l'une des entités prévues dans l'annexe 2 de la présente circulaire.

Article 8:

Les établissements assujettis doivent observer les diligences prévues par la décision de la CTAF n°2017-3 et prendre toutes les mesures raisonnables conformément à l'article 108 de la

loi organique pour vérifier l'identité du bénéficiaire effectif notamment en consultant des informations ou données pertinentes obtenues de sources fiables.

À cet effet, ils doivent notamment :

- déterminer, pour l'ensemble des clients, si le client agit pour le compte d'une tierce personne et prendre, si c'est le cas, toutes mesures raisonnables pour obtenir des données d'identification suffisantes permettant de vérifier l'identité de cette tierce personne;
- prendre, lorsque le client est une personne morale ou une construction juridique, toutes les mesures raisonnables pour *(a)* comprendre la propriété et la structure de contrôle du client ; *(b)* déterminer qui sont les personnes physiques qui en dernier ressort, possèdent ou exercent un contrôle effectif sur le client; et
- s'assurer que le client n'est pas un prête-nom ou une société écran.

Article 9 :

Lorsque les établissements assujettis font recours à des tiers pour s'acquitter de l'obligation de connaissance du client, ils doivent:

- obtenir immédiatement les informations nécessaires concernant les mesures de vigilance relatives à la clientèle
- prendre les mesures adéquates pour s'assurer que le tiers est à même de fournir, sur demande et dans les délais les plus brefs, des copies des données d'identification et d'autres documents pertinents liés aux devoirs de vigilance relatifs à la clientèle;
- s'assurer que le tiers est soumis à une réglementation et une surveillance relative à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme et qu'il a pris des mesures pour respecter les diligences de vigilance relatives à la clientèle et les obligations de conservation des documents; et
- s'assurer que le tiers est une construction juridique dont l'identité est claire et pourrait être facilement identifiable.

Le recours à un tiers n'exonère pas l'établissement assujetti de ses responsabilités en matière d'identification du client et dans tous les cas il doit continuer à assurer les obligations mises à sa charge par le cadre légal et réglementaire régissant l'externalisation.

Lorsqu'un établissement assujetti fait recours à un tiers faisant partie du même groupe financier, les obligations indiquées ci-dessus sont satisfaites dans les circonstances suivantes :

(a) le groupe applique des mesures de vigilance relative à la clientèle et des obligations de conservation des documents, et des programmes de lutte contre le blanchiment de capitaux et le financement du terrorisme;

(b) la mise en œuvre de ces mesures de vigilance relatives à la clientèle, des obligations de conservation des documents ainsi que des programmes de lutte contre le blanchiment de capitaux et le financement du terrorisme est contrôlée au niveau du groupe par une autorité compétente;

c) tout risque plus élevé présenté par le pays est atténué de manière satisfaisante par les politiques de Lutte contre le blanchiment d'argent et de financement du terrorisme au niveau du groupe.

Article 10 :

Les établissements assujettis ayant des filiales ou des succursales, installées à l'étranger doivent veiller à ce que ces dernières se prémunissent, sous des formes appropriées, contre le risque d'être utilisées à des fins de blanchiment d'argent et de financement du terrorisme et qu'elles soient dotées d'un dispositif de vigilance au moins équivalent à celui prévu par la présente circulaire.

Ces filiales et succursales doivent communiquer à la maison mère le cas échéant les dispositifs locaux applicables dans les pays d'accueil qui s'opposent à la mise en œuvre de tout ou partie des exigences prévues par la présente circulaire.

Lorsque les obligations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme du pays d'accueil sont moins contraignantes que celles en vigueur en Tunisie, les établissements assujettis doivent s'assurer que leurs succursales et filiales appliquent des mesures supplémentaires appropriées afin de gérer adéquatement les risques de blanchiment de capitaux et de financement du terrorisme et doivent en informer la Banque Centrale de Tunisie.

Article 11 :

Les établissements assujettis appartenant à un conglomérat financier doivent mettre en œuvre des programmes de lutte contre le blanchiment de capitaux et le financement du terrorisme adaptés à toutes leurs succursales et filiales dans lesquelles ils détiennent une participation majoritaire. Ces programmes incluent :

(a) des politiques et des procédures de partage des informations requises aux fins du devoir de vigilance relatif à la clientèle et de la gestion du risque de blanchiment d'argent et de financement du terrorisme ;

(b) la mise à disposition d'informations provenant des succursales et filiales relatives aux clients, aux comptes et aux opérations, lorsqu'elles sont nécessaires aux fins de la lutte contre le blanchiment d'argent et le financement du terrorisme, aux fonctions de conformité et d'audit au niveau du groupe ; et

(c) des garanties satisfaisantes en matière de confidentialité et d'utilisation des informations échangées.

Article 12:

Les établissements assujettis doivent exercer une vigilance continue tout au long de la relation d'affaires. Ils doivent s'assurer que les opérations et les avoirs confiés par les personnes avec lesquelles ils sont en relation sont cohérents avec la connaissance qu'ils ont du client, de ses activités commerciales, de son profil de risque et, le cas échant, de l'origine des fonds.

Les établissements assujettis doivent, à cet effet, s'assurer, à travers un contrôle régulier, de la mise à jour et de la pertinence des documents, données ou informations collectées lors de l'accomplissement du devoir de vigilance relatif à la connaissance de la clientèle.

Article 13 :

Les opérations non cohérentes avec les éléments de connaissance du client prévus par l'article 12 de la présente circulaire doivent faire l'objet d'un examen attentif et le cas échéant d'une

demande de renseignements complémentaires auprès du client pour s'assurer qu'elles ne sont pas suspectes au sens de la présente circulaire.

Chapitre II: Mesures de vigilance renforcée

Article 14:

Les établissements assujettis doivent, lorsqu'ils concluent des conventions avec des correspondants bancaires transfrontaliers et autres relations similaires, notamment celles établies pour opérer des transactions de valeurs mobilières ou de virement électronique de fonds que ce soit pour leur propre compte à l'étranger ou pour le compte de leur client:

- s'assurer que le correspondant est agréé et est soumis au contrôle des autorités compétentes de son pays d'origine ou du pays où il est établi ;
- recueillir, sur l'établissement cocontractant, des informations suffisantes pour connaitre la nature de ses activités et pour apprécier, sur la base d'informations accessibles au public et exploitables, sa réputation et la qualité de la surveillance dont il fait l'objet ;
- évaluer le dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme mis en place par l'établissement y compris au moyen d'un questionnaire dont modèle est joint en annexe 3 à la présente circulaire ;
- s'assurer que la décision de nouer une relation d'affaires avec l'établissement cocontractant est prise par le conseil d'administration ou le directoire ou toute personne habilitée à cet effet ;
- avoir l'assurance, en ce qui concerne les comptes «de passage» que le correspondant applique des mesures de vigilance aux clients ayant un accès direct aux comptes de la banque correspondante et que le correspondant est en mesure de fournir les informations pertinentes s'y rapportant à la demande ; et
- fixer, par écrit, les obligations respectives des deux parties.

Article 15:

Les établissements assujettis doivent apporter une vigilance renforcée pour l'identification des clients ne résidant pas en Tunisie. Ils doivent exiger, par exemple, une lettre de référence délivrée par sa banque dans son pays de résidence.

Article 16:

Les établissements assujettis doivent, en sus des mesures prévues par le chapitre I du titre I, apporter une vigilance renforcée pour leurs relations avec les personnes politiquement exposées.

À cet effet, ils doivent:

a) effectuer les diligences nécessaires permettant de déterminer si leur client est l'une des personnes visées par l'alinéa premier du présent article;

b) obtenir l'autorisation de nouer ou de poursuivre selon le cas une relation d'affaires avec une telle personne, du conseil d'administration ou du directoire ou de toute personne habilitée à cet effet;

c) prendre des mesures raisonnables pour comprendre l'origine du patrimoine de la relation; et

d) assurer une surveillance renforcée et continue de cette relation.

Ces mêmes dispositions s'appliquent aux proches des personnes visées au paragraphe premier du présent article ainsi qu'aux personnes ayant des rapports étroits avec celles-ci.

Sont considérés, comme personnes proches des personnes susvisées, les membres directs de leur famille: les ascendants et descendants, au premier degré ainsi que leurs conjoints.

Est considérée comme personne ayant des rapports avec les personnes susvisées, toute personne physique connue comme entretenant avec celles-ci des liens d'affaires étroits.

Article 17:

Les établissements assujettis doivent soumettre leurs relations d'affaires à une vigilance renforcée lorsqu'elles sont :

- des associations notamment en matière d'identification des personnes agissant en leurs noms et d'analyse des transactions y afférentes,

- des clients présentant un profil de risque élevé dans le cadre du profilage et du filtrage de la clientèle, et

- des clients jugés à risque élevé par référence à l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme.

Article 18 :

Les établissements assujettis doivent appliquer en sus des mesures prévues dans le chapitre I du titre I, pour les clients qui agissent en qualité de donneur d'ordre ou de bénéficiaire des mesures de vigilance renforcée lorsque:

- le client est résident dans des pays signalés, par les communiqués publics du Groupe d'Action Financière (GAFI), comme pays qui n'appliquent pas ou appliquent d'une manière insuffisante les normes internationales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme; et
- l'opération est effectuée aux moyens des nouvelles technologies d'information et de communication.

Article 19 :

Les établissements assujettis sont tenus, dans leurs relations d'affaires et opérations avec des personnes physiques et morales de pays signalés par le GAFI comme pays qui n'appliquent pas ou appliquent d'une manière insuffisante les normes internationales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, d'appliquer des contre-mesures proportionnées aux risques, notamment :

- procéder à la déclaration de soupçon systématique des opérations financières ;
- s'abstenir d'ouvrir des filiales, des succursales ou des bureaux de représentation dans ces pays ;
- limiter les relations d'affaires ou les opérations financières avec les pays identifiés et les personnes dans ces pays ; et

- s’interdire de recourir à des tiers établis dans le pays concerné pour exercer certains éléments du processus de vigilance relative à la clientèle.

Article 20:

Les établissements assujettis doivent mettre en place un dispositif permettant de prévenir les risques inhérents à l’utilisation des nouvelles technologies à des fins de blanchiment d’argent ou de financement du terrorisme. À cet effet, ils doivent se doter de dispositifs de gestion des risques permettant d’identifier et d’évaluer les risques de blanchiment d’argent ou de financement du terrorisme pouvant résulter :

- du développement de nouveaux produits et services, y compris de nouveaux canaux de distribution ; et
- de l’utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants.

L'évaluation des risques visée à l'alinéa premier du présent article, doit avoir lieu avant le lancement de nouveaux produits ou services ou avant l’utilisation de technologies nouvelles ou en développement. Les établissements assujettis doivent prendre les mesures appropriées pour gérer et atténuer ces risques ainsi que les risques spécifiques liés aux relations d’affaires et aux transactions qui n’impliquent pas la présence physique des parties.

Article 21:

Les établissements assujettis doivent accorder une vigilance renforcée à toute opération ou transaction :

- qui paraît sans rapport avec la nature de l’activité du client ;

- dont les documents ou informations faisant apparaître sa finalité n’ont pas été produits ;

- qui ne revêt aucune justification économique ou licite apparente ; et
- revêt un caractère inhabituel.

L’annexe 4 à la présente circulaire établit une typologie indicative d’opérations nécessitant une vigilance renforcée.

Les établissements assujettis doivent examiner le cadre dans lequel les opérations ou transactions nécessitant une vigilance renforcée sont réalisées et doivent consigner les résultats de cet examen par écrit et les mettre à la disposition de la Banque Centrale de Tunisie et des commissaires aux comptes.

Chapitre III : des mesures de vigilance spécifique à l'égard des opérations de virement électronique de fonds

Article 22 :

Les diligences de vigilance prévues par le présent chapitre sont applicables à toutes les opérations de virement électronique de fonds, quelle qu'en soit la monnaie, qui sont émis ou reçus par une banque ou un établissement financier.

Elles ne sont pas toutefois applicables, aux virements:

a) effectués au moyen de cartes de crédit et de débit pour l'achat de biens ou de services tant que le numéro de la carte accompagne l'ensemble des virements découlant de l'opération ;

b) qui constituent des virements de fonds au profit d'une administration publique pour le paiement d'impôts, d'amendes ou d'autres prélèvements ; et

c) pour lesquels le donneur d'ordre et le bénéficiaire sont tous les deux des banques ou/et des établissements financiers agissant pour leur propre compte.

Section I : Les diligences à observer par l'établissement du donneur d'ordre

Article 23:

L'établissement assujetti du donneur d'ordre veille à ce que les virements internationaux qualifiés comportent les informations exactes et complètes suivantes sur le donneur d'ordre:

a) le nom et le prénom du donneur d'ordre;

b) le numéro de compte bancaire du donneur d'ordre dès lors qu'un tel compte est utilisé pour réaliser l'opération, ou un numéro de référence unique d'opération permettant la traçabilité de l'opération ; et

c) l'adresse du donneur d'ordre, son numéro de carte d'identité nationale ou le numéro de passeport pour les non-résidents, leurs dates d'émission et de validité, ainsi que la date et le lieu de naissance.

L'établissement du donneur d'ordre veille à ce que les virements internationaux qualifiés de fonds comportent les informations complètes suivantes sur le bénéficiaire :

a) le nom et le prénom du bénéficiaire; et

b) le numéro de compte bancaire ou postal du bénéficiaire ou en l'absence de compte, un numéro de référence unique d'opération permettant la traçabilité de l'opération.

Les virements internationaux non qualifiés doivent contenir le nom et le prénom du donneur d'ordre et le nom et le prénom du bénéficiaire ainsi que le numéro de compte de chacun d'eux ou le numéro de référence unique de l'opération. Dans ce cas, l'établissement du donneur d'ordre peut ne pas vérifier l'exactitude de ces informations, sauf en cas de soupçon de blanchiment d'argent ou de financement du terrorisme.

Article 24:

L'établissement du donneur d'ordre vérifie avant d'émettre un virement international qualifié, l'exactitude des informations visées à l'article 23 de la présente circulaire sur la base de documents, de données ou de renseignements obtenus d'une source fiable.

La vérification visée au paragraphe premier de cet article est réputée avoir eu lieu lorsque l'identité du donneur d'ordre a été vérifiée conformément aux diligences et aux mesures de vigilance à l'égard des clients et des opérations prévues par la présente circulaire et que les informations obtenues lors de cette vérification ont été conservées conformément à l'article 51 ci-après.

Article 25:

L'établissement du donneur d'ordre doit refuser d'exécuter tout virement international de fonds dont les informations requises ne sont pas complètes ou font défaut.

Article 26 :

Lorsque plusieurs virements électroniques transfrontaliers émanant d'un même donneur d'ordre font l'objet d'une transmission par lot à des bénéficiaires, ils peuvent être dispensés des obligations prévues à l'article 23 de la présente circulaire concernant les informations sur le donneur d'ordre, à condition qu'ils comportent le numéro de compte ou le numéro de référence unique d'opération du donneur d'ordre et que le lot comporte les informations requises et exactes sur le donneur d'ordre, ainsi que des informations complètes sur les bénéficiaires et que le parcours de ces informations puisse être entièrement reconstitué dans le pays de réception.

Article 27:

Les virements nationaux de fonds doivent comporter les informations prévues dans l'article 23 de la présente circulaire à moins que celles-ci puissent être mises à disposition :

a) de l'établissement du bénéficiaire ou de la Banque Centrale de Tunisie par tout autre moyen dans les 3 jours ouvrables à compter de la réception, par l'établissement du donneur d'ordre, de la demande émanant de l'établissement du bénéficiaire ou de la Banque Centrale de Tunisie ; et

b) des autorités judiciaires immédiatement à leurs demandes.

Dans ce cas, l'établissement du donneur d'ordre inclut seulement le numéro de compte ou un numéro de référence unique d'opération permettant de reconstituer le parcours de l'opération jusqu'au donneur d'ordre ou au bénéficiaire.

Section II : Les diligences à observer par les banques intermédiaires

Article 28:

La banque intermédiaire doit s'assurer que toutes les informations sur le donneur d'ordre et le bénéficiaire qui accompagnent un virement électronique y restent attachées.

Lorsque des contraintes d'ordre technique font obstacle à ce que les informations requises sur le donneur d'ordre ou le bénéficiaire contenues dans un virement électronique transfrontalier soient transmises avec le virement électronique correspondant, la banque intermédiaire est tenue de conserver pendant au moins dix ans les informations reçues de l'établissement du donneur d'ordre ou d'une autre banque intermédiaire.

Article 29:

La banque intermédiaire est tenue de mettre en place des procédures appropriées pour détecter si, dans le système de messagerie ou le système de paiement et de règlement utilisé pour effectuer le virement de fonds, les champs devant comporter les informations sur le donneur d'ordre et le bénéficiaire ont été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions de ce système.

Article 30:

La banque intermédiaire doit disposer de politiques et de procédures fondées sur le risque pour décider de l'opportunité d'exécuter ou de suspendre ou de demander des informations complémentaires ou de rejeter les virements de fonds dont les informations requises sur le donneur d'ordre et le bénéficiaire font défaut ou sont incomplètes ou que les champs concernant ces informations n'ont pas été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions du système de messagerie ou du système de paiement.

Article 31:

Lorsqu'un établissement omet de manière répétée de fournir les informations requises sur le donneur d'ordre ou le bénéficiaire, la banque intermédiaire doit prendre les mesures

nécessaires qui peuvent dans un premier temps comporter l'émission d'avertissements et la fixation d'échéances avant soit de rejeter tout nouveau virement de fonds provenant de cet établissement, soit de restreindre sa relation d'affaires avec celui-ci ou d'y mettre fin.

La banque intermédiaire doit déclarer à la Banque Centrale de Tunisie cette omission ainsi que les mesures prises.

Article 32:

La banque intermédiaire apprécie, en fonction des informations manquantes ou incomplètes sur le donneur d'ordre ou sur le bénéficiaire si le virement de fonds, ou toute transaction qui s'y rattache, présente un caractère suspect et doit être déclaré(e) à la CTAF.

Section III : Les diligences à observer par l'établissement du bénéficiaire

Article 33:

L'établissement du bénéficiaire doit appliquer des procédures appropriées pour détecter si, dans le système de messagerie Swift ou dans le système de paiement et de règlement utilisé pour effectuer le virement de fonds, les champs devant contenir les informations sur le donneur d'ordre et le bénéficiaire ont été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions de ce système.

Article 34:

Pour les virements de fonds qualifiés en devises, l'établissement du bénéficiaire doit, pour les transferts effectués en une transaction unique ou en plusieurs transactions qui semblent être liées, vérifier, avant de créditer le compte du bénéficiaire ou de mettre les fonds à sa disposition, et lorsque cela n'a pas été fait précédemment, l'exactitude des informations sur son identité sur la base de documents, de données ou de renseignements obtenus d'une source fiable.

L'établissement du bénéficiaire doit conserver les informations sur le bénéficiaire conformément à l'article 51 de la présente circulaire.

Article 35:

L’établissement du bénéficiaire n'est pas tenu de vérifier l'exactitude des informations sur le bénéficiaire pour les virements de fonds non qualifiés en devises qui ne semblent pas être liés à d'autres transferts de fonds et dont le montant, cumulé avec celui du virement en question, excède la contrevaleur de 1000 dinars , à moins qu’il :

a) effectue le versement des fonds en espèces

b) ait des motifs raisonnables de suspecter des actes de blanchiment d’argent ou de financement du terrorisme.

Article 36 :

L’établissement du bénéficiaire doit disposer de politiques et de procédures fondées sur le risque pour décider de l’opportunité d’exécuter ou de suspendre ou de demander des informations complémentaires ou de rejeter les virements de fonds dont les informations requises sur le donneur d’ordre et le bénéficiaire font défaut ou sont incomplètes ou que les champs concernant ces informations n'ont pas été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions du système de messagerie ou du système de paiement.

Article 37:

L’établissement du bénéficiaire prend des mesures raisonnables pour détecter les virements électroniques transfrontaliers pour lesquels il manque les informations requises sur le donneur d’ordre ou sur le bénéficiaire notamment au moyen d’un contrôle à postériori ou, lorsque cela est possible, d’un contrôle en temps réel.

Lorsqu'un établissement omet de manière répétée de fournir les informations requises sur le donneur d'ordre ou le bénéficiaire, l’établissement du bénéficiaire prend les mesures nécessaires qui peuvent dans un premier temps comporter l'émission d'avertissements et la fixation d'échéances, soit de rejeter tout nouveau virement provenant de cet établissement, soit de restreindre sa relation d'affaires avec celui-ci ou d'y mettre fin.

L’établissement du bénéficiaire déclare à la Banque Centrale de Tunisie cette omission et les mesures prises à cet égard.

Article 38:

L'établissement du bénéficiaire doit décider, en fonction des informations manquantes ou incomplètes, de l'obligation de déclarer à la CTAF, conformément à l'article 58 de cette circulaire, le virement ou la transaction qui s'y rattache.

Chapitre IV: Des interdictions

Article 39:

Lorsque les établissements assujettis ne parviennent pas à vérifier les données d'identification de la clientèle ou si les informations recueillies sont insuffisantes ou sont manifestement fictives, ils doivent s'abstenir d'ouvrir le compte, de nouer ou de continuer la relation d'affaires ou d'effectuer l'opération ou la transaction et envisager de faire une déclaration de soupçon.

Article 40:

Les établissements assujettis doivent refuser de nouer ou de poursuivre une relation de correspondant bancaire transfrontalier avec une banque fictive.

Article 41:

Les établissements assujettis doivent refuser de nouer des relations avec les organismes financiers étrangers qui autorisent des banques fictives à utiliser des comptes ouverts sur leurs livres.

Article 42:

Les établissements assujettis s'interdisent, en application de l'article 98 de la loi organique, d'apporter toute forme de soutien et de financement direct et indirect à travers des personnes physiques ou des personnes morales aux personnes, organisations ou activités en rapport avec des infractions terroristes et autres activités illicites.

Article 43:

Les établissements assujettis ne doivent ni tenir de comptes anonymes ni de comptes sous des noms fictifs.

Titre II : Dispositif de contrôle interne

Chapitre I : Des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme

Article 44:

Les établissements assujettis doivent se doter d'une organisation, de moyens humains et logistiques et de procédures internes claires et précises en vue d'assurer la bonne application et le respect des dispositions légales et réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

Les procédures visées dans l'alinéa précédent font partie intégrante du système de contrôle interne tel que défini par l'article 3 de la circulaire n°2006-19 et doivent décrire les diligences à accomplir et les règles à suivre notamment en matière:

- d'identification et de connaissance de la clientèle ;
- de constitution et d'actualisation des dossiers de la clientèle ;
- de détermination des délais pour la vérification de l'identité des clients et la mise à jour des informations y afférentes. Ces délais doivent être plus fréquents pour les clients soumis à une vigilance renforcée ;
- d'exécution des opérations de virement électronique de fonds ;
- d'établissement de relations avec les correspondants bancaires transfrontaliers ;
- de surveillance et d'examen des opérations et des transactions inhabituelles dont les résultats doivent être consignés par écrit et mis à la disposition de la Banque Centrale de Tunisie et des commissaires aux comptes ;

- d’analyse des opérations ou des transactions susceptibles de faire l’objet d’une déclaration de soupçon conformément à l’article 125 de la loi organique;
- de conservation de documents ; et
- de constitution et de conservation de bases de données.

Les procédures internes doivent être examinées et validées par le comité d’audit et approuvées par le conseil d’administration ou le conseil de surveillance de l’établissement assujetti.

Article 45:

Le risque de blanchiment d’argent et de financement du terrorisme doit figurer au niveau de la cartographie des risques sur lesquels le comité des risques doit assister le conseil d’administration ou le conseil de surveillance dans la conception et la mise à jour d’une stratégie de gestion appropriée et la fixation des règles de gestion et de contrôle.

Article 46 :

Les établissements assujettis sont tenus de mettre en place des procédures formalisées, claires et rapides pour :

- la subordination du paiement des fonds, à toute personne morale soumise à une restriction pour la réception de virement provenant de l’étranger, à l’autorisation préalable du ministre chargé des finances conformément à l’article 102 de la loi organique et ;

- l’exécution des décisions prises dans le cadre de l’article 103 de la loi organique concernant le gel des biens des personnes ou d’organisations dont le lien avec des crimes terroristes est établi par les instances internationales compétentes.

Article 47:

Les établissements assujettis doivent se doter d’un système d’information permettant:

- le profilage des clients et des comptes ;
- le filtrage en temps réel des clients et des transactions ;
- le monitoring des mouvements sur comptes et la génération des alertes ;
- de disposer de la position de l’ensemble des comptes détenus par un même client;
- de recenser les opérations effectuées par un même client qu’il soit occasionnel ou habituel ; et

- d’identifier les transactions à caractère suspect ou inhabituel.

Les établissements assujettis doivent prendre en compte tout élément de nature à modifier le profil du client.

Article 48 :

Les établissements assujettis doivent instituer, pour chaque catégorie de clients, des règles de détection d’opérations de blanchiment d’argent notamment des seuils au-delà desquels des opérations pourraient être considérées comme inhabituelles ou suspectes. Ces seuils doivent également prendre en compte le risque de fractionnement de montants.

Article 49:

Le système d’information prévu dans l’article 47 de la présente circulaire doit faire l’objet d’un examen périodique de son efficacité en vue de l’adapter en fonction de la nature et de l’évolution de l’activité de l’établissement et de l’environnement légal et réglementaire.

Article 50 :

Les établissements assujettis doivent assurer un contrôle permanent et périodique rigoureux au sens de l’article 7 de la circulaire n°2006-19 sur la bonne application des procédures internes visées dans l’article 44 de la présente circulaire.

Le dispositif de contrôle interne pour la gestion du risque blanchiment d’argent doit être audité selon une périodicité qui tient compte de la nature, du volume et de la complexité des opérations de l’établissement et dans tous les cas au moins une fois tous les 2 ans.

Les termes de référence des missions d’audit du dispositif de contrôle interne pour la gestion du risque de blanchiment d’argent doivent être validés par le comité d’audit.

Les conclusions des missions d’audit doivent être consignées dans un rapport qui doit être validé par le comité d’audit et transmis au Conseil d’Administration ou au Conseil de Surveillance qui prend les mesures nécessaires pour en assurer un suivi rigoureux.

Article 51:

Les établissements assujettis doivent conserver les dossiers de leurs clients permanents ou occasionnels et les pièces se rapportant à leurs identités pendant dix ans au moins à compter de la date de la fin de la relation.

Ils doivent, en outre, conserver les documents et les informations relatifs aux opérations et transactions effectuées par leurs soins sur support électronique et/ou sur support papier pendant au moins 10 ans à compter de la date de leur réalisation, compte tenu de la possibilité de leur consultation par les autorités compétentes.

Article 52:

L'organisation de la conservation des documents doit notamment permettre de reconstituer toutes les transactions et de communiquer dans les délais requis, les informations demandées par toute autorité habilitée.

Article 53:

Les établissements assujettis doivent définir les règles de déontologie et de professionnalisme en matière de déclaration de soupçon notamment celles relatives à l'obligation de confidentialité.

Ces règles font partie intégrante du Code déontologique prévu par l'article 6 de la circulaire n°2011-06 relative au renforcement des règles de bonne gouvernance dans les établissements de crédit.

Article 54:

Les commissaires aux comptes des établissements sont tenus d'évaluer le dispositif de contrôle interne pour la gestion du risque blanchiment d'argent prévu par la législation et la réglementation en vigueur.

Leurs conclusions doivent être consignées dans leurs rapports adressés à la Banque Centrale de Tunisie et doivent comporter, notamment:

- une appréciation de la politique de gestion du risque de blanchiment d'argent mise en place ; et
- une évaluation du dispositif de contrôle interne pour la gestion du risque de blanchiment d'argent notamment en matière de son efficacité et de son adéquation

avec le degré d'exposition de l'établissement à ce risque en rapport avec la nature, le volume et la complexité de son activité.

Article 55:

Les procédures internes relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme, prévues par l'article 44 de la présente circulaire, doivent être portées à la connaissance du personnel en contact avec la clientèle ainsi que tout le personnel concerné.

Article 56:

Les établissements assujettis doivent mettre en place un programme de formation continue au profit des employés comprenant des informations sur les techniques , méthodes et tendances en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Cette formation doit porter sur tous les aspects de la réglementation en la matière et notamment les obligations relatives au devoir de vigilance à l'égard des clients et des opérations et de déclaration des opérations et des transactions suspectes.

Chapitre II: De la déclaration de soupçon

Article 57:

Le responsable désigné en qualité de correspondant de la CTAF selon les dispositions de l'article 13 de la décision de la CTAF n°2017-2 ainsi que son suppléant doivent faire partie de l'organe permanent de contrôle de la conformité.

Les agents chargés de l'examen des opérations ou transactions inhabituelles ou suspectes relevant du contrôle de la conformité doivent avoir des qualifications professionnelles appropriées. Au moins un de ces agents doit avoir obtenu une attestation diplômante en matière de lutte anti blanchiment d'argent et financement de terrorisme.

Article 58:

Les établissements assujettis doivent veiller à déclarer les opérations et les transactions suspectes conformément au modèle prévu par la décision de la CTAF n°2017-01 du 2 mars 2017.

Ils sont tenus, également, de déclarer toute tentative d'effectuer lesdites opérations ou transactions.

L'obligation de déclaration s'applique, également, même après la réalisation de l'opération ou de la transaction, lorsque de nouvelles informations sont susceptibles de relier, directement ou indirectement, ladite opération ou transaction à des fonds provenant d'actes illicites qualifiés par la loi de délit ou de crime, ou au financement de personnes ou d'organisations ou d'activités en rapport avec des infractions terroristes.

Chapitre III : De l'information de la Banque Centrale de Tunisie

Article 59:

Les établissements assujettis doivent adresser à la Banque Centrale de Tunisie (Direction Générale de la Supervision Bancaire) au plus tard, un mois après la clôture de chaque exercice, un document conforme à l'annexe 5 de la présente circulaire qui indique :

- le nombre total des déclarations effectuées à la CTAF au cours de l'exercice clôturé ; et
- le montant total des opérations déclarées au cours de l'exercice clôturé réparti par nature d'opération et par catégorie de clientèle (personnes physiques et personnes morales)

Article 60:

Les établissements assujettis incluent dans le rapport de contrôle interne, qu'ils sont tenus d'adresser à la Banque Centrale de Tunisie conformément à l'article 50 de la circulaire n°2006-19, un chapitre consacré à la description des dispositifs de vigilance mis en place et des activités de contrôle effectuées en la matière.

Le rapport d'évaluation des risques de blanchiment d'argent et de financement de terrorisme visé dans l'article 4 du titre premier de la présente circulaire doit être communiqué à la Banque Centrale de Tunisie avant fin septembre 2018. Toute mise à jour de ce rapport doit également être communiquée à la Banque Centrale de Tunisie.

Article 61:

Tout manquement aux obligations prévues par la présente circulaire expose l'établissement contrevenant aux sanctions disciplinaires prévues par la loi n°2016-48 relative aux banques et aux établissements financiers.

Article 62 :

Les établissements assujettis disposent d'un délai de 6 mois pour se conformer aux dispositions du chapitre III du titre I de la présente circulaire.

Article 63:

La présente circulaire abroge et remplace la circulaire n°2013-15 du 7 novembre 2013 relative à la mise en place des règles de contrôle interne pour la gestion du risque du blanchiment d'argent et de financement du terrorisme.

Le Gouverneur

Chedly Ayari