



**GUIDE**  
**relatif à la lutte contre le Blanchiment d'argent,**  
**le financement du terrorisme et la prolifération**  
**des armes destiné aux intermédiaires en**  
**bourse et aux sociétés de gestion des**  
**portefeuilles de valeurs**  
**mobilières pour le compte de tiers**

**Avril 2018**

## **PREAMBULE**

### **Références légales du Guide**

- Loi organique n°2015-26 du 7 août 2015 relative à la lutte contre le terrorisme et à la répression du blanchiment d'argent ;
- Décret gouvernemental n° 2018-1 du 4 janvier 2018, portant sur les procédures de mise en œuvre des résolutions prises par les instances onusiennes compétentes liées à la répression du financement du terrorisme ;
- Arrêté du ministre des finances du 1<sup>er</sup> mars 2016, portant fixation des montants prévus aux articles 100, 107, 108, 114 et 140 de loi n° 2015-26 du 7 août 2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent.
- Règlement du Conseil du Marché Financier relatif aux mesures pratiques pour la répression du blanchiment d'argent, la lutte contre le financement du terrorisme et la prolifération tel que visé par l'arrêté de la Ministre des finances en date du 19 janvier 2017 et modifié par l'arrêté du Ministre des finances en date du 6 mars 2018.
- Décisions de la Commission tunisienne des analyses financières n°2017-1, 2017-2 et 2017-3 du 2 mars 2017.

### **Quel est l'objectif du présent guide ?**

Le présent guide a pour objectif de sensibiliser les professionnels au problème que représente le blanchiment d'argent et le financement du terrorisme et de les guider dans le processus de mise en place des mesures pratiques permettant la lutte contre ces deux formes de criminalité financière et ce, conformément aux dispositions législatives et réglementaires régissant la matière.

Le guide présente également les mesures pratiques relatives à la lutte contre la prolifération et le financement de la prolifération d'armes de destruction massive.

### **Quels sont les établissements concernés par ce guide ?**

- Les intermédiaires en bourse ;
- Les sociétés de gestion des portefeuilles de valeurs mobilières pour le compte de tiers.

### **Définition légale du blanchiment d'argent (article 92 de la loi organique n° 2015-26) :**

- Tout acte intentionnel qui vise par tout moyen à la justification mensongère de l'origine illicite des biens meubles ou immeubles ou des revenus provenant directement ou indirectement de tout crime ou délit passible d'une peine d'emprisonnement de trois ans ou plus ainsi que tout délit sanctionné en vertu du code des douanes.

- Tout acte intentionnel ayant pour but le placement, le dépôt, la dissimulation, le camouflage, l'administration, l'intégration ou la conservation du produit provenant directement ou indirectement des infractions susmentionnées ainsi que la tentative, la complicité, l'incitation, la facilitation, ou l'apport de concours à le commettre.
- L'infraction de blanchiment d'argent est indépendante de l'infraction principale quant à sa constitution. Elle est prouvée par l'existence de présomptions et de preuves suffisantes sur l'origine illégale des biens objet de blanchiment.
- Les dispositions des alinéas précédents sont applicables même si l'infraction dont provient l'argent objet du blanchiment n'a pas été commise sur le territoire tunisien.

#### **Définition légale du financement du terrorisme (article 98 de la loi organique n°2015-26):**

- Toutes formes de soutien et de financement de personnes ou organisations ou activités en rapport avec les infractions terroristes prévues par la loi n°2015-26 et autres activités illégales, qu'elles leur soient accordées de manière directe ou indirecte, à travers des personnes physiques ou morales, quelqu'en soit la forme ou l'objet, même si le but qu'elles poursuivent est à caractère non lucratif.

#### **Qu'est-ce que le blanchiment d'argent en pratique ?**

Le blanchiment d'argent est le fait de dissimuler la provenance des fonds illicites en conférant une assise juridique à cette source illégitime dont proviennent ces fonds afin qu'ils apparaissent in fine comme ayant été acquis de façon légale et qu'ils ne soient pas soumis aux lois incriminant les revenus provenant des activités délictueuses ou criminelles.

Les techniques de blanchiment d'argent se déroulent généralement en trois étapes :

- **Le placement**, qui consiste à introduire les fonds illégaux dans le système financier soit par un transfert physique ou électronique.
- **La dispersion (ou empilage)**, qui consiste à dissimuler la source illégitime des fonds en créant un enchevêtrement d'opérations financières complexes dans le but de brouiller la piste de vérification. Par exemple la dispersion des fonds dans de nombreux investissements ou leur transfert entre plusieurs succursales d'une même institution financière ou encore entre plusieurs institutions dans divers pays.
- **L'intégration**, qui consiste à réintroduire les fonds dont l'origine a été dissimulée dans des activités économiques légitimes (ex le fait de rendre liquides certains actifs non monétaires tels que les valeurs mobilières) afin de donner aux fonds une apparence légitime.

Ces trois étapes se retrouvent également dans les schémas de financement du terrorisme, excepté le fait que l'étape 3 (l'intégration) implique dans ce cas la distribution des fonds aux terroristes et aux organisations qui les soutiennent, alors que dans le cas du blanchiment d'argent, au contraire – l'intégration des fonds illégaux s'opère dans des activités économiques légitimes.

## DISPOSITIONS DU GUIDE

### Chapitre préliminaire - Définitions

Dans le cadre du présent manuel, l'on entend par :

#### 1° les établissements concernés:

- Les intermédiaires en bourse ;
- Les sociétés de gestion des portefeuilles de valeurs mobilières pour le compte de tiers.

**2° Client :** le client des établissements qu'il soit habituel ou occasionnel, personne physique ou entité morale. Est considéré comme client occasionnel, toute personne qui s'adresse aux établissements dans le but de préparer ou de réaliser une transaction ou une opération ponctuelle. Est considérée comme une transaction ou une opération ponctuelle, celle qui ne donne pas lieu à l'établissement d'une convention d'ouverture de compte ou de gestion.

**3° Entité morale:** toute entité dotée de ressources propres et d'un patrimoine autonome distinct de celui de ses membres ou de ses associés, et ce, même si la personnalité morale ne lui a pas été attribuée en vertu d'un texte spécial.

**4° Sources fiables et indépendantes :** autorités officielles centrale ou locales ou établissements financiers établis dans un pays appliquant de manière suffisante les normes internationales de répression du blanchiment d'argent et de lutte contre le financement du terrorisme.

**5° Transfert électronique :** toute opération de transfert de fonds par voie électronique au sens de la loi n°2005-51 du 27 juin 2005 relative au transfert électronique de fonds.

**6° Le groupe d'action financière :** un organisme intergouvernemental ayant notamment pour objectifs l'élaboration de normes et la promotion de politiques relatives à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme.

**7° CTAF :** la Commission tunisienne des analyses financières.

**8° Personne ou entité désignée :** toute personne physique ou morale ou entité désignée pour l'application de sanctions financières ciblées liées au financement de la prolifération d'armes de destruction massives en vertu des résolutions du Conseil de Sécurité des Nations Unies et figurant sur les listes arrêtées par l'autorité nationale compétente ayant autorité légale.

**9° Sanctions financières ciblées :** ce terme désigne à la fois le gel des fonds et autres biens ainsi que les interdictions visant à empêcher des fonds et autres biens d'être mis, directement ou indirectement, à la disposition d'une personne ou entité désignée ou à son profit.

**10° Autorité nationale compétente ayant autorité légale :** la ou les autorités nationales compétentes désignées par la loi et chargées de mettre en œuvre et de faire respecter les sanctions financières ciblées.

## **Chapitre 1. Principes de base de la prévention du blanchiment d'argent et du financement du terrorisme**

L'obligation générale de se prémunir contre le blanchiment d'argent et le financement du terrorisme en exerçant une vigilance constante à l'égard des opérations et transactions conclues au profit des clients se décline en diverses obligations plus détaillées mises à la charge des établissements concernées, notamment :

- l'obligation d'identifier et de vérifier l'identité de leurs clients, cette obligation se prolongeant logiquement par celle d'identifier et de vérifier également l'identité des bénéficiaires effectifs de l'opération ou de la transaction et de mettre à jour les données d'identification;
- l'obligation d'attacher une attention particulière aux opérations et aux transactions inhabituelles ainsi que l'obligation de détecter les opérations et les transactions entachées de soupçons de blanchiment d'argent ou de financement du terrorisme ;
- l'obligation de coopérer activement et utilement avec la Commission tunisienne des analyses financières (CTAF) en lui déclarant toutes les opérations ou transactions suspectes détectées et en répondant à ses demandes d'information relatives aux déclarations ;
- l'obligation de conservation des documents liés à l'identification et aux opérations effectuées.

- Satisfaire à l'ensemble de ces obligations requiert, plus généralement :

- que les établissements concernés disposent d'une organisation et de procédures de contrôle interne adéquates ;
- et que les membres de leur personnel ou les personnes qui les représentent soient adéquatement sensibilisés à l'importance de la lutte contre le blanchiment d'argent et le financement du terrorisme et disposent des connaissances requises pour leur permettre de coopérer de manière constructive à cette lutte notamment via des programmes de formation continue.

## **Chapitre 2. Identification des clients, des mandataires et des bénéficiaires effectifs et vérification de leurs identités:**

- Il faut entendre par «identifier les clients, les mandataires et les bénéficiaires effectifs » : recueillir les données d'identification qui leur sont relatives.

- Il faut entendre par «vérifier l'identité des clients, des mandataires et des bénéficiaires» : confronter ces données d'identification à une source fiable et indépendante d'information (documents officiels) apte à les confirmer ou à les infirmer.

- L'identification et la vérification de l'identité du client, de ses mandataires et des bénéficiaires effectifs doivent être effectuées lorsque :

- ✓ La relation d'affaires est nouée ou
  - ✓ l'opération occasionnelle réalisée est d'une valeur égale ou supérieure à dix milles dinars.
  - ✓ L'opération comprend un virement électronique quel que soit le montant.
  - ✓ Il y a suspicion de blanchiment d'argent ou de financement du terrorisme ou des doutes quant à la véracité ou à la pertinence des données d'identification du client précédemment obtenues.
- **Les établissements concernés doivent dans tous les cas s'abstenir d'ouvrir des comptes anonymes ou sous des noms fictifs.**
- **Ils doivent également s'abstenir de recevoir des fonds en espèces dont la valeur est supérieure ou égale à cinq milles dinars même au moyen de plusieurs versements susceptibles de présenter des liens . Ils doivent également s'abstenir de recevoir des chèques ou des virements bancaires non émis par le client ou son représentant.**

### **Section 1. Les documents servant à l'identification:**

#### **1. Pour les personnes physiques**

- Le nom complet, la date et le lieu de naissance ainsi que la nationalité,
- Le numéro de la carte d'identité ou du passeport, leur date d'émission et de validité,
- L'adresse du lieu de résidence effective comportant le code postal, le numéro de téléphone et le cas échéant l'adresse électronique,
- La profession et son adresse,
- L'objectif de la relation d'affaires et sa nature,
- Un exemplaire de signature.

Les données susvisées sont notamment vérifiées sur la base de la carte d'identité nationale pour les tunisiens et d'une pièce d'identité officielle reconnue par les autorités tunisiennes comportant la photo, l'adresse et l'activité de son titulaire pour les étrangers.

#### **2. Pour les entités morales**

- La date de sa constitution, sa raison sociale ou sa dénomination, sa forme juridique et son objet social,
- Le numéro d'immatriculation au registre du commerce et l'identifiant fiscal,

-Adresse du siège social comportant le code postal, les numéros de téléphone et de fax et l'adresse électronique. Lorsque les activités principales ne sont pas exercées au sein du siège social, il convient d'indiquer l'adresse effective d'exercice de l'activité,

-Répartition du capital,

-Identité de ses dirigeants et des personnes pouvant s'engager en son nom ainsi que les documents prouvant leur capacité à le faire avec l'obligation de recueillir en ce qui les concerne, les données relatives aux personnes physiques susmentionnées,

-Identités et adresses des principaux associés dont la participation au capital de la société s'élève au moins à 40% et des personnes qui la contrôlent lorsqu'il s'agit d'une société ou s'il s'agit d'une entité autre qu'une société, l'identité des constituants et des personnes qui exercent un contrôle effectif ou qui sont les bénéficiaires effectifs avec l'obligation de recueillir en ce qui les concerne, les données relatives aux personnes physiques susmentionnées,

-L'objectif de la relation d'affaires et sa nature.

Les données susvisées sont notamment vérifiées sur la base des statuts, d'un extrait du registre de commerce, d'un acte de constitution et de tout document officiel équivalent ou tout autre document émanant de sources fiables et indépendantes, lorsque l'entité morale est enregistrée à l'étranger.

## **Section 2. Copie des documents officiels :**

- La copie du document officiel que les établissements concernés sont tenus de prendre peut l'être tant sur support papier qu'électronique. Cette alternative s'applique à tous les documents officiels utilisés. Ces copies sont conservées dans un dossier propre à chaque client et leur conformité à l'original est certifiée par l'agent en charge du client.

- Toutefois, les établissements concernés sont encouragés à évoluer rapidement d'un enregistrement des données d'identification des clients par photocopie vers un enregistrement électronique systématique de ces données, dans un environnement adéquatement sécurisé.

## **Section 3. Cas des mandataires :**

- Sans préjudice de l'identification du client, l'identification des personnes agissant à quelque titre que ce soit au nom et pour le compte du client doit être opérée.

- Les établissements concernés prennent en outre connaissance des pouvoirs de représentation de la personne agissant au nom du client et procèdent à leur vérification au moyen de documents susceptibles de faire preuve dont ils prennent copie. Sont notamment visés :

- les représentants légaux de clients incapables ;
- les personnes autorisées à agir au nom des clients en vertu d'un mandat général ou spécial ;
- les personnes autorisées à représenter les clients qui sont des personnes morales, des fonds ou toutes autres structures juridiques dénuées de personnalité juridique dans leurs relations avec l'établissement concerné.

#### **Section 4. Cas des bénéficiaires effectifs:**

- Les établissements concernés, doivent identifier et prendre toutes les mesures raisonnables pour vérifier l'identité de la ou des personnes pour laquelle ou lesquelles la transaction ou l'opération est effectuée notamment en cas de doute sur la question de savoir si les clients visés agissent pour leur propre compte ou en cas de certitude qu'ils n'agissent pas pour leur propre compte.

- A ce titre, les établissements concernés doivent prendre en compte les principes directeurs suivants :

- le bénéficiaire effectif est une personne physique. Il n'est pas nécessairement le bénéficiaire déclaré de l'opération ou la transaction. Il importe de distinguer clairement ces deux notions.
- le bénéficiaire effectif n'est pas nécessairement le client, que ce dernier soit une personne physique, une personne morale ou une construction juridique.
- le bénéficiaire effectif et le bénéficiaire peuvent être, dans certains cas, une seule et même personne, par exemple lorsque le bénéficiaire effectif d'un client donneur d'ordre d'un virement en est aussi le destinataire.
- Une relation d'affaires, une opération ou une transaction, avec un client occasionnel peut dissimuler un ou plusieurs bénéficiaires effectifs.
- Certaines relations d'affaires ou opérations réalisées avec des clients occasionnels, font ressortir que le bénéficiaire et le bénéficiaire effectif ne sont pas distincts.

- Dans tous les cas, est considéré comme bénéficiaire effectif :

- la personne ou les personnes physiques qui en dernier lieu possède/possèdent ou contrôle/ contrôlent le client, que ce dernier soit une personne physique, une personne morale ou une construction juridique.
- la personne physique, en droit ou en fait, pour le compte de laquelle une/des opération(s) est/sont effectuée(s).
- la personne ou les personnes physiques qui exerce /exercent, en dernier lieu un contrôle effectif, de fait ou de droit, sur une personne morale ou une construction juridique.

- Est ou sont considéré(s) comme bénéficiaire(s) effectif(s), lorsque le client est une société :

- la ou les personne(s) physique(s) qui détient/ détiennent, directement ou indirectement, 40% des parts du capital ou des droits de vote de la société et à défaut des parts du capital ou des droits de vote conférant un contrôle effectif sur la société.
- la ou les personne(s) physique(s) qui exerce/exercent, par tout autre moyen, de fait ou de droit, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction ou sur l'assemblée générale ou sur le fonctionnement de la société.

- Est ou sont considéré(s) comme bénéficiaire(s) effectif(s), lorsque le client est une personne morale autre qu'une société (ex. association, fondation ou groupement d'intérêt économique), la ou les personnes physiques qui satisfait/satisfont à l'une des conditions suivantes :



- la ou les personne(s) qui a /ont vocation par l'effet d'un acte juridique les ayant désignées à cette fin, à devenir titulaires de 25% au moins des biens de la personne morale.
- la ou les personne(s) titulaire(s), de fait, de 25% au moins des biens de la personne morale.

En général, les établissements concernés doivent identifier le ou les bénéficiaire(s) effectif(s) parmi la ou les personne(s) physique(s) qui exercerait/exerceraient par tout autre moyen, de fait ou de droit, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction ou sur l'assemblée générale ou sur le fonctionnement de la personne morale.

- Est ou sont considéré(s) comme bénéficiaire(s) effectif(s), dans le cas des patrimoines d'affectation relevant d'un droit étranger tels que les trusts et les fiducies et autres constructions similaires, la ou les personnes physiques qui satisfait/satisfont à l'une des conditions suivantes :

- la ou les personnes qui a /ont vocation par l'effet d'un acte juridique les ayant désignées à cette fin, à devenir titulaires de 25% au moins des biens transférés à un patrimoine d'affectation relevant d'un droit étranger.
- la ou les personnes titulaire(s), de fait, de 25 % au moins des biens d'un patrimoine d'affectation relevant d'un droit étranger.
- la ou les personnes qui appartient/ appartiennent à un groupe dans l'intérêt duquel un patrimoine d'affectation relevant d'un droit étranger a été constitué, lorsque les bénéficiaires personnes physiques ne sont pas encore désignées.

En général, les établissements concernés doivent identifier le ou les bénéficiaire(s) effectif(s) parmi la ou les personne(s) physique(s) qui exercerait/exerceraient par tout autre moyen, de fait ou de droit, un pouvoir de contrôle sur le patrimoine d'affectation relevant d'un droit étranger.

Les banques, les établissements financiers, les avocats, les entreprises d'assurance, les entreprises d'investissement et les experts comptables doivent, lorsqu'ils agissent en qualité de fiduciaire ou de trustee, déclarer leur statut de fiduciaire ou de trustee à l'établissement concerné lors de l'établissement de la relation d'affaires ou de l'exécution d'une opération ou transaction.

Pour la bonne exécution des dispositions ci-dessus, on entend par les termes susmentionnées ce qui suit :

- Patrimoine d'affectation : patrimoine affecté pour la création de la fiducie ou autres constructions juridiques.

- Fiducie ou Trust et constructions juridiques similaires : est l'opération par laquelle un ou plusieurs constituants (settlor) transfère/ transfèrent des biens, des droits ou des sûretés ou un ensemble de biens, de droits ou de sûretés, présents ou futurs, à un ou plusieurs fiduciaires (trustees) qui, les tenant séparés de leur patrimoine propre, agit/agissent dans un but déterminé au profit d'un ou plusieurs bénéficiaires.

Entrent également dans la catégorie de patrimoine d'affectation relevant d'un droit étranger, toutes autres constructions juridiques similaires et qui fonctionnent sur le même modèle telles que « el wakf » ou « el habouss ».

- Le contrat de fiducie ou de trust ou autre construction similaire fait intervenir trois personnes:

\* le constituant/ settlor : une personne physique ou morale qui possède un patrimoine et décide de transférer la propriété d'un ou plusieurs de ses biens dans un but déterminé.

\* le fiduciaire/ trustee : la personne qui reçoit la propriété des biens transférés et qui doit les administrer et les gérer selon la mission qui lui est dévolue par le constituant. Néanmoins, les biens transférés n'entrent pas dans le patrimoine personnel du fiduciaire. Ils constituent un patrimoine appelé « patrimoine d'affectation ». Le fiduciaire ou le trustee peut être une banque, une institution financière, un avocat, une société d'assurance, une société d'investissement ou un expert-comptable.

\* le bénéficiaire/beneficiary : personne physique ou morale au profit de laquelle est réalisé le but de la fiducie. Il peut être le constituant ou le fiduciaire.

#### **Section 5. Mesures d'identification propres à la lutte contre le financement du terrorisme :**

Les établissements concernés doivent prendre les mesures nécessaires pour vérifier, au moment de nouer la relation d'affaires ou de réaliser une transaction ou une opération occasionnelle et par la suite périodiquement, que le client ou le bénéficiaire effectif ne figure pas sur la liste des personnes ou des organisations dont le lien avec des crimes terroristes est établi par les organismes internationaux compétents ou par la commission nationale de lutte contre le terrorisme prévue à l'article 66 de 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.

Ils doivent également procéder au gel des biens appartenant aux personnes ou organisations visées au paragraphe premier du présent article et faire la déclaration y afférente, conformément aux dispositions de l'article 103 de la loi n° n°2015-26 du 7 août 2015 relative à la lutte contre le terrorisme et à la répression du blanchiment d'argent.

#### **Section 6. Mesures d'identification propres à la lutte contre la prolifération et le financement de la prolifération des armes de destruction massive :**

Les établissements concernés doivent prendre les mesures nécessaires pour vérifier, au moment de nouer la relation d'affaires ou de réaliser une transaction ou une opération occasionnelle et par la suite périodiquement, que le client ou le bénéficiaire effectif n'est pas inscrit sur la liste des personnes ou entités faisant l'objet de sanctions financières ciblées relatives à la prévention, la répression et l'interruption de la prolifération des armes de destruction massive et de son financement tel qu'arrêtée par l'autorité nationale compétente ayant autorité légale.

Les établissements concernés doivent également:

- geler, sans délai et sans notification préalable, les fonds et autres biens des personnes et entités désignées. L'obligation de gel doit s'étendre à :

- tous les fonds ou autres biens qui sont possédés ou contrôlés par la personne ou l'entité désignée, et pas seulement ceux susceptibles d'être liés à un acte, un complot ou une menace de prolifération particuliers ;
  - les fonds ou autres biens possédés ou contrôlés intégralement ou conjointement, directement ou indirectement, par des personnes ou entités désignées ;
  - les fonds ou autres biens provenant de ou générés par des fonds ou autres biens possédés ou contrôlés, directement ou indirectement, par des personnes ou entités désignées ;
  - les fonds ou autres biens de personnes physiques ou morales agissant au nom, ou sur instructions des personnes ou entités désignées.
- S'interdire de mettre à la disposition des personnes ou entités désignées les fonds et autres biens gelés sauf autorisation de l'autorité nationale compétente ayant autorité légale,
  - déclarer, à l'autorité nationale compétente ayant autorité légale, tous les fonds ou autres biens gelés et toutes les mesures prises conformément aux interdictions édictées par elle, y compris les tentatives d'opérations.

### **Section 6. Impossibilité d'identifier ou de vérifier l'identité :**

- Lorsque les établissements concernés ne peuvent accomplir leur devoir de vigilance tel qu'énoncé ci-dessus ou si les informations dont ils disposent sont insuffisantes ou qu'elles 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 d'opération suspecte (voir chapitre 4). Cela concerne aussi bien les clients nouveaux que ceux existants.

## **Chapitre 3. Stratégie d'acceptation des clients**

### **Section 1. Principe de base :**

- La stratégie d'acceptation des clients des établissements concernés soumet à un examen particulier et à un pouvoir de décision à un niveau hiérarchique adéquat (direction générale, conseil d'administration ; directoire) l'acceptation des clients susceptibles de présenter des niveaux élevés de risque.
- Les critères de risques se subdivisent en des critères communs, d'une part et des critères propres à chaque établissement concerné, d'autre part.

#### **A. Critères communs de risque**

- Les critères communs révélateurs d'un niveau particulier de risque sont :
  - lorsque les clients sont résidants dans les pays qui n'appliquent pas ou appliquent de façon insuffisante les normes internationales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. (Les personnes résidentes dans un pays ou un

territoire qualifié de pays ou territoire non coopératif par le Groupe d'Action Financière) ;

- lorsque les clients sont des personnes physiques dont l'identification a été opérée à distance notamment à travers l'utilisation de nouvelles technologies.

## **B. Critères de risque définis par chaque établissement concerné**

- Il appartient à chaque établissement concerné de définir, en fonction des caractéristiques des produits et services qu'il offre et de la clientèle à laquelle il s'adresse, des critères conduisant à la mise en œuvre de procédures différenciées d'acceptation pour tenir compte du niveau de risque élevé.

- Peuvent notamment constituer des critères pertinents pour définir des niveaux particuliers de risque :

- le fait que le client est une société de droit étranger dont une part importante du capital est représentée par des actions au porteur susceptibles de changer aisément de propriétaire à l'insu de l'établissement concerné;
- le fait qu'il s'agisse d'un fonds ou d'une autre structure juridique dont une bonne connaissance requiert une analyse plus approfondie ;
- le fait qu'il s'agisse d'un client présentant des caractéristiques inhabituelles pour l'établissement concerné;
- l'importance des valeurs patrimoniales remises...

- Les informations à recueillir doivent permettre tant de sélectionner ceux des clients qui présentent des niveaux particuliers de risque que de documenter de manière adéquate l'examen et la décision de leur acceptation par l'établissement concerné.

## **Section 2. Dispositions propres à des situations ou clients particuliers :**

### **A. Les personnes ayant exercé ou exerçant de hautes fonctions publiques**

- Les établissements concernés doivent disposer de systèmes adéquats de gestion des risques en cas de relation avec des personnes ayant exercé ou exercent de hautes fonctions publiques et avec leurs conjoints, ascendants et descendants jusqu'au premier degré et avec les personnes qui leur sont étroitement associées notamment celles qui entretiennent des liens d'affaires étroits avec elles.

- Dans cette optique la première obligation des établissements concernés consiste à déterminer la méthodologie permettant de déterminer si le client rentre dans cette catégorie particulière et ce, en recourant à des sources d'informations fiables ou en s'appuyant sur les déclarations recueillies auprès du client.

- Les établissements concernés doivent obtenir l'autorisation de leurs dirigeants avant de nouer ou de continuer une relation d'affaires avec ce type de clients, assurer une surveillance renforcée et continue de cette relation et prendre des mesures raisonnables pour identifier l'origine de leurs fonds.

- Sont considérées comme des personnes exposées aux risques en raison de leurs fonctions : les personnes qui exercent ou qui ont exercé, en Tunisie ou dans un pays étranger, jusqu'à l'année précédent l'entrée en relation d'affaires, des hautes fonctions publiques ou des missions représentatives ou politiques et notamment :

- Chef d'Etat, chef de gouvernement ou membre d'un gouvernement,
- Membre d'un parlement,
- Membre d'une cour constitutionnelle, ou d'une haute juridiction dont ses décisions ne sont pas susceptibles de recours,
- Membre d'une instance constitutionnelle,
- Officier militaire supérieur,
- Ambassadeur, chargé d'affaires ou consul,
- Membre des organes de direction des autorités de contrôle et de régulation,
- 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.

## **B. Encadrement des relations d'affaires et des opérations nouées avec des clients identifiés à distance**

- Les établissements concernés doivent prendre les dispositions spécifiques et adéquates pour faire face au risque accru de blanchiment d'argent et de financement du terrorisme qui existe lorsqu'ils nouent des relations d'affaires ou effectuent une transaction avec un client qui n'est pas physiquement présent aux fins de l'identification.

- Les établissements concernés qui nouent des relations d'affaires ou réalisent des opérations occasionnelles avec des clients, personnes physiques, qu'ils ont identifiés à distance mettent en œuvre des procédures qui :

- interdisent de nouer une relation d'affaires ou de réaliser une opération occasionnelle avec un client identifié à distance, lorsqu'il existe des raisons de croire que le client cherche à éviter un contact face-à-face afin de dissimuler plus aisément sa véritable identité, ou lorsqu'ils soupçonnent son intention de procéder à des opérations de blanchiment d'argent ou de financement du terrorisme ;
- imposent, en fonction du risque, des mesures complémentaires visant à corroborer davantage les informations d'identification obtenues ;
- visent à améliorer progressivement la connaissance du client.

- Les mesures à arrêter par chaque établissement concerné doivent être définies en fonction du niveau de risque lié à la procédure d'identification. Une identification à distance en vue de nouer une relation d'affaires, dans le cadre de laquelle des contacts réguliers avec le client seront entretenus, peut être considérée comme moins risquée qu'une identification à distance en vue de réaliser une opération occasionnelle.

- Dans le but de corroborer les données d'identification du client et d'améliorer la connaissance qu'a l'établissement concerné de son client, les mesures spécifiques complémentaires peuvent notamment consister à:

- requérir du client la production de documents complémentaires corroborant son identification ;
- procéder à des recoupements avec les informations pouvant être obtenues auprès de sources fiables et indépendantes ;
- mettre en place une procédure d'identification face-à-face ultérieure dès que cela s'avère possible ;
- exiger que le client indique l'identité de son établissement financier habituel établi dans un pays de la zone GAFI et autorise la collecte directe d'informations auprès de cet établissement ;
- prévoir des envois réguliers de courriers nominatifs à l'adresse du client et à mettre en œuvre un suivi attentif des retours de courrier; etc.

### **C. Établissement de relation avec un correspondant transfrontalier**

- Les établissements concernés peuvent faire exécuter les devoirs de vigilance par un correspondant transfrontalier. L'intervention de ce dernier est soumise aux conditions suivantes :

1° les établissements concernés sont tenus à l'obligation de son identification. A cet effet ils doivent vérifier :

- son agrément ainsi que sa soumission au contrôle de la part des autorités compétentes de son pays d'origine ou du pays où il est établi ;
- la nature de son activité et l'évaluation de sa réputation et l'efficacité du système de contrôle auquel il est soumis dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme ;
- s'il a fait l'objet d'une enquête ou d'une mesure de l'autorité de contrôle ayant trait au blanchiment d'argent ou au financement du terrorisme.

2° le recours au correspondant transfrontalier doit être autorisé par les instances dirigeantes de l'établissement concerné ;

3° les obligations des deux parties doivent être établies par écrit ;

4° le correspondant transfrontalier s'engage préalablement à fournir dans les plus brefs délais à l'établissement concerné les informations d'identification des clients ou des bénéficiaires qu'il introduira et une copie des documents au moyen desquels il aura vérifié leur identité.

- La faculté de faire exécuter par un correspondant transfrontalier les obligations incombant aux établissements concernés notamment en matière d'identification des clients requiert néanmoins que le correspondant ait procédé personnellement à l'identification face-à-face du client, à l'exclusion du cas où il a lui-même procédé à cette identification par le recours à un autre correspondant transfrontalier, et de celui où il a procédé à une identification à distance du client.

- Le recours à un correspondant transfrontalier ne porte pas préjudice à la responsabilité de l'établissement concerné de contrôler que l'identification du client introduit ou du bénéficiaire et la vérification de leur identité ont été complètement et correctement opérées par le correspondant, conformément à la législation qui est applicable à celui-ci, et, au besoin, de procéder lui-même aux compléments nécessaires d'identification et de vérification, voire, le cas échéant, à une nouvelle identification et à une nouvelle vérification de l'identité du client introduit ou du bénéficiaire.

- Les établissements concernés s'abstiennent de nouer ou de poursuivre une relation de correspondant transfrontalier avec un organisme étranger qui s'avère fictif et de nouer des relations avec des institutions étrangères qui autorisent des organismes fictifs à utiliser leurs comptes.

Est considéré comme correspondant étranger fictif, toute banque ou institution financière étrangère ne disposant pas d'un siège social fixe pour y exercer ses activités et qui n'est pas soumise au contrôle d'une autorité de régulation. Cette définition ne s'applique pas aux établissements rattachés à une banque ou à une institution financière agréée et soumise au contrôle d'une autorité de régulation établie dans un pays appliquant de manière suffisante les normes internationales de répression du blanchiment d'argent et de lutte contre le financement du terrorisme.

En ce qui concerne les comptes de passage, l'établissement concerné doit s'assurer que son correspondant a appliqué des mesures de vigilance à ses clients ayant un accès direct aux comptes ouverts sur ses livres et est en mesure de fournir les informations pertinentes s'y rapportant, à sa demande.

#### **D. Recours à un tiers pour l'identification des clients :**

- Les établissements concernés qui recourent à un tiers pour nouer des relations d'affaires ou réaliser des transactions ou des opérations occasionnelles doivent :

- S'assurer qu'il est soumis à une législation et à une surveillance relative à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme,
- Lui préciser par écrit les procédures à mettre en place pour vérifier l'identité des clients conformément aux dispositions du présent règlement et s'assurer de leur respect,
- Obtenir sans délai les données d'identification relatives aux clients,
- S'assurer qu'il est capable de fournir sur demande et dans les plus brefs délais, des copies des documents sur la base desquels a été vérifiée l'identité des clients et les autres documents y afférents.

- Au cas où les établissements concernés recourent à un tiers appartenant au même groupe, ils doivent s'assurer que les entités du groupe appliquent des mesures de vigilance et des

procédures en matière de répression du blanchiment d'argent et de lutte contre le financement du terrorisme qui couvrent le recours à un tiers pour nouer des relations d'affaires ou réaliser des transactions ou des opérations occasionnelles.

- Dans le cas où le recours au tiers donne lieu à l'établissement d'une convention, celle-ci doit mentionner les obligations à la charge du tiers prévues aux tirets de 2 à 4 susmentionnés.

- Lorsque les établissements n'ont pas pu prendre les mesures de vigilance pour s'assurer de la bonne exécution des mesures de prévention, ils doivent s'abstenir de recourir au tiers.

- Dans tous les cas, le recours à un tiers n'exonère pas les établissements concernés de leur responsabilité en matière de respect des dispositions en vigueur relatives à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme et plus particulièrement leur responsabilité quant à la vérification de l'identité des clients.

## **Chapitre 4. Devoirs de vigilance**

### **Section 1. Obligation de mise à jour des données d'identification**

- Le devoir de vigilance inclut celui de vérifier et, le cas échéant, de mettre à jour de manière régulière les données d'identification et les autres informations que les établissements concernés détiennent concernant les clients avec lesquels ils entretiennent une relation d'affaires lorsque des indications leur sont fournies que ces données ne sont plus actuelles.

La mise à jour des données d'identification requiert que les nouvelles données soient vérifiées au moyen de documents officiels et dont il est pris copie sur support papier ou électronique.

- Le délai de mise à jour des informations peut être défini en fonction du risque. Il appartient à chaque établissement concerné de définir des critères adéquats à cet effet, en cohérence avec ceux qui ont été définis dans le cadre de la stratégie d'acceptation des clients.

### **Section 2. Obligation de prêter une attention particulière à certaines opérations**

- Les établissements concernés doivent exercer une vigilance constante à l'égard de la relation d'affaires et assurer un examen attentif des opérations effectuées afin de s'assurer que celles-ci sont cohérentes avec la connaissance qu'ils ont de leur client, de ses activités et de son profil de risque.

**1.-** Dans ce cadre les établissements concernés examinent avec une attention particulière toute opération qu'ils considèrent particulièrement susceptible d'être liée au blanchiment d'argent ou au financement du terrorisme de par sa nature ou de par son caractère inhabituel au regard des activités du client, de par les circonstances qui l'entourent ou de par la qualité des personnes impliquées.

- Constitue notamment une opération ou une transaction inhabituelle celle :

- Revêtant un caractère complexe,
- Portant sur un montant anormalement élevé,
- Dont le but économique ou la licéité n'apparaissent pas manifestement,



- N'apparaissant pas cohérentes avec les données d'identification du client,
- Réalisées par des personnes établies dans des pays qui n'appliquent pas ou appliquent de manière insuffisante les normes internationales en matière de répression du blanchiment d'argent et de lutte contre le financement du terrorisme et qui sont signalés dans les communiqués du groupe d'action financière.

- Les établissements doivent examiner attentivement le cadre dans lequel les transactions ou opérations inhabituelles sont réalisées ainsi que leur nature, et le cas échéant demander des informations supplémentaires concernant la raison de la transaction ou de l'opération et l'origine des fonds des clients, afin de déterminer qu'il ne s'agit pas de transactions ou d'opérations suspectes. Les résultats de l'examen doivent être consignés par écrit dans un registre tenu à cet effet et mis à la disposition du CMF à sa demande.

2.- Les établissements concernés doivent également prendre les mesures nécessaires pour identifier et évaluer les risques de blanchiment d'argent et de financement du terrorisme liés au développement de nouveaux produits et services ou à l'utilisation de nouvelles technologies. Ils doivent le cas échéant mettre à jour les règles et les procédures relatives à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme.

3.- Les établissements concernés doivent exercer une vigilance particulière à l'égard des transactions et des opérations réalisées via des transferts électroniques notamment lorsque :

- L'ordre de transfert électronique est donné par un client occasionnel,
- ou les transferts électroniques sont réalisés par masse dans le cadre de transactions ou d'opérations prévues à l'article 15 du présent règlement.

Les établissements doivent incorporer dans tout transfert électronique et dans les documents s'y rapportant, les informations pertinentes relatives à la transaction ou à l'opération concernée ainsi qu'au client qui a donné l'ordre de transfert et au client qui en est bénéficiaire notamment leur identité complète conformément aux dispositions de l'article 5 du présent règlement et les numéros de comptes.

Dans le cas où les informations suffisantes concernant un transfert électronique ne sont pas disponibles, les établissements doivent décider, en fonction du degré de risque, s'ils doivent s'abstenir d'exécuter le transfert ou de le recevoir.

➤ **Les établissements doivent envisager une vigilance renforcée s'agissant de ce type d'opérations ou transactions.**

On entend par vigilance renforcée, les mesures à prendre lorsque les risques de blanchiment d'argent et de financement du terrorisme sont élevés, et notamment :

- l'obtention d'informations supplémentaires sur le client par exemple (profession, volume des actifs, informations disponibles dans des bases de données publiques, sur internet, ...) et la mise à jour des données d'identification du client et du bénéficiaire effectif.
- l'obtention d'informations supplémentaires sur la nature envisagée de la relation d'affaires.
- l'obtention d'informations sur l'origine des avoirs du client.
- l'obtention d'informations sur les raisons des opérations envisagées ou réalisées.

- l'obtention de l'autorisation de la direction générale ou directoire pour l'entrée en relation d'affaires ou sa continuité.
- la mise en œuvre d'une surveillance renforcée de la relation d'affaires par l'augmentation du nombre et de la fréquence des contrôles et la sélection des schémas d'opérations qui nécessitent un examen plus approfondi.

## **Chapitre 4. Devoirs de détection et de déclaration des opérations ou des transactions suspectes**

### **Section 1. Définition des opérations ou transactions suspectes:**

- Les établissements concernés doivent mettre en place un système interne de détection permettant notamment d'aider à la prise de décision en matière de déclaration des opérations ou transactions susceptibles d'être liées au blanchiment d'argent ou au financement du terrorisme.

- Par opération ou transaction suspecte il faut entendre notamment :

- l'opération ou la transaction qui paraît incohérente et incompatible avec la situation du client telle qu'elle apparaît des données et informations recueillies lors de l'ouverture du compte ou de sa mise à jour;
- l'opération ou la transaction dont les documents ou informations faisant apparaître sa finalité n'ont pas été produits.

Les opérations suspectes répondent à certaines grandes caractéristiques, notamment, à l'évidence, le fait de s'écarter des profils normaux de transactions portées en compte. Les éléments repris ci-après constituent des indices sur le caractère suspect d'opérations ou transactions (la liste n'est pas exhaustive) :

- Des fonds sont retirés immédiatement après avoir été crédités sur un compte.
- Un compte dormant devient subitement actif sans raison apparente.
- La valeur élevée des actifs d'un client ne correspond pas aux informations sur le client ou son activité.
- Un client fournit de fausses informations ou refuse de communiquer à l'établissement concerné les renseignements requis.
- Des mouvements d'espèces fréquents incompatibles avec les informations concernant le client ou son activité y compris de fréquentes opérations en espèces dont les montants unitaires sont à peine inférieurs au seuil réglementaire.
- La clôture d'un compte suivie par l'ouverture de nouveaux comptes sous le même nom ou par des membres de la famille du client.

### **Section 2. Les mesures de surveillance et de détection des opérations ou transactions suspectes:**

- La vigilance à l'égard des relations d'affaires et des opérations s'articule autour d'une surveillance à deux niveaux.

## **A. Surveillance de première ligne**

- La surveillance de première ligne doit être exercée par les salariés de l'établissement concerné qui sont en contact direct avec les clients, dans le but de détecter les opérations suspectes sur la base de la cartographie des risques établie par l'établissement concerné. Cette cartographie doit être mise à jour régulièrement

- Les établissements concernés élaborent un manuel écrit à l'intention de leurs salariés chargés de la surveillance de première ligne précisant les critères appropriés leur permettant de déterminer les opérations suspectes, auxquelles il est requis qu'ils attachent une attention particulière, et qui doivent être consignées par écrit. Le manuel élaboré doit être présenté au responsable de la conformité et du contrôle interne et agréé par les organes de direction.

- L'examen des opérations suspectes inclut, notamment, celui de leur justification économique et de leur légitimité apparente.

- Les établissements concernés précisent également par écrit à l'intention de leurs salariés chargés de la surveillance de première ligne la procédure requise en vue de la transmission des rapports écrits à la personne ou aux personnes responsables de l'obligation de déclaration à la CTAF au sein de la société.

- Les procédures écrites doivent notamment préciser que l'employé doit en cas de détection d'une opération ou transaction suspecte:

- Ne pas alerter le client ;
- Prendre en charge rapidement l'opération ou transaction concernée ;
- Informer immédiatement sa direction ;
- Envoyer à la personne chargée de la déclaration à la CTAF l'ensemble des informations pertinentes concernant l'opération ou la transaction concernée.

- Un respect scrupuleux de cette interdiction de divulgation apparaît capital au regard des objectifs poursuivis au travers de la déclaration. En effet, le secret des déclarations d'opérations suspectes constitue une condition indispensable pour que les auteurs d'opérations de blanchiment de capitaux ou de financement du terrorisme puissent être appréhendés et leurs avoirs saisis par les autorités judiciaires.

- Il importe de souligner qu'une rupture de l'obligation de secret dans le but de permettre à l'auteur de l'opération de blanchiment de capitaux ou de financement du terrorisme de se soustraire aux conséquences de la déclaration effectuée ou à effectuer pourrait, en fonction des circonstances, constituer en outre un acte de complicité de blanchiment de capitaux ou de financement du terrorisme.

## **B. Surveillance de seconde ligne**

- Les établissements concernés complètent la surveillance de première ligne par une surveillance de seconde ligne exercée par un système de surveillance efficace.

- Les établissements concernés doivent instaurer un système de surveillance automatisé, sauf s'ils démontrent que la nature et le volume des opérations à surveiller ne requièrent pas l'automatisation du système de surveillance ;

- De même le système de surveillance doit faire l'objet d'un réexamen périodique de sa pertinence en vue de l'adapter, au besoin, en fonction de l'évolution des activités, ou de la clientèle.

- Le système de surveillance doit :

- couvrir l'intégralité des comptes des clients et de leurs opérations ;
- permettre une détection rapide des opérations suspectes ;
- produire des rapports écrits décrivant les opérations suspectes détectées et ceux des critères sur la base desquels elles sont considérées suspectes. Ces rapports étant transmis à la personne ou aux personnes responsables de l'obligation de déclaration à la CTAF au sein de la société.

- Lorsqu'il y a suspicion de blanchiment d'argent ou de financement du terrorisme, et que la mise en œuvre des mesures de vigilance risquerait d'alerter le client concerné, les établissements concernés peuvent immédiatement faire la déclaration à la CTAF sans appliquer les mesures de vigilance.

### **Section 3. Procédures de déclaration des opérations ou transactions suspectes à la CTAF :**

- Les établissements concernés doivent désigner une ou des personnes chargées d'accomplir l'obligation de déclaration à la CTAF parmi leurs employés ou dirigeants ainsi que leurs suppléants.

- Les établissements concernés doivent communiquer au secrétariat général de la CTAF la décision de désignation du correspondant et de son suppléant avec indication de leur qualité, fonction ainsi que de leurs coordonnées et adresses électroniques.

-Le correspondant et son suppléant doivent assister aux réunions périodiques des correspondants avec la Commission chaque fois qu'ils y sont conviés.

-Le correspondant ou son suppléant doivent fournir, dans les meilleurs délais, à la Commission tous les documents et informations qu'elle demande.

- La ou les personnes ainsi désignées doivent disposer de l'expérience professionnelle, et du niveau hiérarchique au sein de l'établissement concerné qui sont nécessaires à l'exercice effectif et autonome de leurs fonctions.

- La ou les personnes désignées procèdent à l'analyse des opérations et des transactions suspectes et effectuent le cas échéant, la déclaration à la CTAF conformément au modèle prévu par la décision de la CTAF n°2017-1 du 02 mars 2017. Cette obligation de déclaration s'impose également concernant toute tentative desdites opérations ou transactions.

En principe, la transmission de l'information doit être obligatoirement préalable à l'exécution de l'opération ou de la transaction. Dans ce cas, la déclaration doit indiquer le délai dans

lequel l'opération sera exécutée, afin de permettre à la CTAF, si elle l'estime nécessaire en raison de la gravité ou de l'urgence de l'affaire, de faire opposition avant l'expiration de ce délai. L'information peut être également communiquée à la CTAF postérieurement à l'exécution de l'opération ou de la transaction dans ce cas là l'établissement concerné doit dument justifier les raisons de la non déclaration préalable.

- La transmission d'informations complémentaires à la CTAF est effectuée par la ou les personnes désignées.

- La ou les personnes susvisées veillent, d'une manière générale, au respect par l'établissement concerné de l'ensemble de ses obligations de prévention du blanchiment d'argent et du financement du terrorisme. Elles veillent également à la sensibilisation du personnel à ces problématiques

### **Chapitre 5. Adoption de règles en matière de contrôle interne :**

- Les établissements concernés doivent établir des règles de contrôle interne en vue d'évaluer l'efficacité du système instauré. La justification de la fréquence choisie pour réaliser les opérations de contrôle ainsi que les résultats de ces opérations doivent être consignés dans le rapport du responsable de conformité et de contrôle interne et les organes de direction doivent en être informés.

- Ce rapport mentionne le cas échéant, les suspicions de blanchiment d'argent ou de financement du terrorisme, et comprend un jugement sur l'adéquation de l'organisation administrative et des contrôles internes mis en œuvre, et de la collaboration des services de l'établissement concerné à la prévention.

- Il est recommandé notamment que ce rapport contienne :

- un aperçu de la nature, du nombre et du montant des opérations détectées, ainsi que des actions qui ont été entreprises, notamment sous la forme d'une transmission à la CTAF ;
- une analyse des évolutions des méthodes et des moyens spécifiques éventuellement constatés en rapport avec ces pratiques de blanchiment d'argent ou de financement du terrorisme, en ce qui concerne, notamment, le type de clientèle, le type d'opérations, ou tout autre élément pertinent ;
- la communication de tout élément utile concernant le fonctionnement des procédures de contrôle interne, en distinguant notamment la surveillance de première ligne et de seconde ligne, et des procédures de transmission, de centralisation et d'analyse des renseignements, en vue de prévenir, d'identifier et dénoncer les pratiques de blanchiment d'argent ou de financement du terrorisme ;
- la mention des nouvelles instructions et/ou procédures, et des initiatives de formation à la problématique du blanchiment d'argent et du financement du terrorisme à l'attention du personnel, et, le cas échéant, l'évaluation des moyens complémentaires qui sont nécessaires à cet effet.

## **Chapitre 6. Dispositions relatives aux filiales et aux succursales situées à l'étranger**

- Les établissements concernés doivent prendre les diligences nécessaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme en ce qui concerne leurs filiales, les sociétés dont ils détiennent la majorité du capital social ou leurs succursales situées à l'étranger.

- Les établissements concernés doivent imposer aux sociétés dont ils détiennent la majorité du capital social ainsi qu'à leurs filiales et succursales situées à l'étranger de mettre en œuvre des dispositifs de prévention équivalents à ceux qui sont requis par la législation et la réglementation tunisienne, si de tels dispositifs de prévention équivalents ne sont pas déjà mis en œuvre en vertu des exigences légales et réglementaires locales.

- Sont notamment visées :

- les exigences d'identification des clients et des bénéficiaires,
- l'encadrement spécifique des relations d'affaires et des opérations avec les clients identifiés à distance,
- les devoirs de vigilance à l'égard des relations d'affaires et des opérations,
- les obligations de formation et de sensibilisation du personnel,
- et, d'une manière générale, la mise en œuvre d'une organisation administrative et d'un audit interne adéquats.

- Si la législation locale ne permet pas l'application de ces dispositifs dans les sociétés dont ils détiennent la majorité du capital social ou dans leurs filiales et leurs succursales situées à l'étranger, ils doivent en informer le CMF.

## **Chapitre 7. Obligation de formation et de sensibilisation du personnel:**

- Les établissements concernés prennent les mesures appropriées pour sensibiliser leurs employés et leurs représentants aux dispositions de la législation en vigueur en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Ces mesures comprennent la participation de leurs employés et de leurs représentants concernés à des programmes de formation continue afin de les aider à reconnaître les opérations et les faits qui peuvent être liés au blanchiment d'argent et au financement du terrorisme et de les instruire sur la manière de procéder en pareil cas.

- La mise en place des programmes de formation doit être réalisée en concertation avec la CTAF conformément à la décision de la CTAF n° 2017-02 du 2 mars 2017.

- Ces programmes sont destinés aux membres du personnel des établissements concernés et toute personne qui les représente :

- dont les tâches en relation avec les clients ou les opérations les exposent au risque d'être confrontés à des tentatives de blanchiment d'argent ou de financement du terrorisme ;
- ou dont les tâches consistent à développer des procédures ou des outils informatiques ou autres applicables à des activités sensibles du point de vue de ce risque.

- La formation continue du personnel vise notamment :

- à acquérir les connaissances nécessaires pour détecter les opérations suspectes ;

- à acquérir la connaissance des procédures qui est nécessaire pour réagir adéquatement face à de telles opérations ;
- à intégrer adéquatement la problématique de la prévention du blanchiment d'argent et du financement du terrorisme dans les procédures et outils développés pour être appliqués à des activités sensibles du point de vue de ce risque.

- Dès lors, cette formation devrait utilement porter sur :

- les obligations légales et réglementaires en vigueur et applicables à l'établissement concerné;
- l'organisation et les procédures de prévention au sein de l'établissement concerné ;
- l'étude du phénomène de blanchiment d'argent et de financement du terrorisme dans la pratique (définition, facteurs de risques, etc.)

- De même, il est également recommandé aux établissements concernés d'inclure dans leurs procédures de recrutement des membres de leur personnel et de leurs représentants un contrôle approprié lorsque les fonctions qu'ils seront appelés à exercer sont exposées au risque de blanchiment d'argent ou de financement du terrorisme.

### **Chapitre 8. Conservation des documents**

- Les établissements concernés conservent, pendant dix ans au moins à compter de la date de la réalisation de l'opération ou de clôture du compte les registres, livres comptables et autres documents qu'ils détiennent sur support matériel ou électronique aux fins de consultation, le cas échéant, et ce, pour les besoins de traçabilité des différentes phases des transactions ou opérations financières effectuées par leurs soins ou par leur intermédiaire et d'identifier tous les intervenants ou de s'assurer de leur véracité.

### **Chapitre 9. Obligations d'information périodiques à l'égard du CMF**

- Les établissements concernés doivent informer le Conseil du Marché Financier dans un délai d'un mois suivant la fin de chaque semestre du nombre des déclarations de transactions et d'opérations suspectes effectuées à la commission et de leur teneur. Ces informations doivent être consignées dans le rapport du responsable de la conformité et du contrôle interne.

- Les établissements concernés doivent, sans délai, mettre à la disposition du Conseil du Marché Financier sur sa demande :

- Les registres comportant les résultats de l'analyse des transactions et des opérations inhabituelles et des transactions et des opérations suspectes,
- Les programmes de formation de leurs agents en matière de répression du blanchiment d'argent et de lutte contre le financement du terrorisme avec indication de leur teneur, de la date de leur mise en place et de l'identité et des fonctions des agents qui y ont participé.