

الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DES FINANCES
Commission de Supervision des Assurances

وزارة المالية
لجنة الإشراف على التأمينات
الرئيس

Le Président

N°...../CSA/Président.

رقم / ل إ ت / الرئيس.

Instruction n° ⁰¹ du ^{21 NOV. 2024} relative au devoir de vigilance à l'égard de la clientèle en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive.

Article 1er : En application des dispositions du règlement n° 01 du 06 novembre 2024, relatif aux obligations des assujettis en matière d'assurance, au titre de la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive, la présente instruction a pour objet de préciser les mesures de vigilance à l'égard de la clientèle et des opérations que doivent observer les sociétés d'assurance et/ou de réassurance et les courtiers d'assurance, ci- après désignés «assujettis ».

Titre I - Politique d'acceptation de la clientèle et procédures internes

Art. 2. — Les assujettis doivent définir et mettre en œuvre une politique claire d'acceptation de la clientèle qui vise à déterminer les conditions d'établissement, de maintien ou de refus de la relation d'affaires ou d'exécution d'une opération occasionnelle ainsi que des mesures de vigilance appropriées à mettre en œuvre. On entend par opération occasionnelle, toute opération unique ou ponctuelle effectuée par un client qui n'a pas établi de relation d'affaires continue avec l'assujetti.

La politique d'acceptation des clients doit permettre de détailler les catégories de risque qui peuvent être attribuées aux relations d'affaires qu'ils établissent en tenant compte de l'évaluation globale des risques de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive.



destruction massive, ainsi qu'à la taille et la nature de leur activité.

Cette évaluation des risques de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive associés à chaque relation d'affaires, doit permettre l'établissement d'un profil de la relation d'affaires, en vue d'exercer la vigilance constante, et l'allocation efficiente des ressources.

La politique d'acceptation de la clientèle doit permettre de détecter les types de clients susceptibles de présenter un risque élevé de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive afin de les soumettre à un examen approprié et à une décision de la direction générale ou du directoire quant à leur acceptation.

Elle ne doit, cependant, pas être trop restrictive au point de priver les personnes financièrement ou socialement défavorisées de l'accès aux services assurantiels de base.

Art. 3.— Lors de l'évaluation individuelle du risque de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive associée à chaque relation d'affaires ou à une opération occasionnelle, les assujettis doivent prendre en compte l'ensemble des informations relatives aux caractéristiques du client ainsi qu'à l'objet et à la nature de la relation d'affaires ou de l'opération occasionnelle.

Cette évaluation doit notamment inclure les facteurs de risques pertinents comme l'activité du client, la source de ses revenus et de son patrimoine, la nature et l'objet du compte, le pays de résidence, les produits et services utilisés, les activités commerciales, ainsi que d'autres indicateurs de risques axés sur le client afin de déterminer la nature et le niveau des mesures de vigilance appropriées à mettre en œuvre.

Art. 4. — Les assujettis doivent mettre en place des procédures internes pour l'ensemble de leurs activités, qui précisent :

- les modalités de définition du profil de risque de chaque relation d'affaires et les modalités de mise à jour de ce profil selon une approche fondée sur les risques ;
- les mesures de vigilance requises en fonction du profil de risque de chaque relation d'affaires, identifié par l'évaluation mentionnée à l'article 3 ;
- les critères de détection des opérations atypiques ainsi que l'ensemble des diligences requises en vue de soumettre ces opérations à une analyse



appropriée, pour en confirmer ou infirmer le caractère suspect et procéder s'il y a lieu à une déclaration de soupçon auprès de la Cellule de Traitement du Renseignement Financier ;

- les modalités d'information et de déclaration des opérations suspectes à la Cellule de Traitement du Renseignement Financier ;
- les modalités de conservation des informations et documents.

La définition et la mise en œuvre de ces politiques et procédures impliquent un engagement de la direction générale ou du directoire, qui doit exercer un suivi permanent quant à leur saine et harmonieuse implémentation, notamment par le biais de procédures de contrôle interne des risques liés au blanchiment d'argent, au financement du terrorisme et au financement de la prolifération des armes de destruction massive, qui doit en évaluer l'exécution et en rapporter toute déficience, à l'effet d'engager les mesures correctives appropriées pour y remédier.

Lesdites politiques et procédures internes doivent être formalisées par écrit et être suffisamment précises pour permettre leur mise en œuvre opérationnelle. Elles sont régulièrement mises à jour et à la disposition des personnels concernés.

Les assujettis doivent mettre en œuvre des procédures de sélection et garantissant l'embauche des employés, selon des critères de compétence élevés.

Titre II – Mesures de vigilances à l'égard de la clientèle

Art. 5. — Les assujettis doivent prendre les mesures de vigilance à l'égard de leur clientèle :

- a) Ils établissent des relations d'affaires ;
- b) lorsqu'elles réalisent une opération occasionnelle dont le montant est supérieur au seuil fixé par voie réglementaire, que celle-ci soit exécutée en une seule fois ou au moyen de plusieurs opérations entre lesquelles semble exister un lien ;
- c) lorsqu'elles effectuent une opération occasionnelle sous forme de virement électronique supérieure au seuil fixé par voie réglementaire, ou plusieurs opérations qui semblent liées et dont le montant global dépasse le seuil fixé ;
- d) Il existe un soupçon de blanchiment d'argent, de financement du terrorisme ou de financement de la prolifération des armes de destruction massive, quel que soit le niveau minimum stipulé dans les règlements ;



e) Il existe un doute quant à l'exactitude ou l'adéquation des données d'identification du client précédemment obtenues.

Art. 6. — Avant l'entrée en relation d'affaires ou l'exécution d'une opération occasionnelle, les assujettis doivent appliquer les mesures suivantes :

a) identifier et vérifier l'identité des clients (personnes physiques, morales, organisations à but non lucratif), leurs mandataires ainsi que toute personne prétendant agir pour le compte du client, au moyen de documents, données et informations de sources fiables et indépendantes ;

b) identifier le bénéficiaire effectif et prendre des mesures raisonnables pour vérifier son identité, à l'aide d'informations ou données pertinentes obtenues d'une source fiable et indépendantes, de sorte qu'ils aient l'assurance qu'ils savent qui est le bénéficiaire effectif ;

c) établir l'objet et la nature envisagée de la relation d'affaires et de l'opération occasionnelle ;

d) prendre immédiatement les mesures nécessaires pour obtenir, dans les meilleurs délais, tous les renseignements utiles pour une bonne identification du client, dans le cas où les données disponibles sont insuffisantes ;

e) s'assurer de la bonne application des mesures de gel et/ou de saisie de fonds et biens et d'interdiction de mise à disposition ou d'utilisation des fonds ou ressources économiques à l'ensemble de leurs activités. À cet effet, les assujettis mettent en place un dispositif garantissant la consultation et la vérification continues et permanentes de la liste récapitulative des sanctions ainsi que de la liste nationale. Les procédures internes doivent prévoir des mécanismes de détection, immédiatement, sans délais et sans préavis, de toute opération réalisée au bénéfice d'une personne faisant l'objet d'une mesure de gel et/ou de saisie et d'interdiction de mise à disposition ou d'utilisation des fonds et ressources économiques ainsi que les fonds et ressources économiques détenus, appartenant, possédés ou contrôlés par des personnes qui font l'objet desdites mesures ;

f) vérifier et s'assurer de la véracité des données ou des documents remis par les clients lors de l'identification, par tous moyens possibles en cas de soupçon sur leur véracité ;



g) prendre des mesures de vigilance renforcée à l'égard de leur clientèle avant de compléter la transaction ou la demande du client, en cas de soupçon de blanchiment d'argent, de financement du terrorisme ou de financement de la prolifération des armes de destruction massive, ou d'un doute sur l'exactitude, la véracité, ou la pertinence des données d'identification du client précédemment obtenues ;

h) veiller à ce que les documents, données ou informations obtenus dans le cadre des mesures de vigilance soient constamment à jour et appropriés, notamment les clients présentant des risques identifiés plus élevés ;

i) s'abstenir d'ouvrir ou de conserver des comptes anonymes ou numérotés, ou des comptes sous des noms manifestement fictifs.

Lorsque l'assujetti ne peut pas respecter les obligations de vigilance à l'égard de la clientèle visées ci-dessus, ou que les opérations effectuées par le client au cours de la relation d'affaires ne sont pas cohérentes avec la connaissance qu'elle a de ce dernier, elle ne doit pas, selon le cas : ni ouvrir de compte, ni établir de relation d'affaires, ni effectuer l'opération. En outre, l'assujetti doit mettre un terme à la relation d'affaires, clôturer le compte et, le cas échéant, établir et transmettre une déclaration de soupçon.

Titre III - Identification et vérification de l'identité de la clientèle

Art. 7. — Les assujettis doivent déterminer les mesures de vigilance élémentaires pour identifier tous les clients ainsi que des vérifications proportionnées au niveau de risque de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive associé aux clients. Conformément aux dispositions de l'article 7 du règlement n°01 susvisé, lorsque les risques sont plus élevés, les assujettis doivent prévoir des mesures de vigilance renforcées pour les atténuer et les gérer. Lorsqu'il est établi que les risques sont plus faibles, des mesures de vigilances simplifiées peuvent être appliquées conformément aux prescriptions de l'article 15 dudit règlement.

Art. 8. — L'identification de la clientèle intervient avant l'établissement de la relation d'affaires ou l'exécution de l'opération occasionnelle, elle consiste à recueillir sur une base déclarative tous les renseignements relatifs à l'identité et à l'activité du client, permettant à l'assujetti d'établir le profil du client, le fonctionnement envisagé de son compte et déterminer le niveau de risque associé, à l'effet d'adapter le niveau de vigilance à observer.



Art. 9. — Les assujettis sont tenus de déterminer et d'identifier le ou les bénéficiaires effectifs de leurs clients personnes morales.

On entend par le bénéficiaire effectif :

- La ou les personnes physiques qui possèdent ou contrôlent le client, le représentant du client, ou le bénéficiaire des contrats d'assurance-vie.
- La ou les personnes physiques qui détiennent ou exercent le contrôle ultime sur un client, le représentant de ce client, ou le bénéficiaire de contrats d'assurance-vie et/ou d'autres contrats d'assurance liés à des investissements, de manière directe ou indirecte.

Ce terme inclut :

- La ou les personnes physiques qui agissent pour le compte d'une autre personne physique pour laquelle l'opération est réalisée ou avec laquelle une relation commerciale est établie.
- Les personnes qui exercent un contrôle effectif ultime sur des personnes morales ou des constructions juridiques.

En l'absence de bénéficiaires effectifs identifiables selon les critères susmentionnés, le dirigeant principal de l'entité peut être désigné comme bénéficiaire effectif, sous réserve pour l'assujetti de pouvoir justifier les mesures de vérification exhaustives entreprises pour identifier le véritable bénéficiaire effectif.

Dans le cadre de cette identification, l'assujetti doit, de surcroît, analyser les mécanismes de contrôle de manière approfondie, notamment en examinant :

- les décideurs stratégiques capables d'influencer les contrats, accords ou décisions ayant un impact majeur sur les opérations ou la stratégie de la personne morale ;
- les membres du conseil d'administration ou les dirigeants ayant le pouvoir de révoquer ou nommer des membres de direction ;
- les personnes physiques exerçant un contrôle par des liens familiaux ou des relations personnelles étroites ;
- le pouvoir de bloquer les décisions importantes de la personne morale ;
- le droit de percevoir au moins 20 % des actifs lors de la dissolution de la personne morale.

Article 10 : Les sociétés d'assurance, de réassurance et intermédiaires (agent général, courtier) doivent prendre les mesures suivantes, outre les procédures de vigilance requises pour les clients et les bénéficiaires effectifs conformément aux



dispositions du présent chapitre :

- a) Prendre des mesures de vigilance sur les bénéficiaires de contrats d'assurance vie et autres produits d'assurance investissement, dès l'identification ou dénomination de ces bénéficiaires :
1. Obtenir le nom de la personne pour les bénéficiaires des personnes physiques ou morales ou des constructions juridiques spécifiquement désignées nommément ;
 2. Obtenir des informations suffisantes sur les bénéficiaires nommés par des attributs ou des catégories (comme un mari ou enfants au moment où survient l'incident assuré) ou par d'autres moyens comme un testament, pour que les sociétés d'assurance et de réassurance et intermédiaires (agent général, courtier) puissent identifier le bénéficiaire au moment de l'indemnisation ;
 3. Vérification de l'identité des bénéficiaires visés au paragraphe 1 et 2 de cet article, au moment de l'indemnisation.
- b) Considérer le bénéficiaire d'un contrat d'assurance vie comme un facteur de risque associé pour déterminer l'applicabilité des mesures requises de vigilance renforcée.

Et lorsque les entreprises d'assurance, de réassurance et intermédiaires (agent général, courtier) parviennent à considérer le bénéficiaire de l'assurance comme étant une personne morale ou une construction juridique à hauts risques, des procédures de vigilance renforcées nécessaires doivent être appliquées conformément aux dispositions du présent règlement, y compris la prise de mesures adéquates pour identifier le bénéficiaire effectif d'un contrat d'assurance et le vérifier au moment de l'indemnisation.

Les entreprises d'assurance, de réassurance et intermédiaires (agent général, courtier) doivent élaborer et prendre les mesures nécessaires pour déterminer si une personne politiquement exposée est bénéficiaire ou bénéficiaire effectif d'un contrat d'assurance vie. Si tel est le cas, elles doivent procéder comme suit :

- Informer la direction générale avant de verser une indemnisation à partir du produit d'assurance-vie et procéder à un examen attentif de la relation d'affaires ;
- Envisager l'envoi d'une déclaration de soupçon à la Cellule de Traitement du Renseignement Financier.



Art. 11. — Pour lui permettre de dresser le profil de risque du client, l'assujetti doit se doter d'un questionnaire « connaître son client - KYC » renseigné et signé sous la propre responsabilité du client (ou de son représentant légal), dans lequel doivent figurer les données, et renseignements relatifs aux caractéristiques de ce dernier, ainsi que l'objet et la nature de la relation d'affaires envisagée ou de l'opération occasionnelle. Doivent ainsi être recueillis, notamment les renseignements ci-après :

1- Clients personnes physiques (y compris les personnes agissant pour le compte de celui-ci)

- l'identité du client (ses nom et prénoms, date et lieu de naissance) ;
- l'adresse du domicile à jour au moment où les éléments sont recueillis ;
- la nationalité du client ;
- la qualité de résident ou de non-résident ;
- la profession ou les fonctions exercées de manière suffisamment claire et précise et l'affiliation du client (salarié, profession libérale, commerçant, etc....) ;
- la nature et l'objet attendu de la relation d'affaires ;
- les données sur son patrimoine, ses revenus et autres mouvements d'affaires à confier à l'assujetti ainsi que la provenance des fonds, le cas échéant ;
- les modalités d'utilisation du ou des comptes ouverts (virement, encaissement/paiement de chèques, etc...)

2- Clients personnes morales (y compris les organisations à but non lucratif)

- la dénomination, la forme juridique ;
- l'adresse du siège social et l'adresse de l'un des principaux lieux d'activité si celles-ci sont différentes ;
- l'identité des actionnaires ou associés, des membres fondateurs et dirigeants, ainsi que des représentants légaux ou de leurs équivalents en droit étranger de la personne morale et de l'organisation à but non lucratif ;
- les éléments concernant la structure de propriété et de contrôle de la personne morale, permettant d'identifier la personne physique qui exerce, en dernier ressort, un contrôle sur celle-ci ou, à défaut, occupe la position de dirigeant principal ;
- la nature et l'objet attendu de la relation d'affaires ;
- les données sur les revenus et autres mouvements d'affaires à confier à l'assujetti, ainsi que les sources de ces mouvements le cas échéant



Les personnes morales concernées incluent aussi bien celles régies par le droit algérien que les formes juridiques créées à l'étranger, y compris les constructions juridiques et les trusts.

3- Les bénéficiaires effectifs

- les nom et prénoms, date et lieu de naissance ;
- l'adresse du domicile à jour au moment où les éléments sont recueillis ;
- les modalités et l'étendue du contrôle exercé sur la personne morale ;
- la date à laquelle la ou les personnes physiques sont devenues bénéficiaires effectifs de la personne morale.

Les assujettis doivent en sus des éléments d'identification cités ci-dessus, recueillir les pouvoirs et les autorisations accordés respectivement, aux mandataires et aux personnes prétendant agir pour le compte du client. À cet effet, ils collectent un document justifiant leur qualité de représentants.

Les assujettis peuvent, s'ils estiment cela nécessaire, demander toutes informations supplémentaires auprès de leurs clients.

Art. 12. — La vérification de l'identité du client intervient avant l'établissement de la relation d'affaires ou l'exécution de l'opération occasionnelle, elle consiste pour l'assujetti à vérifier l'exactitude des informations collectées sur le client, via le questionnaire « connaître son client - KYC » visé à l'article 11 de la présente instruction, au moyen de document(s) probant(s).

- Pour une personne physique, la vérification de l'identité s'effectue au moyen de ses documents officiels originaux, en cours de validité, et comportant sa photographie. La vérification de son adresse se fait par la présentation d'un document officiel en établissant la preuve. L'assujetti doit conserver une copie des documents officiels originaux présentés par le client ;
- Pour une personne morale, la vérification de l'identité s'effectue par le biais de l'original de ses statuts et de tout document officiel établissant qu'elle est légalement enregistrée ou agréée, comportant sa dénomination, sa forme juridique, l'adresse de son siège social et l'identité de ses actionnaires ou associés et dirigeants, ainsi que de ses représentants légaux ou de leurs équivalents en droit étranger. L'assujetti doit conserver une copie desdits documents ;



- Pour le(s) bénéficiaire(s) effectif(s), la vérification de l'identité s'effectue au moyen de ses documents officiels originaux, en cours de validité, et comportant sa photographie, vérifiée au moyen de sources fiables et indépendantes. En cas de risque élevé, d'autres documents supplémentaires, incluant la preuve de la provenance des fonds ainsi que la documentation certifiée, doivent être également recueillis.

Art. 13. — L'assujetti doit définir de manière précise les documents probants et les sources fiables et indépendantes d'information acceptés aux fins de vérification de l'identité de son client, de toute personne agissant pour celui-ci et des bénéficiaires effectifs. Les sources d'informations auxquelles l'assujetti a recours doivent permettre d'acquérir un niveau élevé de certitude quant à l'identité d'une personne. Sont notamment considérées comme sources fiables et indépendantes : les administrations locales et centrales, les bases de données publiques accessibles, et le centre national du registre du commerce ou toutes autres sources internationales reconnues.

Lorsque l'assujetti constate des divergences entre les informations figurant dans les registres publics, y compris l'absence d'enregistrement de ces informations, et celles obtenues auprès du client ou d'autres sources fiables et indépendantes lors de l'exercice de la vigilance à l'égard de la clientèle, il doit signaler ces divergences aux institutions gestionnaires des registres publics qu'ils aient été constatés, lors de l'entrée en relation d'affaires ou lors de l'actualisation du dossier client.

Art. 14. — Lorsqu'il ressort de l'évaluation individuelle des risques, conduite en application de l'article 3 de la présente instruction, que le risque associé au client ou à l'opération occasionnelle est élevé, ou lorsque le client ou l'opération relève d'une des situations mentionnées à l'article 29 ci-après, l'assujetti doit renforcer sa vigilance. Les mesures de vigilance renforcée susceptibles d'être adoptées comprennent, notamment :

- l'obtention d'informations supplémentaires sur le client, et la mise à jour à une fréquence rapprochée 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 fonds ou l'origine du patrimoine du client. Ces informations peuvent être obtenues en interrogeant le client ou/et en consultant des sources fiables et indépendantes ;
- l'obtention d'informations plus étendues sur les raisons des opérations



- envisagées (destination des fonds, objet des opérations) ;
- l'autorisation de la direction générale ou du directoire pour établir ou maintenir la relation d'affaires ;
 - la réalisation du premier paiement par l'intermédiaire d'un compte ouvert au nom du client auprès d'un autre assujetti à des normes de vigilance similaires ;
 - l'augmentation du nombre et de la fréquence des contrôles et la sélection des types ou modèles d'opérations qui nécessitent un examen plus approfondi.

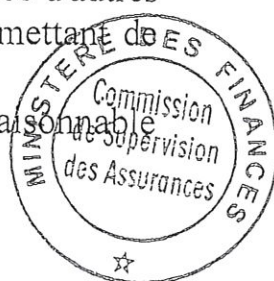
Art. 15. — Lorsqu'il ressort de l'évaluation individuelle des risques conduites en application de l'article 3 de la présente instruction que le risque associé au client ou à l'opération occasionnelle est faible, ou lorsque le client ou l'opération relève de l'une des situations mentionnées à l'article 30 ci-après, et qu'il n'existe pas de soupçon de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive, l'assujetti peut alléger les mesures de vigilance. Les mesures de vigilance simplifiée se traduisent par les contrôles et vérifications ci-après :

- vérification de l'identité du client et du bénéficiaire effectif après établissement de la relation d'affaires. La mise en œuvre des mesures de vérification doit néanmoins intervenir dans un délai raisonnable après l'entrée en relation d'affaires et au plus tard avant la réalisation de la première opération sur le compte ou de l'exécution de l'opération occasionnelle ;
- réduction de la fréquence des mises à jour des éléments d'identification du client ;
- réduction de l'intensité de la vigilance constante et de la profondeur de l'examen des opérations sur la base d'un seuil raisonnable.

Titre IV – Mesures de Vigilance dans le cadre des relations d'affaires à distance

Art. 16. — L'assujetti doit faire preuve d'une vigilance renforcée dans le cadre des relations d'affaires où la présence physique du client n'est pas requise. En conséquence, des mesures de diligence supplémentaires doivent être appliquées, notamment :

- la comparaison des données et informations obtenues du client avec d'autres informations provenant de sources fiables et indépendantes, permettant de valider la véracité des éléments fournis ;
- l'organisation d'un entretien direct avec le client dans un délai raisonnable



afin de compléter l'identification et d'assurer la cohérence des informations.

Titre V – Actualisation de la connaissance client : mise à jour des données

Art. 17. — Les assujettis doivent s'assurer que les informations et les documents obtenus dans le cadre de la mise en œuvre de leur devoir de vigilance à l'égard de leur clientèle restent à jour, exacts et pertinents. Ils actualisent les informations, les données et les documents obtenus, en temps opportun et de manière appropriée pendant toute la durée de la relation d'affaires selon une approche fondée sur les risques.

Les assujettis doivent prévoir dans leur procédure interne, les modalités de mise à jour de la connaissance de leur client en définissant la fréquence de la mise à jour ainsi que la nature des informations à mettre à jour.

La fréquence de la mise à jour ainsi que la nature des informations à mettre à jour, doivent être adaptées au niveau de risque de blanchiment de l'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive présenté par la relation d'affaires, sans pouvoir excéder un an (1) lorsque le niveau de risque associé au client est élevé.

La mise à jour intervient également dans les cas suivants :

- changement significatif dans la relation d'affaires, y compris tout changement de bénéficiaire effectif, de personnes agissant pour le compte du client, développement d'un nouveau produit ou service;
- aux fins de traitement d'une alerte relative à une ou plusieurs opération(s) atypique(s) incohérente(s) avec la connaissance du client, ses activités commerciales et son profil de risque. Cette mise à jour peut notamment porter sur l'activité du client, les revenus/ situation financière du client, l'origine des fonds, l'objet de l'opération ;
- à l'occasion d'une modification substantielle des normes de documentation sur la clientèle ou d'un changement important dans le mode de gestion du compte ainsi que dans les situations b et c citées dans l'article 09 du règlement n° 01 du 06 novembre 2024, susvisé.

Art. 18. — Les assujettis doivent analyser les informations, données et documents mis à jour afin de réévaluer le profil de risque du client.

Art. 19. — Les assujettis doivent mettre en place un dispositif de contrôle interne adapté à la taille et à la nature de l'activité et doté de moyens humains suffisants pour s'assurer de la mise à jour régulière des éléments de connaissance de leur



client en fonction d'une approche fondée sur les risques et de la pertinence des documents, données et informations collectés à cette fin.

A cet égard, les assujettis doivent définir :

- un calendrier détaillé pour l'actualisation de la connaissance client en fonction de la catégorie de risque auquel appartient le client (faible, normal, élevé) ainsi que la nature et l'étendue des vérifications à opérer, en veillant à renforcer les mesures de vigilance pour les risques élevés et à alléger celles pour les risques faibles
- les rôles et les responsabilités, en désignant des personnes ou équipes spécifiques chargées de la mise à jour des données, et en précisant les fonctions et responsabilités de chaque intervenant dans ce processus en fonction du niveau de risque;
- s'assurer que les documents et informations mis à jour sont pertinents et suffisants pour la gestion du risque.

Art. 20. — Si après l'ouverture d'un compte apparaissent des problèmes de mise à jour des éléments d'informations d'identification d'un client, l'assujetti doit clôturer le compte, en informer le titulaire, la Cellule de Traitement du Renseignement Financier et l'autorité de contrôle des assurances, et restituer le solde sauf stipulation contraire d'une autorité compétente. L'assujetti doit également cesser la relation d'affaires avec le client.

Titre VI - Surveillance continue des opérations

Art. 21. — L'assujetti doit exercer une vigilance constante à l'égard de la relation d'affaires, en procédant à un examen, adéquat et proportionné aux risques, des opérations effectuées pendant toute la durée de cette relation d'affaires. La surveillance continue des opérations doit reposer sur des informations à jour concernant les clients et doit permettre à l'assujetti de détecter de manière fiable les transactions inhabituelles ou suspectes.

Art. 22. — L'assujetti est tenue de disposer de procédures internes adéquates permettant, sur la base de son évaluation globale des risques, de formaliser (a) les critères et (b) seuils de significativité permettant d'identifier des opérations atypiques.



(a) Doivent être inclus notamment les critères suivants :

- toute opération particulièrement complexe;
- opération d'un montant anormalement élevé compte tenu de la connaissance client;
- toute opération effectuée dans des conditions inhabituelles compte tenu de l'activité normalement attendue ou habituelle du client ;
- toutes opérations qui portent notamment sur des montants, en liquide, sans relation avec les transactions habituelles ou concevables du client ;
- toute opération ne paraissant pas avoir de justification économique ou d'objet licite ;
- toute opération qui dépasse, le cas échéant, le seuil fixé par la réglementation en vigueur ;
- les opérations réalisées par des personnes établies dans des pays qui n'appliquent pas ou appliquent de manière insuffisante les normes internationales sur la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive, tels que publiés par la Cellule de Traitement du Renseignement Financier.

(b) Les seuils de significativité doivent être adaptés notamment à la nature de la clientèle, aux moyens de paiement, au montant moyen des opérations effectuées, aux zones géographiques concernées par les opérations.

Art. 23. — Le système de surveillance des opérations doit couvrir toutes les activités et tous les comptes de la clientèle, et doit permettre de détecter rapidement les opérations ayant un caractère inhabituel ou suspect en vue de les soumettre à un examen approfondi pour déterminer si ces opérations sont susceptibles d'être liées au blanchiment d'argent, au financement du terrorisme et au financement de la prolifération des armes de destruction massive.

Le système de surveillance peut être automatisé, toutefois, lorsque la nature et le volume des opérations ne justifient pas l'utilisation d'un tel système, un système manuel peut être mis en place.

Ce système de surveillance doit :

- 1- couvrir l'intégralité des comptes et contrats des clients et de leurs opérations ;
- 2- être basé sur des critères précis et pertinents, fixés par chaque assujettie en tenant compte, notamment, des caractéristiques de sa clientèle, des pays



zones géographiques concernées, des produits, services, opérations et canaux de distribution, et être suffisamment discriminants pour permettre de détecter efficacement les opérations atypiques ;

- 3- permettre une détection rapide de ces opérations ;
- 4- faire l'objet d'un examen périodique de sa pertinence en vue de l'adapter, au besoin, en fonction de l'évolution de la clientèle qu'elles ont, des produits et/ou des services qu'elles fournissent (interface et/ou canal de distribution), des pays ou zones géographiques dans lesquelles les transactions sont effectuées.

En cas de soupçon, l'assujetti doit faire une déclaration de soupçon à la Cellule de Traitement du Renseignement Financier quel que soit le montant de l'opération.

Art. 24. — Les assujettis doivent disposer de moyens humains suffisants pour analyser les alertes générées par le système de surveillance des opérations. En outre, le personnel concerné par le traitement de ces alertes doit disposer d'une qualification et d'une formation suffisante ainsi qu'un accès à toutes les informations internes nécessaires à l'exercice de sa mission.

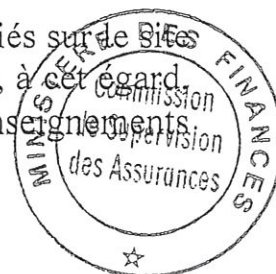
Titre VII – Dispositions relatives aux pays à risque

Art. 25. — Les assujettis doivent appliquer les procédures de diligence renforcée suivantes aux relations d'affaires effectuées avec des personnes physiques et morales, y compris les institutions financières des pays identifiés par la Cellule de Traitement des Renseignements Financiers comme présentant un risque élevé de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive, conformément aux critères définis par le Groupe d'Action Financière (GAFI) ou selon l'appréciation indépendante de la Cellule de Traitement des Renseignements Financiers :

- toute mesure ou procédure renforcée supplémentaire communiquée par la cellule ;
- toute autre procédure renforcée ayant un effet similaire pour atténuer les risques.

Les assujettis doivent également appliquer des contre-mesures relatives aux pays à haut risque, telles que communiquées par la Cellule de Traitement des Renseignements Financiers.

La liste des pays à risque élevé ainsi que les contre-mesures sont publiés sur le site web officiel de la Cellule de Traitement du Renseignement Financier, à cet égard, des notifications sont effectuées par la Cellule de Traitement des Renseignements



Financiers pour assurer la bonne application des ces mesures par les assujettis.

Art. 26. — Les assujettis sont tenus de s'abstenir d'établir ou de maintenir toute relation d'affaires avec des entités qui répondent aux caractéristiques de « institutions fictives ». Ils doivent également effectuer les diligences nécessaires pour s'assurer que leurs correspondants étrangers ne permettent pas à des institutions fictives d'accéder à leurs comptes ou de les utiliser de manière directe ou indirecte.

Titre VIII – Dispositions particulières sur les constructions juridiques-trusts

Art. 27. — On entend par construction juridique : Toute entité non régie par la législation en vigueur, y compris les trusts, constituée à l'étranger dans le cadre d'un contrat ou d'un accord par lequel une personne met des biens à la disposition d'une autre personne ou sous son contrôle pour une durée déterminée, avec l'intention de les gérer au profit d'un bénéficiaire spécifique ou dans un but défini. Ces biens ne sont alors pas considérés comme faisant partie du patrimoine de la personne qui en assure la gestion ou le contrôle.

Préalablement à l'entrée en relation d'affaires ou à la réalisation de toute opération, y compris occasionnelle, avec des entités juridiques non résidentes ou des structures équivalentes telles que les trusts ou autres constructions juridiques étrangères, l'assujetti doit recueillir les informations suivantes :

- la dénomination complète de l'entité ;
- les éléments de constitution de l'entité, incluant ses statuts, actes constitutifs, ou tout autre document d'enregistrement officiel dans le pays d'origine ;
- l'identité du constituant, du ou des trustees, du protecteur, des bénéficiaires ou de la catégorie de bénéficiaires, ainsi que de toute autre personne physique exerçant un contrôle effectif sur la structure, y compris à travers une chaîne de contrôle/propriété ;
- l'identité des bénéficiaires effectifs, incluant toute personne physique qui, en dernier ressort, détient ou contrôle l'entité, directement ou indirectement, par l'intermédiaire de parts, actions, ou tout autre instrument juridique ;
- les pouvoirs attribués aux personnes concernées, ainsi que les noms et rôles des personnes occupant des fonctions de direction ou de gestion ;
- les objectifs poursuivis par l'entité, ainsi que les modalités de gestion et de représentation de l'entité, y compris toute information sur la manière



les décisions sont prises ;

- l'adresse du siège social, et si elle est différente, l'adresse de l'un des principaux lieux d'activité, ainsi que le lieu de résidence du représentant légal de l'entité ;
- les documents supplémentaires nécessaires pour établir la chaîne de contrôle/propriété, notamment lorsque la structure de contrôle est complexe, ou lorsqu'elle implique plusieurs intermédiaires ou juridictions.

L'assujetti doit vérifier les informations ci-dessus au moyen de tout document constitutif de preuve et conserver une copie de ces documents.

Art. 28. — L'assujetti doit mettre en œuvre les mesures suivantes pour identifier et vérifier les bénéficiaires effectifs des constructions juridiques, des trusts ou des entités juridiques étrangères :

- recueillir des informations complètes permettant d'identifier chaque bénéficiaire effectif, en incluant toute personne physique exerçant un contrôle direct ou indirect sur l'entité, ainsi que ceux détenant des droits économiques, financiers ou de gestion ;
- exiger des renseignements supplémentaires sur la nature et l'étendue de la participation de chaque bénéficiaire effectif, y compris les droits de propriété, de contrôle ou d'influence exercés, qu'ils soient directs ou indirects ;
- vérifier l'identité de chaque bénéficiaire effectif en s'appuyant sur des documents probants, indépendants et fiables, tels que les registres officiels, les documents notariés, ou tout autre document certifié ;
- s'assurer que les informations sur les bénéficiaires effectifs sont mises à jour régulièrement, notamment lors de changements significatifs dans la structure de contrôle ou de propriété de l'entité ;
- conserver une copie de tous les documents et informations obtenus relatifs aux bénéficiaires ;
- appliquer toute autre mesure jugée nécessaire pour atteindre un niveau de certitude élevé dans l'identification et la vérification des bénéficiaires effectifs.

Titre IX – L'adaptation du niveau de vigilance selon la nature et le niveau du risque

Art. 29. — Le degré et la nature de la surveillance de la relation d'affaires présentant des risques plus élevés doivent être renforcés conformément à l'article 14 de la présente instruction dans les cas suivants :



a- Les clients présentant, par nature, un risque élevé

- les clients identifiés par l'assujetti dans le cadre de l'analyse et l'évaluation des risques ;
- la relation d'affaires se déroule dans des circonstances inhabituelles ;
- les clients non-résidents ;
- les sociétés dont le capital est détenu par des mandataires ;
- les activités nécessitant beaucoup d'espèces ;
- la structure de la propriété de la société semble inhabituelle ou excessivement complexe au regard de la nature de l'activité de la société ;
- les personnes politiquement exposées ;
- les personnes politiquement exposées appartenant aux organisations internationales ;
- les organisations à but non lucratif ;
- les constructions juridiques établies à l'étranger, y compris les trusts.

b- Les opérations effectuées par le client avec certains pays ou liées à ces pays

- les pays identifiés par des sources crédibles telles que les rapports d'évaluation mutuelle ou d'évaluation détaillée ou des rapports de suivi publiés, comme n'étant pas dotés d'un dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive satisfaisant ;
- les pays soumis à des sanctions, des embargos ou des mesures similaires prises par exemple, par les Nations Unies ;
- les pays identifiés par des sources crédibles comme étant caractérisés par des niveaux considérables de corruption ou autres activités criminelles ;
- les pays ou zones géographiques identifiés par des sources crédibles comme apportant des financements ou un soutien à des activités terroristes ou dans lesquels opèrent des organisations terroristes désignées ;
- les pays qui souffrent de conditions politiques et sécuritaires qui entravent leur engagement envers les recommandations du Groupe d'action financière.



c- Les produits et services utilisés par le client ainsi que certaines opérations

- gestion de patrimoine et de fortune ;
- opérations en espèces non identifiées ;
- opérations qui n'impliquent pas la présence physique des parties ;
- paiement reçu de tiers non associés ou inconnus ;
- opérations effectuées par ou au bénéfice des clients résidant dans des pays présentant un risque élevé de blanchiment de capitaux, de financement de terrorisme et de financement de la prolifération des armes de destruction massive, notamment ceux listés par les instances internationales habilitées.

Art. 30. — Les mesures de vigilance peuvent être simplifiées conformément à l'article 15 de la présente instruction, lorsque le risque de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive présenté par une relation d'affaires leur paraît faible et dans les cas suivants en l'absence de soupçon de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération des armes de destruction massive.

a- Les clients présentant un risque faible

- les institutions financières; lorsqu'elles sont soumises à des obligations de lutte contre le blanchiment d'argent et le financement du terrorisme et le financement de la prolifération des armes de destruction massive, conformes aux recommandations du groupe d'action financière (GAFI), qu'elles ont efficacement mis en œuvre ces obligations et qu'elles font l'objet d'un contrôle ou d'une surveillance efficace conformément aux recommandations garantissant qu'elles respectent leurs obligations ;
- les sociétés cotées sur le marché boursier et soumises par des moyens légaux ou contraignants, à des règles de publication garantissant une transparence suffisante des bénéficiaires effectifs ;
- les administrations ou entreprises publiques.

b- Les produits, services, opérations présentant un risque faible

- les régimes de retraite ou régimes similaires qui servent des prestations de retraite aux employés, lorsque les cotisations sont acquittées par prélèvement sur les salaires et que les règles du régime n'autorisent pas



la cession des droits détenus par un membre dans le cadre du régime ;

- les services ou produits financiers qui fournissent des services limités et définis de façon pertinente afin d'en accroître l'accès à certains types de clients à des fins d'inclusion financière.

c- Les opérations transfrontalières avec certains pays ou liées à ces pays

- les pays identifiés par des sources crédibles telles que les rapports d'évaluation mutuelle ou d'évaluation détaillée comme disposant de systèmes de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive efficaces ;
- les pays identifiés par des sources crédibles comme étant caractérisés par un faible niveau de corruption ou autres activités criminelles.

Art. 31. — Les assujettis sont tenus de justifier auprès de l'autorité de contrôle des assurances que l'étendue des mesures de vigilance qu'ils mettent en œuvre est adaptée aux risques qu'ils ont évalués.

Titre X- Conservation des documents

Art. 32. — Les assujettis doivent :

- conserver tous les documents obtenus dans le cadre des mesures de vigilance relatives à la clientèle, pendant au moins cinq (5) ans à compter de la date de la fin de la relation d'affaires ;
- conserver tous documents relatifs aux opérations effectuées, y compris les rapports confidentiels, durant une période de cinq (5) ans au moins, après l'exécution de l'opération ;
- s'assurer que toutes les informations obtenues dans le cadre des mesures de vigilance relatives à la clientèle et les documents relatifs aux opérations sont rapidement disponibles pour les autorités compétentes, lorsque ces dernières en font la demande.

Les documents relatifs aux opérations doivent être suffisants pour permettre la reconstitution d'opérations individuelles.



Art. 33. — Les assujettis sont tenus de conserver les documents, dossiers et registres ci-après :

- dossiers et documents obtenus par l'application d'une diligence raisonnable à l'égard des clients et des bénéficiaires effectifs y compris les demandes d'ouverture de comptes ou de tout autre produit ou service fourni de l'assujetti, ainsi que les copies de la correspondance échangée avec eux ;
- les preuves et les documents à l'appui des opérations entre l'assujetti et le client, y compris les documents originaux ou des copies acceptables par les autorités compétentes ;
- livres de comptes et documents relatifs aux opérations commerciales avec les clients, y compris des données suffisantes pour reconnaître les détails de chaque opération ;
- les rapports sur les opérations inhabituelles, l'examen de ces rapports et les dossiers et documents relatifs aux décisions prises sur les opérations examinées ;
- les dossiers des opérations suspectes, y compris les copies des déclarations de soupçon envoyées à la Cellule de Traitement de Renseignement Financier, ainsi que les données et documents connexes ;
- les dossiers et documents relatifs aux résultats de toute analyse effectuée sur les opérations examinées.

Art. 34. — Les assujettis doivent respecter les conditions suivantes lors de la conservation des registres et documents stipulés dans la clause précédente :

- la conservation doit se faire de manière sécurisée, avec des copies de sauvegarde dans un emplacement distinct et sécurisé ;
- les copies numérisées des registres et documents susmentionnés doivent être dûment conservés ;
- les relevés de transactions doivent être suffisants pour permettre la reconstitution des transactions individuelles afin qu'ils puissent fournir, si nécessaire, des preuves contre une activité criminelle ;
- les enregistrements et les documents conservés doivent pouvoir être retrouvés facilement et rapidement, et toute donnée ou information demandée doit être fournie promptement de manière adéquate ;
- les procédures et les systèmes de conservation des enregistrements et des documents doivent préciser le pouvoir des personnes concernées d'accéder à ces enregistrements et documents.



Titre XI -Virements électroniques

Art . 35. — Ce chapitre s'applique exclusivement aux sociétés d'assurances et de réassurances, ci-dessous désignées « institution financière », lorsqu'elles participent indirectement aux systèmes de paiement dans le cadre des virements électroniques.

Art. 36. — Au sens du présent titre, on entend par :

Donneur d'ordre : Il s'agit de la personne physique ou morale qui donne instruction à l'institution financière de procéder à un virement électronique, même lorsqu'elle ne dispose pas de compte ouvert auprès de la dite institution financière.

Bénéficiaire : Désigne la personne physique ou morale, identifiée par l'expéditeur (donneur d'ordre), comme le destinataire du virement électronique.

Institution financière du donneur d'ordre : l'institution financière qui initie le virement électronique et procède au transfert de fonds par virement électronique sur instruction et pour le compte du donneur d'ordre.

Institution financière du bénéficiaire : l'institution financière qui reçoit le virement électronique de l'institution financière du donneur d'ordre, via une institution financière intermédiaire, et met les fonds à disposition du bénéficiaire.

Virement électronique : toute opération effectuée par voie électronique pour le compte d'un donneur d'ordre via une institution financière en vue de mettre à la disposition d'un bénéficiaire une somme d'argent auprès d'une autre institution financière, étant entendu que le donneur d'ordre et le bénéficiaire peuvent constituer une seule et même personne.

Virement électronique national : un virement électronique pour lequel l'institution financière du donneur d'ordre et celui du bénéficiaire sont situés dans le territoire national.

Art. 37. — Les institutions financières doivent s'assurer, pour tous les virements électroniques nationaux, qu'ils sont accompagnés obligatoirement des informations requises et exactes suivantes, à moins que ces informations puissent être mises à la disposition de l'institution financière du bénéficiaire et des autorités concernées par d'autres moyens :

a- Le nom et prénom(s) du donneur d'ordre ;



b- Le numéro de compte du donneur d'ordre dès lors qu'un tel compte est utilisé pour la réalisation de l'opération. En l'absence de compte, un numéro de référence unique d'opération permettant la traçabilité de l'opération ;

c- L'adresse du donneur d'ordre, ou son numéro d'identité national, ou son numéro d'identification client, ou sa date et son lieu de naissance.

d- Le nom et prénom(s) du bénéficiaire ;

e- Le numéro de compte du bénéficiaire dès lors qu'un tel compte est utilisé pour la réalisation de l'opération. En l'absence de compte, un numéro de référence unique d'opération permettant la traçabilité de l'opération.

Ces informations doivent être intégrées dans le système d'information de l'institution financière et facilement exploitables.

Art. 38. — Toutefois, lorsque ces informations peuvent être mises à la disposition de l'institution financière du bénéficiaire et des autorités concernées par d'autres moyens, l'institution financière du donneur d'ordre doit seulement inclure le numéro de compte ou un numéro de référence unique d'opération, à condition que ce numéro de compte ou cet identifiant permette de reconstituer le parcours de l'opération jusqu'au donneur d'ordre ou au bénéficiaire.

Art. 39. — Dans les trois (03) jours ouvrables à compter de la réception de leur demande, l'institution financière du donneur d'ordre doit mettre à la disposition, selon le cas, de l'institution financière du bénéficiaire et/ou des autorités compétentes concernées, les informations concernant le donneur d'ordre.

Conformément aux dispositions législatives en vigueur, ces informations sont mises immédiatement, à la disposition de l'autorité judiciaire.

Art. 40. — Les informations recueillies sur le donneur d'ordre et le bénéficiaire doivent être conservées pendant au moins cinq (05) ans après l'exécution de l'opération, par l'institution financière du donneur d'ordre.

Art. 41. — Les institutions financières ne sont pas autorisées à exécuter les virements électroniques ne comportant pas les informations requises sur le donneur d'ordre et le bénéficiaire, telles que visées dans l'article 37 ci-dessus.



Titre XII - Dispositions diverses

Art. 42. — Le non-respect des dispositions de la présente instruction expose l'assujetti aux sanctions prévues par la législation et la réglementation en vigueur.

Art. 43. — La présente instruction prend effet à compter de la date de sa signature.

Le Président de la Commission de Supervision
des Assurances



Le Président de la Commission
de Supervision des Assurances


Hadj Mohammed SEBA