



**POLITIQUE DE LUTTE CONTRE LE BLANCHIMENT DE
CAPITAUX, LE FINANCEMENT DU TERRORISME ET DE LA
PROLIFERATION DES ARMES DE DESTRUCTION MASSIVE**

TABLE DES MATIERES

I. CONTEXTE	2
II. DEFINITIONS.....	2
III. OBJET DU DISPOSITIF.....	4
IV. TERMINOLOGIE	4
V. L'IDENTIFICATION DES CLIENTS ET DES BENEFICIAIRES EFFECTIFS	8
VI. GESTION DES RISQUES DE BLANCHIMENT DE CAPITAUX, DE FINANCEMENT DU TERRORISME ET DE LA PROLIFERATION DES ARMES DE DESTRUCTION MASSIVE ...	10
VII. VIGILANCE A L'EGARD DE LA CLIENTELE	13
a) Personnes Physiques	13
b) Personnes Morales et les constructions juridiques.....	17
c) Clients occasionnels	20
d) Bénéficiaires effectifs	20
e) Les Correspondants Bancaires hors UMOA.....	22
f) Cas spécifiques.....	23
g) Cas des établissements publics et autres entités :.....	24
VIII. SURVEILLANCE DES OPERATIONS.....	26
a) Détections à priori :	27
i. Les opérations en espèces.....	27
ii. Les remises de chèques.....	28
iii. Les virements/prélèvements	28
iv. Les placements	29
b) Détections à posteriori	29
c) Autres opérations à surveiller	29
d) Conduites à adopter face aux opérations suspectes.	33
e) Surveillance continue du dispositif de vigilance.....	34
IX. CONSERVATION DES PIECES ET DOCUMENTS.....	36
X. ORGANISATION DU CONTROLE INTERNE	37
a) 1ère ligne de défense	37
b) 2e ligne de défense	37
c) 3 ^{ème} ligne de défense.....	38
d) Structure d'appui et de conseil : La Direction Juridique et du recouvrement (DJR)	38
XI. GESTION DE LA CONFORMITE AUX DISPOSITIONS DE LA PRESENTE ORDONNANCE ET DES TEXTES PRIS EN APPLICATION.....	38
XII. PROTECTION DES DONNEES	38
XIII.RECRUTEMENT, FORMATION CONTINUE ET L'INFORMATION ET LA SENSIBILISATION DU PERSONNEL	39
XIV. RESPECT DES SANCTIONS INTERNATIONALES ET EMBARGOS.....	40
a) Définitions et normes	40
b) Les bonnes pratiques	41
c) Catégories des sanctions internationales	42



I. CONTEXTE

Le présent dispositif s'inscrit dans le cadre de la mise en œuvre de la Directive n° 01/2023/CM/UEMOA relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des armes de destruction massives des Etats membres de l'UMOA. Il s'appuie notamment sur les textes réglementaires, ci-après :

- Les 40 recommandations du Groupe d'Action Financière(GAFI) ;
- La Directive n° 01/2023/CM/UEMOA relative à la LBC/FT/FP des Etats membres de l'UMOA ;
- L'Ordonnance n°2023-875 du 23 novembre 2023 relative à la LBC/FT/FP ;
- La Décision n°21 du 21/12/2023 fixant le montant des seuils de la mise en œuvre de la loi uniforme LBC/FT/FP ;
- L'Instruction n° 003-03-2025 relative à l'identification, la vérification de l'identité et la connaissance de la clientèle par les institutions financières ;
- L'Instruction n°001-03-2025 portant modalités de mise en œuvre par les Institutions financières de leurs obligations en matière d'organisation, de contrôle interne et de conformité aux exigences de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive ;
- L'instruction n°10-09-2017 fixant le seuil pour les déclarations systématiques des transactions en espèces à la CENTIF.

II. DEFINITIONS

Au sens de l'Ordonnance n°2023-875 du 23 novembre 2023 relative à la LBC/FT/FP :

- **Le blanchiment de capitaux :** Constituent une infraction de blanchiment de capitaux, les agissements énumérés, ci-après, commis intentionnellement :
 - a) la conversion ou le transfert de biens, par toute personne qui sait ou aurait dû savoir que ces biens proviennent d'un crime ou délit ou d'une participation à un crime ou délit, dans le but de dissimuler ou de déguiser l'origine illicite desdits biens, ou d'aider toute personne impliquée dans cette activité à échapper aux conséquences juridiques de ses actes;
 - b) la dissimulation ou le déguisement de la nature, de l'origine, de l'emplacement de la disposition, du mouvement ou de la propriété réelle de biens ou des droits y relatifs, par toute personne qui sait ou aurait dû savoir que ces biens proviennent d'un crime ou délit ou d'une participation à un crime ou délit;



- c) l'acquisition, la détention ou l'utilisation de biens, dont celui qui s'y livre, sait ou aurait dû savoir, au moment où il les réceptionne, que ces biens proviennent d'un crime ou délit ou d'une participation à un crime ou délit;
 - d) la participation à l'un des actes visés aux points a), b) et c) du présent alinéa, le fait de s'associer pour le commettre, de tenter de le commettre, d'aider ou d'inciter quelqu'un à le commettre ou de le conseiller, à cet effet, ou de faciliter l'exécution d'un tel acte.
- **Le financement du terrorisme :** Constitue une infraction de financement du terrorisme, tout acte commis par une personne physique ou morale qui, par quelque moyen que ce soit, directement ou indirectement, a délibérément fourni ou collecté des biens, des fonds et d'autres ressources économiques financières et matérielles, dans l'intention de les utiliser ou sachant qu'ils seront utilisés, en tout ou partie :
 - a) en vue de la commission d'un ou de plusieurs actes terroristes;
 - b) par une organisation terroriste ou un individu terroriste.

Constitue également une infraction de financement du terrorisme, le fait pour une personne physique ou morale de recruter, proposer de financer ou de financer le voyage d'une personne qui se rend dans un Etat autre que son Etat de résidence ou de nationalité, dans le dessein de commettre, d'organiser ou de pré-parer un acte terroriste, ou afin d'y participer ou de dispenser ou recevoir un entraînement au terrorisme.

- **Le financement de la prolifération des armes de destruction massives :** Constitue une infraction de financement de la prolifération des armes de destruction massive, tout acte commis par une personne physique ou morale qui, par quelque moyen que ce soit, directement ou indirectement, procure délibérément un financement en fournissant, collectant, ou gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens ou en sachant qu'ils sont destinés à être utilisés, en tout ou en partie, pour la fabrication, l'acquisition, la possession, le développement, l'export, le transbordement, le courtage, le transport, le transfert, le stockage ou l'emploi d'armes nucléaires, chimiques, biologiques, de leurs vecteurs et de matériels associés.



III. OBJET DU DISPOSITIF

La présente Politique a pour objectif d'identifier, d'atténuer et de gérer efficacement les risques de blanchiment de capitaux, de financement du terrorisme et de la prolifération des armes de destruction massive identifiés au niveau de la banque, mais aussi aux plans national, régional et international. Elle vise également à protéger la Banque De l'Union Côte d'Ivoire (BDU-CI) contre tout risque pouvant résulter d'opérations de blanchiment d'argent, de prévenir l'utilisation de ses guichets à des fins de recyclage de capitaux issus d'activités illégales ou criminelles, ou de tous autres biens d'origine illicite.

La politique couvre notamment les domaines ci-après :

- L'identification des clients et des bénéficiaires effectifs ;
- La gestion des risques de blanchiment de capitaux, de financement du terrorisme et de la prolifération des armes de destruction massive ;
- La vigilance à l'égard de la clientèle ;
- La surveillance des transactions ;
- La conservation des documents ;
- Le contrôle interne ;
- La gestion de la conformité aux dispositions de la présente ordonnance et des textes pris pour son application ;
- La protection des données à caractère personnel ;
- Le recrutement, la formation continue et l'information et la sensibilisation du personnel ;
- Respect des sanctions internationales et embargos ;
- Déclarations de soupçons ;
- Coopération avec les autorités ;
- Vigilance particulière pour certaines catégories d'opérations.

IV. TERMINOLOGIE

Acte terroriste :

- a) un acte constitutif d'une infraction au sens de l'un des instruments juridiques internationaux énumérés en annexe à la présente ordonnance ;
- b) tout autre acte destiné à tuer ou blesser grièvement un civil, ou toute autre personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, lorsque, par sa nature ou son contexte, cet acte vise à intimider une population ou à contraindre un Gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque.



Actif Virtuel : La représentation numérique d'une valeur qui peut être échangée ou transférée par un procédé numérique. Les actifs virtuels n'incluent pas les représentations numériques des monnaies fiduciaires, titres et autres actifs financiers qui font l'objet d'une réglementation ou de dispositions réglementaires spécifiques.

Activité criminelle : Tout acte criminel ou délictuel constituant une infraction sous-jacente au blanchiment de capitaux, au financement du terrorisme et de la prolifération des armes de destruction massive, à savoir :

- la participation à un groupe criminel organisé ;
- le terrorisme, y compris son financement ;
- la traite des êtres humains et le trafic illicite de migrants;
- l'exploitation sexuelle, y compris le détournement et l'exploitation des mineurs ;
- le trafic illicite de stupéfiants et de substances psychotropes;
- le trafic illicite d'armes ;
- le trafic illicite de biens volés et autres biens ;
- la corruption et la concussion;
- le détournement de fonds par des personnes exerçant une fonction publique ;
- la fraude ;
- le faux monnayage;
- la contrefaçon de biens, y compris monnaie ou de billets de banque et le piratage de produits ;
- le trafic d'organes;
- les infractions contre l'environnement;
- les meurtres et les blessures corporelles graves ;
- l'enlèvement, la séquestration et la prise d'otages ;
- le vol ;
- la contrebande, y compris notamment celle relative aux taxes et droits de douane et d'accise;
- les infractions fiscales;
- l'extorsion ;
- le faux et l'usage de faux;
- la piraterie;
- les délits d'initiés et la manipulation de marchés ;
- tout autre crime ou délit.

Biens : Les avoirs de toute nature, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, fongibles ou non fongibles ainsi que les documents ou instruments juridiques sous quelque forme que ce soit, y compris électronique ou numérique, attestant la propriété de ces avoirs ou de droits y afférents ainsi que les intérêts sur lesdits avoirs, à savoir notamment les crédits, les chèques de voyage, les chèques, les mandats, les actions, les valeurs mobilières, !es obligations, les traites ou lettres de crédit ainsi que les éventuels intérêts, dividendes ou autres revenus ou valeur tirés de tels avoirs, ou générés par de tels avoirs.



Banque fictive : Une banque qui a été constituée et agréée dans un Etat où elle n'a pas de présence physique et qui n'est pas affiliée à un groupe financier réglementé soumis à une surveillance consolidée et effective. L'expression présence physique désigne la présence d'une direction et d'un pouvoir de décision dans un pays. La simple présence physique d'un agent local ou de personnel subalterne ne constitue pas une présence physique.

CENTIF : La cellule Nationale de Traitement des Informations Financières instituées dans chaque état membre de l'UEMOA.

Client occasionnel : toute personne qui s'adresse à l'une des personnes assujetties, dans le but exclusif de préparer ou d'effectuer une opération ponctuelle ou d'être assistée dans la préparation ou la réalisation d'une telle opération, que celle-ci soit réalisée en une seule opération ou en plusieurs opérations apparaissant comme liées entre elles. La notion de client occasionnel exclut l'existence d'un compte au nom du client ouvert dans les livres de la personne assujettie à la présente ordonnance.

Personnes Politiquement Exposées (PPE) étrangères : les personnes physiques qui exercent ou qui ont exercé d'importantes fonctions publiques dans un autre Etat membre ou un Etat tiers notamment :

- a) les Chefs d'Etat ou de Gouvernement, les Ministres, les Ministres délégués et les Secrétaires d'Etat ;
- b) les membres de familles royales ;
- c) les Secrétaires Généraux de la Présidence de la République, du Gouvernement ou des ministères ainsi que les Directeurs généraux des ministères ;
- d) les parlementaires ;
- e) les membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles ;
- f) les membres des cours des comptes ou des conseils ou directoires des banques centrales ;
- g) les ambassadeurs, les chargés d'affaires et les officiers supérieurs des forces armées
- h) les membres des organes d'administrations, de direction ou de surveillance des entreprises publiques ;
- i) les hauts responsables des partis politiques ;



- j) les membres de la famille d'une PPE, en l'occurrence : le conjoint ; tout partenaire considéré comme l'équivalent d'un conjoint ; les enfants et leurs conjoints ou partenaires ; les autres parents ;
- k) les personnes connues pour être étroitement associées à une PPE
- l) les personnes connues pour être étroitement associées à une PPE ;
- m) toute autre personne désignée par la personne assujettie sur la base de l'analyse de son profil risque ;

Personnes Politiquement Exposées (PPE) nationales : les personnes physiques qui exercent ou qui ont exercé d'importantes fonctions publiques dans l'Etat membre concerné, notamment les personnes physiques visées au a) à i) ci-dessus ;

PPE des organisations internationales : les personnes qui exercent ou qui ont exercé d'importantes fonctions au sein de ou pour le compte d'une organisation internationale, notamment les membres de la haute direction, en particulier, les directeurs, les directeurs adjoints et les membres du Conseil d'Administration et toutes les personnes exerçant des fonctions équivalentes.

Bénéficiaire Effectif : Le bénéficiaire effectif est la ou les personnes physiques qui, en dernier ressort, possèdent ou contrôlent le client, le mandataire du client ou le bénéficiaire des contrats d'assurance vie, et/ou la ou les personnes physiques pour lesquelles une opération est exécutée ou une relation d'affaires nouée. Sont considérés comme possédant ou contrôlant, en dernier ressort le client, le mandataire du client ou le bénéficiaire d'une personne morale ou d'une construction juridique :

- a) dans le cas d'une société, la ou les personnes physiques qui soit détiennent, directement ou indirectement, plus de vingt-cinq pour cent du capital ou des droits de vote de la société, soit exercent, par tout autre moyen, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction de la société ou sur l'assemblée générale de ses associés ;
- b) dans le cas d'un organisme de placements collectifs, la ou les personnes physiques qui soit détiennent, directement ou indirectement, plus de vingt-cinq pour cent des parts ou actions de l'organisme, soit exercent un pouvoir de contrôle sur les organes d'administration ou de direction de l'organisme de placements collectifs ou, le cas 20



- échéant, de la société de gestion ou de la société de gestion de portefeuille le représentant ;
- c) dans le cas d'une personne morale qui n'est ni une société ni un organisme de placements collectifs, ou lorsque le client intervient dans le cadre d'une fiducie ou de tout autre dispositif juridique comparable relevant d'un droit étranger, la ou les personnes physiques qui satisfont à l'une des conditions suivantes :
- i. elles ont vocation, par l'effet d'un acte juridique les ayant désignées à cette fin, à devenir titulaires de droits portant sur vingt-cinq pour cent au moins des biens de la personne morale ou des biens transférés à un patrimoine fiduciaire ou à tout autre dispositif juridique comparable relevant d'un droit étranger ;
 - ii. elles appartiennent à un groupe dans l'intérêt principal duquel la personne morale, la fiducie ou tout autre dispositif juridique comparable relevant d'un droit étranger a été constitué ou a produit ses effets, lorsque les personnes physiques qui en sont les bénéficiaires n'ont pas encore été désignées ;
 - iii. elles sont titulaires de droits portant sur vingt-cinq pour cent au moins des biens de la personne morale, de la fiducie ou de tout autre dispositif juridique comparable relevant d'un droit étranger ;
 - iv. elles ont la qualité de constituant, de fiduciaire ou de bénéficiaire, conformément aux textes législatifs et réglementaires en vigueur ;

GIABA : Le Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest.

RECEN-UMEOA : Le Réseau des CENTIF de l'UEMOA.

Sans délai : Un délai maximal de 24 heures.

V. L'IDENTIFICATION DES CLIENTS ET DES BÉNÉFICIAIRES EFFECTIFS

L'entrée en relation avec un nouveau client suppose une connaissance parfaite de son identité, son adresse et son activité. L'obligation de « bien connaître son client » est la base de la lutte contre le Blanchiment.

La notion de client doit être envisagée dans son acception la plus large, à savoir l'ensemble des relations, qu'elle qu'en soit la nature, (entreprises, particuliers, banques, institutionnels, sociétés de gestion etc.). De même, doit être considérée comme un client, toute personne ayant



procuration sur le fonctionnement d'un compte de particulier ou d'entreprise (mandataire). Il en est également ainsi des personnes intervenant en qualité de garant sur une opération initiée au profit d'un autre client (tiers caution).

Dans le cadre de nos activités, l'identification de notre clientèle (personnes physiques, personnes morales) se fait en collectant les informations ci les informations ci-après :

- **Personnes physiques** : les nom et prénoms, les date et lieu de naissance, la nationalité ; l'adresse du domicile, le numéro de la pièce d'identification, l'emploi ou l'activité commerciale, la situation financière notamment les revenus et tout élément permettant d'estimer les autres ressources disponibles ainsi que d'apprécier le patrimoine du client, la nature des liens existants, le cas échéant, avec les tiers amenés à intervenir dans la relation d'affaires (mandataires ayant procuration, tiers payeurs, etc.).
- **Personne morale** : la raison sociale, la forme juridique, la liste des dirigeants et actionnaires ou associés, les éléments d'identification des personnes physiques habilitées, à représenter la personne morale concernée vis-à-vis des tiers ou à agir en son nom en vertu d'un mandat, l'adresse du siège social ou celle du lieu où sont prises les décisions stratégiques nécessaires à la conduite des affaires de la personne morale, si celle-ci est différente de l'adresse du siège social, la liste des bénéficiaires effectifs , le numéro national d'immatriculation, d'enregistrement, du Registre du Commerce et du Crédit Mobilier ou d'identification fiscale, le cas échéant, l'objet social ainsi que le secteur d'activité, les mandats et pouvoirs des dirigeants et représentants légaux de la structure, tout élément permettant d'apprécier la situation financière.

Au-delà de la connaissance du titulaire du compte, la Banque a donc l'obligation de connaître les véritables **bénéficiaires effectifs** des comptes et de constituer un dossier les concernant et de collecter les informations nécessaires à la satisfaction de ses obligations en matière d'entrée en relation et de surveillance.

Il convient de préciser que sont ici visés aussi bien les comptes que les transactions.

Aussi, la procédure de connaissance clientèle **s'applique au tiers** si le client ne semble pas être le bénéficiaire de l'ouverture de **compte ou de la réalisation de l'opération** pour laquelle il entre en relation avec notre établissement, **conformément aux exigences de l'instruction d'entrée en relation de la BDU-CI** en identifiant **ce dernier** au même titre que la relation. A défaut cesser toute relation.

A cet effet, la Banque doit s'efforcer **non seulement** de vérifier l'identité de ses clients, mais également de déterminer les opérations **susceptibles** de lui être confiées par ce client en fonction de ses revenus, de son activité, de son patrimoine, etc. Ainsi, la collecte des informations et



l'obtention de la totalité des documents nécessaires à l'ouverture de comptes ou à l'attribution d'un coffre-fort, ainsi que la mise à jour des renseignements constituent le noyau de la politique de vigilance en matière de lutte contre le blanchiment, le financement du terrorisme et la prolifération des armes de destruction massive.

L'analyse des données recueillies (identité, adresse, activité) doit permettre d'attribuer à chacune d'elles un niveau de risque (faible, modéré, élevé). Le niveau de risque global du client sera celui des données affichant le niveau de risque le plus élevé. La vigilance pour rassembler ces informations est indispensable pour analyser ultérieurement les opérations suspectes ou atypiques qui pourraient masquer une activité délictueuse.

Cette vigilance s'étend aux opérations sur bons, titres et valeurs bénéficiant de l'anonymat fiscal.

La capacité de répondre aux 3 questions suivantes est la règle d'or de la lutte contre le blanchiment :

- **D'où viennent les fonds ? (Donneur d'ordre) ;**
- **Où vont-ils ? (Bénéficiaire) ;**
- **Pourquoi ? (Justification économique de l'opération).**

La règle « connaît ton client » ou « KYC » est d'application générale et s'applique à toute la clientèle de la Banque sans exception.

VI. GESTION DES RISQUES DE BLANCHIMENT DE CAPITAUX, DE FINANCEMENT DU TERRORISME ET DE LA PROLIFERATION DES ARMES DE DESTRUCTION MASSIVE

La BDU-CI doit procéder à la classification de ses clients, selon leur profil de risque et en tenant compte notamment des principaux facteurs de risques ci-dessous :

- **Risque produit** : les risques liés aux types de services, produits ou transactions concernés notamment en termes de (i) transparence ou d'opacité, (ii) de complexité, (iii) de valeur, taille ou montant de la transaction ainsi que (iv) de canaux de commercialisation y compris les technologies ou les intermédiaires auxquels l'institution financière pourrait avoir recours.



- **Risque pays** : les risques qui sont liés aux territoires :

- ✓ dans lesquels l'institution financière el/ou ses clients el/ou bénéficiaires effectifs ont leur siège social et/ou exercent des activités ;
- ✓ avec lesquels l'institution financière el/ou ses clients ont des relations d'affaires ;
- ✓ où les fonds utilisés pour l'opération ont été générés ou ont transité
- ✓ Identifiés comme la destination finale des fonds utilisés pour l'opération.

Dans l'évaluation du risque pays, les institutions financières tiennent également compte : (i) de l'appartenance des pays à des unions monétaires el/ou économiques, (ii) des listes grise ou noire du GAFI, (iii) de la liste de pays, organisations et personnes qui font l'objet de sanctions financières ciblées publiées par les Nations Unies, (iv) des autres listes pertinentes publiées par les Etats membres de l'UMOA le cas échéant, (v) des rapports d'évaluations mutuelles et des publications du GAFI el/ou du GIABA, (vi) des évaluations du FMI et des rapports du Programme d'évaluation du secteur financier, (vii) des informations diffusées par les autorités compétentes et (viii) de toute autre information pertinente.

- **Risque client** : les risques relatifs aux caractéristiques des clients et de la relation d'affaires. Les éléments à considérer portent notamment sur :

- ✓ la nature des clients (personne physique, personne morale ou construction juridique se présentant sous forme de structure plus ou moins complexe favorisant ou non l'anonymat, personne agissant pour son compte propre ou pour le compte d'un tiers, personne politiquement exposée, personne physique non présente physiquement, client occasionnel ou permanent etc.) ;
- ✓ les activités professionnelles ou économiques du client ;
- ✓ la situation financière et patrimoniale du client ;
- ✓ l'origine du patrimoine du client ;
- ✓ le montant, la nature et le volume des opérations envisagées ou effectuées ;
- ✓ la provenance et la destination des fonds ;
- ✓ les antécédents financiers du client ;
- ✓ l'historique des transactions financières du client ;
- ✓ la justification économique de la relation d'affaires envisagée
- ✓ la durée de la relation d'affaires en cours ;
- ✓ l'intervention d'intermédiaires entre le client et l'institution financière ;
- ✓ le comportement du client (refus de fournir des informations) ;



- ✓ la présence du client sur une liste de sanctions pour financement du terrorisme ou de la prolifération des armes de destruction massive.

Les informations permettant la classification des clients par niveau de risque LBC/FT/FP sont en partie collectées dès l'entrée en relation (ex. caractéristiques clients : Secteurs d'activité, canal d'entrée en relation...), d'autres sont identifiées tout au long de la vie de la relation (ex. pays de réalisation d'une transaction, typologie d'une transaction...).

Afin d'attribuer une classification finale pour chaque client, un système de pondération doit être mis en place pour chaque facteur de risque sans que la note finale ne soit influencée de manière excessive par la pondération d'un seul facteur ou par des considérations d'ordre économique ou de profit.

Le résultat de cette classification donne lieu à trois (03) niveaux de risque :

- **Risque faible** : risque auquel les règles professionnelles normales s'appliquent
- **Risque moyen ou modéré** : les risques modérés sont au-dessus du risque faible ou normal et mérite une attention plus soutenue mais n'atteignent pas le niveau de risque élevé.
- **Risque élevé** : ces risques sont significatifs mais n'entraînent pas nécessairement d'interdiction. Pour réduire les risques élevés, l'entreprise devrait appliquer des contrôles plus stricts.

Les mesures de vigilance associées à ces niveaux de risques s'appliquent comme suit :

- Pour un risque faible, la mesure de surveillance allégée doit s'appliquer ;
- Pour un risque moyen ou modéré, la mesure de surveillance normal doit s'appliquer ;
- Pour un risque élevé, la mesure de surveillance continue et renforcée doit s'appliquer.

La BDU-CI doit procéder au moins une fois l'an, à une analyse et une évaluation du système de classification des risques BC/FT/FP ou en cas de changements significatifs de la situation de l'établissement en particulier elle identifie et évalue les risques de BC/FT/FP inhérents :

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



Cette évaluation des risques est réalisée préalablement au lancement ou à l'utilisation de ces produits, pratiques et technologies. Les personnes assujetties instaurent des mesures appropriées pour gérer et atténuer ces risques.

Les évaluations des risques sont documentées, tenues à jour et mises à la disposition l'autorité compétente concerné.

VII. VIGILANCE A L'EGARD DE LA CLIENTELE

Conformément aux dispositions de l'article 16 de l'Ordonnance N°2023-875 du 23 novembre 2023, avant d'entrer en relation d'affaires avec un client ou de l'assister dans la préparation ou la réalisation d'une transaction, la Banque est tenue d'observer les conditions préalables à l'entrée en relation d'affaires à savoir :

- identifier leurs clients, y compris les clients occasionnels et les bénéficiaires effectifs de la relation d'affaires, par des moyens adaptés ;
- vérifier les éléments d'identification collectés auprès de leurs clients, sur présentation de tout document obtenu de sources fiables et indépendantes ;
- recueillir et d'analyser les éléments d'information nécessaires à la connaissance de leur client ainsi que l'objet et la nature de la relation d'affaires, pour évaluer le risque de BC/FT/FP.

Les Chef d'agences, les chargés d'affaires et les chargés de clientèle doivent connaître leurs clients en procédant de façon rigoureuse à leur identification lors de l'entrée en relation d'affaires.

La vigilance doit s'exercer à tout moment de la vie de la relation avec le client. Elle s'applique en effet lors de l'entrée en relation et se poursuit dans la gestion quotidienne des comptes de la clientèle. A ce titre elle concerne aussi bien le comportement de la relation que l'ensemble des transactions en cours d'initiation et celles initiées et traitées.

a) Personnes Physiques

Lors de l'ouverture d'un nouveau compte, le gestionnaire de comptes s'assure de l'identité du client par la présentation d'un document d'identité officiel, qu'elle soit résidente ou non résidente délivrée par une autorité ivoirienne habilitée ou une autorité étrangère reconnue, en cours de validité comportant sa photographie. *✓*



- **La fiche d'ouverture de compte doit comporter les informations suivantes :**
- Le(s) prénom(s) et le nom ; ainsi que les noms et prénoms de ses parents ;
- La date et lieu de naissance ;
- La nationalité ;
- La photographie du client ;
- Le numéro de la carte d'identité nationale et sa durée de validité pour les nationaux ;
- Le numéro de la carte consulaire ou carte de résident et sa validité pour les étrangers résidents ;
- Le numéro du passeport ou de toute autre pièce d'identité en tenant lieu et sa durée de validité pour les étrangers non-résidents ;
- L'adresse géographique exacte du domicile privé et professionnel ;
- La profession ;
- Le secteur d'activité ;
- Le revenu régulier ;
- Le numéro d'immatriculation au registre de commerce, pour les personnes physiques ayant la qualité de commerçant ainsi que le centre d'immatriculation ;
- Le numéro de la patente et de l'enseigne commerciale ;
- Les éléments d'identification ci-dessus doivent également être recueillis auprès des personnes qui pourraient être amenées à faire fonctionner le compte d'un client en vertu d'une procuration.

La fiche d'ouverture de compte ainsi que les photocopies des documents d'identité présentés doivent être classées dans le dossier client.

Si le postulant dispose d'autres comptes ouverts sur les livres de la BDU-CI, se renseigner sur les raisons pour lesquelles la demande d'ouverture d'un nouveau compte est formulée.

- **Contrôle de régularité des informations communiquées :**

A partir de ces documents, il est indispensable de procéder à des contrôles de régularité à travers les actions indicatives suivantes :

- Rapprocher la signature apposée sur la pièce d'identité de celle déposée par le client (spécimen de signature) ;
- Examiner attentivement les anomalies éventuelles sur les rivets attachant la photo d'identité, le timbre éventuel en relief, les gommages, grattages, surcharges ;



- Vérifier s'il y a concordance entre les données figurant sur les documents et l'apparence physique de la personne qui les présente.
- Eviter les notions vagues du genre : **Homme d'affaires, Dirigeant de Société...**
- Etablir clairement l'origine des ressources du client : bulletin de salaire (salarié), estimation du revenu annuel, etc.
- Mentionner les contacts du client dans la Banque, et le nom de l'exploitant qui l'aurait éventuellement démarché.

L'entretien doit servir à l'élaboration d'un compte rendu qui permet une catégorisation des clients selon leur profil risque.

Une lettre de bienvenue est envoyée à tout nouveau client personne physique pour s'assurer de l'exactitude de son adresse postale.

En cas d'adresse erronée, il faut s'assurer par tous les moyens de l'exactitude de l'adresse (Quittance récente d'eau ou d'électricité, etc.). L'adresse doit périodiquement être confirmée et mise à jour en cas de changement conformément à l'article 16 de l'Ordonnance n°2023-875 du 23 novembre 2023 relative à la LBC/FT/FP. A défaut, l'Agence peut décliner l'entrée en relation et procéder à la clôture du compte.

Il convient, par ailleurs, d'être particulièrement vigilant, lorsque :

- Le client fait élection de domicile chez un tiers, sans pouvoir fournir d'explications plausibles ;
- Le client n'habite pas sur le secteur géographique de l'Agence ;
- Les adresses de correspondance ou de chéquier sont distinctes de l'adresse fiscale ;
- L'adresse donnée est une adresse d'hôtel ou située dans un pays ou territoire non coopératif désigné par le GAFI.

Pour les ressortissants des Pays et Territoires Non Coopératifs (PTNC) : les ouvertures doivent être soumises à l'**approbation** de la Direction Générale sur avis de la Conformité. **Toute opération en destination des Pays et Territoires non Coopératifs (PTNC) doit-être exécuté dans la limite des mesures prises par les organismes internationaux.**

Des documents illicites ou **contrefaçons** pouvant être présentés à l'agent en charge de l'ouverture des comptes qui doit faire **preuve de perspicacité** et d'attention lors de l'examen des pièces (nouveau client) ou de la mise à jour des dossiers clientèles (clients anciens). Il devra observer la démarche suivante : ✓



Pour les Personnes Politiquement Exposées et la clientèle à haut risque :

L'autorisation de la haute direction est requise avant de nouer une relation d'affaires ou de réaliser une opération avec ou pour le compte d'une PPE de nouer une relation d'affaires ou de réaliser une opération avec ou pour le compte d'une PPE (Article 29).

La décision d'ouverture de compte est donc du seul ressort de la Direction Générale.

Les PPE sont confrontées à des risques de corruption, de détournement de fonds, de pot de vin notamment dans les pays exposés à des problèmes de gouvernance où la corruption est répandue, que de telles personnes abusent de leur pouvoir ou de leur statut en vue de s'enrichir personnellement. Par conséquent des mesures de surveillance continue et renforcées doivent être assurée.

Lors de la collecte d'information en vue de l'ouverture de compte pour un client, s'il s'avère que ce client est une personne politiquement exposée, des informations doivent être collectées sur l'origine de son patrimoine et l'origine de ses fonds conformément aux articles 19 et 29 de la loi sur la LBC/FT/FP avant de soumettre le dossier à l'autorisation du Directeur Général après avis du Responsable chargé de la conformité qui enregistre ledit client dans la base des PPE.

Les opérations effectuées sur les comptes des PPE font l'objet d'une surveillance continue et renforcée et un examen approfondi de l'origine des fonds est réalisé au moins une (01) fois par an afin de s'assurer que les critères de maintien du compte sont toujours respectés.

Par ailleurs, il est important de préciser que le profil des clients identifiés comme PPE fait l'objet d'une réévaluation tous les trois ans par la BDU CI. Sur la base des résultats de cette évaluation, Nous décidons de mettre à jour leur liste des PPE.

Dans le cas où des opérations effectuées par les PPE semblent suspect, elles doivent être immédiatement signalées au Responsable de la Conformité. En cas de soupçon, elles effectuent une déclaration d'opération suspecte à la CENTIF.

Une mise à jour régulière de la base clientèle est primordiale quant à l'identification et le suivi quotidien de clients sensibles.



Identification à distance :

Le contact personnel et direct du client avec la Banque facilite l'identification. Par conséquent, une prise de contact à distance justifie une attention particulière.

L'identification à distance (courrier, e-mail) n'est possible qu'à la condition qu'aucun motif raisonnable ne laisse penser que le contact direct (face à face) est évité afin de dissimuler l'identité véritable du client et qu'aucun blanchiment de capitaux ne soit suspecté.

Si le client réside dans une localité où la Banque dispose d'un bureau, ou d'une représentation, il devra se présenter au guichet de cette représentation, muni de toutes les pièces officielles justifiant son identité.

b) Personnes Morales et les constructions juridiques

Pour les clients qui sont des personnes morales ou des constructions juridiques, l'exploitant doit comprendre la nature de leur activité ainsi que leur structure de propriété et de contrôle. Il doit identifier et vérifier l'identité de la personne morale ou de la construction juridique et des bénéficiaires effectifs en obtenant les informations suivantes :

- la raison sociale;
- la forme juridique;
- la liste des dirigeants et actionnaires ou associés ;
- les éléments d'identification visés à l'article 5 de l'Instruction 003-03, des personnes physiques habilitées à représenter la personne morale concernée vis-à-vis des tiers ou à agir en son nom en vertu d'un mandat;
- l'adresse du siège social ou celle du lieu où sont prises les décisions stratégiques nécessaires à la conduite des affaires de la personne morale, si celle-ci est différente de l'adresse du siège social;
- la liste des bénéficiaires effectifs;
- le numéro national d'immatriculation, d'enregistrement, du Registre du Commerce et du Crédit Mobilier ou d'identification fiscale, le cas échéant.

La fiche d'ouverture de compte doit contenir, selon la nature juridique de l'entreprise, l'ensemble ou certains des éléments d'identification ci-après :

- La dénomination et ou l'enseigne commerciale ;
- La forme juridique ;
- L'activité ;



- L'adresse du siège social ;
- Le numéro de l'identifiant fiscal, le numéro d'immatriculation au Registre du Commerce ;
- Le numéro de la patente ;
- Une pièce d'identité des personnes habilitées à faire fonctionner le compte ;
- Le nom et prénoms des parents des personnes habilitées à faire fonctionner le compte.
- Les noms des dirigeants et les personnes mandatées pour faire fonctionner le compte.

Cette fiche est conservée dans le dossier client ainsi que les documents complémentaires en fonction de sa forme juridique, ci-après précisés :

- La copie certifiée conforme du statut
- La copie du RCCM datant de moins de 3 mois.
- La publicité légale relative à la création de la société et aux éventuelles modifications statutaires ;
- Les procès-verbaux des délibérations des assemblées générales ou des associés ayant nommé les administrateurs ou les membres du conseil de surveillance ou les gérants ;
- Les états de synthèse de l'exercice écoulé ;

L'identification d'une personne morale s'effectue par la production de documents attestant d'une part, son existence juridique, et d'autre part les pouvoirs des personnes agissant en son nom.

La Banque devra s'assurer de l'activité réelle de l'entreprise (volume d'affaires et secteur), ainsi que de la cohérence de cette activité avec l'objet social déterminé dans les statuts.

De même, les relations d'affaires de la société devront être connues : principaux fournisseurs et clients, éventuels liens économiques avec d'autres acteurs.

La Banque devra avoir connaissance des principaux critères financiers de l'entreprise : chiffre d'affaires, surface financière, états financiers...

Des informations doivent également être recueillies pour connaître les antécédents et autres relations bancaires de la société.

*****Règles concernant à la fois les personnes physiques et les personnes morales*****

Un compte-rendu d'entretien est établi avec le client **afin de recueillir tous les renseignements et documents utiles relatifs à ses activités et à l'environnement dans lequel il opère.** Ce compte-rendu est classé dans le dossier du client.



Lors de l'ouverture de comptes, une recherche doit être à partir des nom et prénoms des personnes physiques (client, bénéficiaire effectif, Client occasionnel), du nom commercial des personnes morales est effectuée dans l'application **SIRON KYC** afin de s'assurer qu'ils ne figurent dans aucune des listes (PPE) et des listes noires (OFAC, ONU, UE et autres listes).

Toute ouverture de compte fait l'objet de l'établissement d'une fiche KYC qui récapitule les données essentielles recueillies. Cette fiche est soumise à l'avis préalable du Responsable chargé de la Conformité au sein de la Banque.

S'agissant des professions réglementées (avocats, notaires, agents immobiliers, etc.) qui effectuent des opérations pour le compte de leur client, l'établissement financier peut adopter des règles analogues à celles applicables aux organismes financiers.

Si les renseignements obtenus ne permettent pas d'avoir une certitude sur l'identité véritable des personnes au bénéfice desquelles le compte est ouvert ou l'opération réalisée, la Banque doit refuser d'ouvrir le compte ou d'effectuer l'opération.

Le tableau ci-dessous liste les éléments à recueillir au minimum pour connaître son client :

Informations – client personne morale	Informations – client Personne Physique
Identité de l'entité, actionnariat, bénéficiaires effectifs	Identité du client, situation familiale
Activité réelle (cohérence avec l'objet social), positionnement par rapport à la concurrence	Profession , employeur.
Historique , antécédents économiques	Antécédents , patrimoine, origine d'une fortune
Relations d'affaires de l'entité : principaux clients, fournisseurs, éventuels liens économiques avec d'autres acteurs.	Relations , entourage.
Chiffre d'affaires (plausibilité économique), surface financière, ...	Situation financière : sources de revenus (justificatifs tels que bulletins de salaires, fiche d'imposition, ...), charges, endettement.

Il convient de souligner que les informations collectées lors de l'entrée en affaires avec un client doivent être actualisées tout au long de la relation bancaire avec ce client.

Les documents produits doivent être en originaux ou à défaut des photocopies dûment certifiées conformes par les autorités compétentes d'une durée de moins de 3 mois.

La Banque devra en outre s'assurer :



- de la localisation précise de l'affaire ;
- de l'identité des personnes habilitées à agir au nom de la société ainsi que de celles de tous les principaux dirigeants et actionnaires ;
- que l'activité réelle de l'entreprise correspond bien à son objet social.

Les informations relatives à la surface financière : patrimoine, revenus, chiffres d'affaires etc.... seront recueillies et mises en parallèle avec la nature de l'activité.

Les soupçons et incohérences perceptibles découlant de ce contrôle devront être remontés à la hiérarchie supérieure.

L'identification à distance des personnes morales est du seul ressort de la Direction de la conformité avec accord de la Direction Générale.

c) Clients occasionnels

Le client occasionnel se définit comme toute personne non-cliente du guichet auquel elle s'adresse, ni d'un autre guichet de la Banque, demande à effectuer une opération, quelle qu'en soit la nature ou à retirer des fonds ou des valeurs mis à sa disposition.

Les diligences ci-après exposées sont à effectuer également à l'égard des clients occasionnels qui souhaitent louer un coffre ou effectuer une opération quelconque :

- ✓ La trace de l'identité du client occasionnel doit être mentionnée sur la pièce comptable ou agrafée à celle-ci.
- ✓ Ne doit pas être considérée comme client occasionnel, la personne qui se présente dans une agence où elle est inconnue, mais dont on peut s'assurer qu'elle possède un compte dans une autre agence de la BDU-CI. Toutefois, pour les personnes non titulaires de comptes, notamment les tiers déposants qui sont bien connus de l'agence et qui y opèrent régulièrement, il suffira de s'être assuré une première fois de leur identité et, par la suite, de relever leur nom sur les pièces à conserver. Aucune vérification d'identité n'est évidemment nécessaire pour les remises de chèques régulièrement libellés et endossés (par courrier, dépôt de nuit, remise au guichet...).

d) Bénéficiaires effectifs

Pour les clients qui sont des personnes morales, la Banque doit identifier et prendre des mesures raisonnables pour vérifier l'identité des bénéficiaires effectifs en obtenant les informations suivantes :



- a) l'identité de la ou des personnes physiques qui détiennent, en dernier lieu, une participation de contrôle dans la personne morale;
- b) l'identité de la ou des personnes physiques exerçant le contrôle de la personne morale par d'autres moyens, lorsque:
 - il existe des doutes suite à la vérification prévue au point a) du présent alinéa, quant au fait de savoir si les personnes ayant une participation de contrôle sont les bénéficiaires effectifs ;
 - aucune personne physique n'exerce de contrôle sur la personne morale au travers d'une participation;
- c) l'identité de la personne physique pertinente qui occupe la position de dirigeant principal, lorsqu'aucune personne physique n'est identifiée dans le cadre de la mise en œuvre des exigences prévues aux points a) ou b)

Pour les clients qui sont des constructions juridiques, la Banque doit identifier les bénéficiaires effectifs et prendre des mesures raisonnables pour vérifier l'identité de ces derniers au moyen des informations suivantes :

- a) pour les fiducies, l'identité du constituant de la fiducie, du ou des fiduciaires, du protecteur, des bénéficiaires ou de la catégorie de bénéficiaires et de toute autre personne physique exerçant en dernier lieu un contrôle effectif sur la fiducie, y compris au travers d'une chaîne de contrôle ou de propriété;
- b) pour d'autres types de constructions juridiques, l'identité des personnes occupant des positions équivalentes ou similaires à celles énumérées au point a) du présent alinéa.

La Banque identifie et vérifie l'identité du ou des bénéficiaires effectifs de son client à partir d'un fichier interne retraçant notamment les noms et prénoms, la participation au capital, le droit de vote ainsi que leurs pourcentages de contrôle.

Elle vérifie l'exactitude de la liste des bénéficiaires effectifs fournie par son client en consultant le registre visé à l'article 122 de la Loi uniforme relative à la LBC/FT/FP.

Dans le cas où la consultation du registre évoqué au présent article ne permet pas à l'institution financière de vérifier l'exactitude de la Liste des bénéficiaires effectifs fournie par son client, elle peut procéder à cette vérification par tout autre moyen fiable en appliquant une approche fondée sur les risques.



e) Les Correspondants Bancaires hors UMOA

Préalablement à l'entrée en affaires avec un correspondant bancaire en dehors de l'UMOA, une fiche de recueil d'informations, lui est adressée conformément à l'article 13 de l'instruction 001/03/2025, stipule que afin d'assurer la mise en œuvre des obligations relatives aux relations de correspondance bancaire transfrontalière et aux autres relations similaires prévues à l'article 31 de la Loi uniforme relative à la LBC/FT/FP, l'institution financière peut recourir aux outils et principes développés par d'autres juridictions, groupements ou associations notamment le GAFI, sous réserve qu'ils incluent la collecte des informations minimales, mentionnées dans le questionnaire figurant à l'Annexe 1 de la présente Instruction.

A cet effet, le questionnaire comporte les renseignements suivants :

- Actionnariat et structure du capital ;
- Nom et adresse de l'établissement ;
- Structure de lutte anti-blanchiment ;
- Nom et contacte du responsable LBC/FT/FP ;
- Liste des membres des organes de direction ;
- Catégories des clients de l'établissement ;
- Autorité de tutelle ;
- Activités principales et clientèle ;
- Législation et procédures de prévention du blanchiment des capitaux et du financement du terrorisme.

Ce document dûment renseigné doit être validé par la Direction Générale ou Organe équivalent du correspondant.

Réciproquement, la Banque veille au respect des normes internationales et souscrit aux questionnaires relatifs à la lutte contre le blanchiment des capitaux, le financement du terrorisme et les sanctions économiques (Wolfsberg) qui lui sont communiqués par les correspondants. Ces questionnaires sont renseignés par le Responsable de la Conformité et validés par l'Autorité compétente indiquée.

Toute nouvelle relation doit être soumise systématiquement à l'accord de la Direction Générale.

La BDU-CI doit évaluer le dispositif de contrôle en matière de LBC/FT/FP mis en place par leur(s) correspondant(s) bancaire(s).

Elle doit également s'assurer que :



- Les correspondants sont assujettis à une réglementation en matière de LBC/FT/FP au moins équivalente à celle applicable en Côte d'Ivoire.
- Leurs dispositifs de vigilance font régulièrement l'objet de contrôle de la part de l'autorité de supervision dont ils relèvent.

A l'occasion de chaque entrée en relation d'affaires ou de mise à jour du dossier KYC, un questionnaire AML doit être transmis aux correspondants. Il peut être également remplacé par le questionnaire Wolfsberg dûment renseigné de la part du partenaire bancaire.

*****Remarque importante :**

En application des résolutions N° 1214, 1267, 1333 et 1363 de l'Organisation des Nations Unies, la BDU-CI ne doit établir aucune relation commerciale avec les organismes ou individus cités dans les listes noires.

Toute personne identifiée dans une liste noire lors d'une transaction quelconque avec la Banque (ouverture de comptes, virements émis ou reçus) doit être signalée aux autorités de tutelle sous signature du Responsable de la Conformité et de la Direction Générale. Les comptes éventuellement existants de cette personne doivent également être bloqués **sans délai**.

f) Cas spécifiques

Les documents énumérés pour les spécifiques ci-après doivent être exigés dans à l'entrée en relation d'affaires :

- **Les sociétés en formation :**
 - ✓ la remise du certificat négatif,
 - ✓ le projet des statuts
 - ✓ les éléments d'identification des fondateurs
 - ✓ et des souscripteurs du capital **ainsi que les sommes versées par chacun d'entre eux.**
- **Les associations :** Les documents complémentaires devant être fournis par les associations incluent :
 - ✓ Les statuts mis à jour ;
 - ✓ Le récépissé de déclaration (Le récépissé de dépôt ne vaut pas déclaration. Pendant un délai de deux mois à compter du dépôt de la déclaration, l'association ne peut exercer aucune activité) ; ✓



- ✓ Les procès-verbaux de l'assemblée générale constitutive portant élection des membres du bureau, du président et la répartition des tâches au sein du bureau, ainsi que la durée du mandat ;
- ✓ Les noms des dirigeants et les personnes mandatées pour faire fonctionner le compte bancaire ;
- ✓ Document d'identité des dirigeants et ceux de leurs parents, des bénéficiaires effectifs et des personnes habilitées à signer sur le compte.

- **Les coopératives** : Les documents complémentaires devant être fournis par les coopératives incluent
 - ✓ Les statuts mis à jour ;
 - ✓ Liste des membres, leurs identités ainsi que leur profession ;
 - ✓ Le procès-verbal de l'assemblée générale constitutive ;
 - ✓ L'acte portant nomination des personnes habilitées à faire fonctionner le compte ;
 - ✓ La décision portant agrément de la constitution de la coopérative.

- **Les mutuelles** : Les documents complémentaires devant être fournis par les coopératives incluent :
 - ✓ Copie de l'attestation d'immatriculation de la mutuelle délivrée par l'Agence Ivoirienne des Régulation de la Mutualité Sociale (AIRMS) ;
 - ✓ Une copie des Statuts légalisée ;
 - ✓ Une copie du règlement intérieur ;
 - ✓ Le procès-verbal de l'assemblée générale constitutive portant élection des membres du bureau, du président et la répartition des tâches de chaque membre du bureau ;
 - ✓ Les noms des dirigeants et personnes mandatés pour faire fonctionner le compte bancaire ;
 - ✓ Une copie de la pièce d'identité valide du ou des signataires.

g) Cas des établissements publics et autres entités :

Les documents complémentaires devant être fournis par les établissements et autres entités publiques incluent :

- ✓ L'acte constitutif ;



- ✓ Les actes portant nomination des représentants ou fixant les pouvoirs des différents organes de l'établissement ;
 - ✓ Les noms des personnes habilitées à faire fonctionner le compte ;
 - ✓ Autorisation d'ouverture du compte par l'autorité de l'établissement public
 - ✓ Identité du représentant légal, des signataires et de l'autorité de l'établissement public
- Pour les autres catégories de personnes morales (groupement d'intérêt économique, groupement d'intérêt public, société anonyme simplifiée, etc....), l'exploitant devra exiger les éléments complémentaires d'identification spécifiques en se référant aux textes législatifs qui les régissent.

*****Les points de vigilance à observer quant à l'identification des clients.**

Les points ci-dessous doivent faire l'objet d'attention par rapport à la régularité apparente des documents fournis sous peine de rejet :

- ✓ La concordance des informations fournies avec les documents présentés.
- ✓ L'existence de compte (en cours ou clôturé) au nom du client et son historique le cas échéant.
- ✓ L'objet réel de la société, et ne pas se contenter de l'objet social indiqué dans les statuts
- ✓ La fiabilité des informations contenues dans les états financiers fournis, qui doivent être certifiés le cas échéant par le commissaire aux comptes, ou par le représentant légal de la société à défaut.

Cas des banques correspondantes : Pour les correspondants bancaires, et sur la base d'informations publiquement disponibles, vérifier si la relation a fait l'objet d'une enquête ou d'une intervention de l'autorité de surveillance.

Une attention particulière doit être réservée aux personnes agissant pour le compte d'autrui, les mandataires, les prête-noms et les sociétés écrans.

Les mandataires pour les sociétés de tout type, il faudrait s'assurer des pouvoirs des personnes habilitées à faire fonctionner le compte :

- A l'occasion de mouvements inhabituels (en montant et en complexité), vérifier la validité des pouvoirs.
- En cas de doute, déclencher la procédure de déclaration d'opération inhabituelle (voir procédure). ✓



Les sociétés écrans : Il s'agit de sociétés dotées de la personnalité juridique qui peuvent exercer une activité, ou plus généralement, présenter le caractère de simple boîte aux lettres, utilisée pour opérer dans d'autres pays, étant entendu qu'il sera très difficile d'identifier les personnes qui se cachent derrière les sociétés en question. L'existence de soupçons quant à une société écran doit motiver le refus de l'ouverture du compte. Au cas où des faits se seraient avérés, alors que le compte est déjà ouvert, les diligences relatives à la déclaration d'opération inhabituelle doivent être accomplies.

VIII. SURVEILLANCE DES OPERATIONS

Dans le cadre de la complémentarité des contrôles, les Agences, Départements et Directions opérationnels qui initient ou traitent des opérations sont concernés en premier lieu et "en temps réel" par le devoir de vigilance et la lutte contre le blanchiment de capitaux ou le financement du terrorisme. Pour ce faire, toute opération qui se présente dans des conditions inhabituelles de complexité et ne paraît pas avoir de justification économique ou d'objet licite apparent, doit faire l'objet d'une attention particulière. Ces opérations peuvent comporter plusieurs indices notamment :

- Un manque de cohésion avec le volume, la nature de l'activité ou les opérations précédentes
- Un fractionnement d'une opération sans justification.
- Des opérations bancaires et commerciales très complexes.
- L'utilisation des paradis fiscaux et de zones off-shore.
- L'utilisation anormale d'argent en espèces et moyens de paiement équivalents sans justification.
- L'utilisation soutenue du coffre-fort.

Pour ces opérations ; il faudra :

- Se renseigner sur l'origine et la destination des sommes en jeu ainsi que l'identité des bénéficiaires.
- Consigner les caractéristiques des opérations dans un document à conserver.
- Déclarer l'opération à la Direction de la Conformité.

Par ailleurs, deux types de détection se présentent : les détections à priori qui concernent essentiellement les opérations en espèces, les remises de chèques, les virements, prélèvements, les placements et les détections à posteriori.



a) Détections à priori :

Dans le cas où l'opération en cours ne semble pas isolée, il convient de se renseigner sur le montant total de la transaction ainsi que sur les canaux de versement (Virements, Chèques, mise à disposition...). Une opération atypique (Montant, complexité...), sur un compte ayant un profil de fonctionnement bien défini, nécessite une justification complète.

i. Les opérations en espèces

Les opérations en espèces sont incontournables dans la chaîne de blanchiment des capitaux issus d'activités illicites.

Avant de traiter une opération douteuse, l'exploitant recueille toutes les informations quant à l'origine des fonds et à leur utilisation. L'opération sera déclarée par les opérationnels si les justificatifs ou les explications semblent superficiels, contradictoires ou ne correspondent pas à l'appréciation qui s'en dégage.

Les versements doivent être en adéquation avec la nature de l'activité de l'opérateur et le profil des clients, de même qu'il y a lieu de justifier les versements ou les retraits anormaux et répétitifs.

La surveillance particulière des opérations suivantes est recommandée :

- Tout paiement en espèces ou par titre au porteur d'une somme d'argent, effectué dans des conditions normales, dont le montant unitaire ou total est égal ou supérieur à cinquante millions (50.000.000) de francs CFA ;
- Toute opération portant sur une somme égale ou supérieure à dix millions (10.000.000) de francs CFA effectuée dans des conditions inhabituelles de complexité ou injustifiées paraissant ne pas avoir de justification économique ou d'objet licite.

Espèces contre espèces

- Echange d'importantes quantités de pièces ou de petites coupures contre des coupures de valeur plus élevée ;
- Opérations de change fréquentes ou importantes à partir d'espèces.

Dépôts d'espèces

- Importants dépôts d'espèces effectués par une personne ou une société dont l'activité ne devrait pas générer des revenus de ce type ;



- Accroissement substantiel des dépôts en espèces par toute personne ou société sans cause réelle, notamment si ces dépôts sont transférés rapidement vers une destination sans rapport avec l'activité du client ;
- Dépôts fréquents d'espèces, de montant unitaire faible, mais dont le total est significatif (fractionnement) ;
- Dépôts d'espèces pour couvrir des demandes de chèques bancaires, des transferts d'argent ou autres instruments monétaires négociables et immédiatement réalisables ;
- Dépôts d'espèces suivis de retraits, par un particulier ou une société, dont l'activité donne lieu habituellement à des paiements ou transferts de fonds au moyen de chèques, virements ou autres moyens de paiement scripturaux ;
- Accroissement significatif et sans cause apparente des dépôts en espèces (ou en valeurs négociables) sur le compte d'un client, si ces dépôts sont rapidement transférés vers des comptes ouverts dont les détenteurs ne sont pas en relation habituelle avec ledit client.

Retraits d'espèces

- Transferts d'importantes sommes d'argent vers ou à partir de pays étrangers, assortis de demandes de paiement en argent liquide ;
- Dépôts et retraits de sommes élevées excédant largement le chiffre d'affaires d'une société ou les revenus d'un particulier ;
- Entrées et sorties fréquentes d'espèces sur le compte d'un particulier dont la profession déclarée (employé de bureau ou fonctionnaire par exemple) ne justifie pas ces multiples opérations ;
- Retraits en espèces sur un compte « dormant » ou sur un compte qui vient juste de recevoir un important crédit inattendu, notamment en provenance de l'étranger.

ii. Les remises de chèques

Les vérifications habituelles sont de rigueur. Les chèques de tiers présentent l'avantage de désigner nommément le tireur. En cas de doute, noter l'objet économique pour toute remise dépassant le profil du client. Les chèques étrangers des pays et territoires non coopératifs (PTNC) doivent faire l'objet d'une attention particulière, et préalablement soumis à l'accord écrit de la hiérarchie.

iii. Les virements/prélèvements

Ils sont généralement identifiés et sont appliqués uniquement quand l'identité de l'ordonnateur est clairement définie et qu'elle n'est pas de relations avec une des entités visées pour ses



activités répréhensibles. Par rapport aux virements/ prélèvements en provenance de PTNC, ils seront analysés et ne seront appliqués qu'après accord du Directeur. Quant aux mouvements d'aller-retour isolés ou cumulés, ils doivent être surveillés dès l'instant où ils sont disproportionnés par rapport au profil du client.

iv. Les placements

Hormis l'origine des fonds, l'attention doit être portée sur toutes les opérations de placement du client en inadéquation avec son profil. Le mode d'utilisation peut également donner de précieuses indications quant à un éventuel blanchiment ou autres activités douteuses.

b) Détections à posteriori

- Les ouvertures de compte sont soumises systématiquement à une validation du responsable hiérarchique,
- Les opérations filtrées par seuil d'alerte sont vérifiées par l'opérationnel, celles qui sont douteuses sont systématiquement déclarées à la DCPC.
- Les mouvements d'aller-retour isolés ou cumulés doivent être surveillés dès l'instant où ils sont en inadéquation avec le profil du client.

En outre, une surveillance particulière doit être assurée sur les comptes et opérations des personnes étrangères, exerçant ou ayant exercé des fonctions publiques de haut rang, ainsi que sur les comptes et opérations des clients ressortissants de pays ne disposant pas d'une réglementation en matière de LBC/FT/FP.

Toutes les opérations en provenance et surtout à destination des pays sous embargo doivent faire l'objet d'une surveillance renforcée.

c) Autres opérations à surveiller

Les guichetiers payeurs et les Chefs d'Agence, ainsi que tout le personnel de la Direction des Opérations avec l'Etranger, Direction de la Comptabilité, la Direction de la Trésorerie, la Direction de l'Exploitation et autres membres du personnel en général, doivent être vigilants vis-à-vis des opérations suivantes :

- Les mouvements d'espèces importants ou répétés y compris le change ;
- Les transferts internationaux notamment par SWIFT à destination ou en provenance de pays à risque ou de territoire considéré comme non coopératif ;
- Les opérations qui par leur nature ou leur montant, ne semblent pas en rapport avec le revenu ou le patrimoine du client, avec ses activités professionnelles ou commerciales, ou encore avec ses habitudes.



- Des opérations effectuées par le personnel pour le compte de tiers (procéder à la formalisation de la surveillance).

Il convient également d'être attentif aux :

- Fonctionnements des nouveaux comptes dont certains pourraient n'être ouverts que pour enregistrer une opération ponctuelle de nature frauduleuse,
- Mouvements démesurés de fonds par rapport au solde du compte,
- Engagements garantis par des dépôts d'espèces,
- En cas de remboursements anticipés ou inattendus de prêts il faut vérifier l'origine des fonds.
- Lorsqu'un client bénéficiaire d'un crédit offre en garanties des biens ou des fonds, il faut vérifier l'adéquation de leur valeur avec les revenus ou le patrimoine déclaré de ce dernier.
- En cas de remboursement par un tiers, il faut vérifier les relations qui existent entre le débiteur et le tiers concerné et s'assurer des motivations de cette opération.

Opérations sur les comptes bancaires

- Mouvements très fréquents sur un compte (dépôts, retraits, virements) sans rapport évident avec la situation, l'activité du titulaire (personne ou société) ;
 - Apparition de dépôts et/ou retraits en espèces sur un compte de particulier ou de société dont l'activité donne lieu habituellement à des mouvements scripturaux ;
 - Apparition de mouvements significatifs sur un compte « dormant » ;
 - Ouverture d'un compte, suivie de mouvements créditeurs importants, puis, dans un court laps de temps, du transfert de ces sommes vers d'autres banques locales ou étrangères, de la clôture ou de l'interruption de son fonctionnement ;
 - Transferts de fonds vers des comptes numérotés ou des comptes domiciliés dans des paradis fiscaux ;
 - Apparition sur le compte de mouvements relatifs à des chèques ayant fait l'objet d'endos successifs ;
 - Existence de plusieurs comptes et versements d'argent liquide sur chacun de ces comptes, représentant une somme globale importante ;
 - Compte d'une personne ou d'une société qui ne révèle en fait aucune activité professionnelle normale ou en rapport avec les affaires de la personne ou de la société,
- 



mais qui est utilisé pour recevoir ou retirer des sommes importantes qui n'ont aucun rapport évident avec la situation du titulaire du compte et/ou avec ses activités ;

- Dépôt de chèques étrangers (endossables) importants, endossés par des tiers au profit d'un client ;
- Importantes transactions en argent liquide ou importantes opérations de changes menées par des clients agissant ensemble et de concert, mais à partir de guichets de banques différentes ;
- Encaissement de chèques au porteur émis à partir de réseaux étrangers ;
- Remise de chèques importants déclarés représenter un « gain de jeu » ;
- Remise, lors de l'ouverture d'un nouveau compte, d'un chèque d'un montant élevé (il sera prudent de prendre une photocopie du chèque) ;
- Virements répétés de montants importants vers l'étranger, avec instruction de payer le bénéficiaire en espèces ;
- Détenzione de multiples comptes par un client, sans motif, nombreux virements de compte à compte.

Opérations bancaires sur valeurs mobilières et autres placements

- Recours des clients au Service de Gestion de patrimoine, alors que l'origine des fonds n'est pas claire ou n'a pas de rapport avec le niveau de vie apparent du client ;
- Paiements de titres en argent liquide pour des montants importants ou inhabituels ;
- Achats ou ventes de titres sans aucun but discernable ou dans des circonstances qui apparaissent inhabituelles.

Opérations liées à une activité internationale off-shore

- Client introduit par une agence étrangère, une filiale ou une autre banque située dans des pays où la production ou le trafic de drogue a une place importante ;
- Utilisation de lettres de crédits et autres méthodes de financement pour faire circuler de l'argent entre différents pays où le client n'a pas ses activités habituelles ;
- Transferts de fonds réguliers et importants (y compris transactions électroniques) dont la justification économique est difficile à identifier, vers des pays communément associés à la production, au traitement ou à la vente de drogue (ou clients qui reçoivent régulièrement des paiements importants en provenance de ces pays) ;



- Constitution de soldes créditeurs importants, incompatibles avec le chiffre d'affaires connu du client et transfert ultérieur vers des comptes à l'étranger ;
- Demandes fréquentes de travellers chèques, de chèques en monnaie étrangère ou autres instruments négociables ;
- Versements fréquents de travellers chèques ou de chèques bancaires en monnaie étrangère provenant en particulier de l'étranger.

Opérations de prêts (garantis ou non garantis)

- Acceptation par le client de crédits à des taux anormalement élevés ;
- Proposition par le client de garanties constituées d'avoirs d'origine inconnue ou incompatibles avec le niveau de vie du client ;
- Demande de prêt garanti par des avoirs détenus par la banque ou par une tierce personne, si l'origine de ces avoirs est inconnue ou si ces avoirs sont incompatibles avec le niveau de vie connu du client ;
- Demande de prêt assorti d'une offre de garantie constituée d'un certificat de dépôt émis par une banque étrangère ;
- Présence dans une structure emprunteuse de personnalités (ou ayants droit économique) connues pour leur moralité douteuse ou leur lien avec des personnes figurant sur les listes des entités terroristes.
- Lorsque ces fonds ou biens ne lui appartiennent pas, est-il vérifié les relations qui lient le client au garant ?"

La vigilance sera étendue aux opérations sur bons et titres anonymes, ainsi que sur l'or :

La banque doit, par la production de tout document écrit probant, s'assurer de l'identité des personnes qui effectuent des opérations (tant à la souscription qu'au remboursement) sur ces supports. Il appartient à la banque d'assurer l'enregistrement et la conservation des références d'identité qu'elle recueille à l'occasion des opérations sur l'or et titres anonymes.

Dans le cas particulier de virements reçus en dollars US ou en provenance de correspondants établis aux Etats-Unis, en faveur de clients de la banque, une plus grande vigilance doit être observée. En effet, en cas d'origine illicite, même après couverture du virement crédité au profit du client, la loi américaine fait obligation aux banques correspondantes de rappeler les fonds douteux ainsi transférés par le débit d'office du compte pendant un délai d'un à trois ans (selon l'Etat de domiciliation du correspondant).



d) Conduites à adopter face aux opérations suspectes.

L'agent en charge de l'opération : Si les indices relevés laissent croire à une tentative de blanchiment, il devra :

1. S'assurer auprès du client sur :

- L'origine et la destination des sommes d'argent en cause ;
- L'objet de la transaction ;
- L'identité des personnes impliquées.

2. Rassembler le maximum d'informations nécessaires tout en restant courtois avec le client qu'il ne cessera d'observer durant le temps de leur entretien.

3. Informer immédiatement sa hiérarchie.

L'agent en charge de l'opération devra :

- Apprécier le caractère licite ou non de l'opération. Au cas où le soupçon s'avérerait fonder, déclarer le soupçon à la Conformité ;
- Consigner les caractéristiques principales de l'opération, l'identité du donneur d'ordre et du bénéficiaire sur une fiche d'incident (annexe n° 1). L'ensemble des fiches seront par la suite enregistrées dans un registre spécial (annexe n° 2) pour des besoins d'investigation en cas de besoin.

Le responsable hiérarchique devra :

- Vérifier la transcription régulière de l'opération suspecte dans le registre spécial anti-blanchiment.
- Informer périodiquement la Direction de la conformité des opérations enregistrées dans ce registre.

L'Analyste Conformité devra :

- Procéder à l'analyse des incidents et s'il y'a lieu informer les autorités légales (CENTIF) dans les formes et délais requis.

➤ La déclaration de soupçon (DS)

Toute opération pour laquelle l'identité du donneur d'ordre ou du bénéficiaire effectif ou du constituant d'un fonds fiduciaire ou de tout autre instrument de gestion de patrimoine d'affectation reste douteuse doit faire l'objet d'une déclaration à la CENTIF.



Une déclaration de soupçon est aussi effectuée à la CENTIF en présence de sommes inscrites dans nos livres ou les opérations portant sur des sommes dont vous soupçonnez ou avez de bonnes raisons de soupçonner qu'elles proviennent d'une fraude fiscale lorsqu'il y a présence d'au moins l'un des critères définis par la réglementation en vigueur conformément à l'article 60 de l'Ordonnance 2023-875 du 23 novembre 2023 relative à la LBC/FT/FP.

La procédure à suivre au cas où une somme ou une opération paraîtrait susceptible de faire l'objet d'une déclaration à la CENTIF ou en cas de demande d'information reçue de la CENTIF devrait être faite dans les formes prévues par l'Arrêté N°391/MEF/CENTIF du 30 octobre 2017 fixant le modèle de déclaration de soupçon.

Aussi, les déclarations de soupçons devront être transmises à la CENTIF par tout moyen laissant trace écrite. Elles peuvent être faites par tout personnel non habilité dans les situations exceptionnelles notamment en cas d'absence du correspondant et son suppléant. Toutefois elles doivent être confirmées par écrit dans un délai de quarante-huit heures par les correspondants CENTIF.

Confidentialité de la déclaration

Il est fait interdiction sous peine de sanctions, de porter à la connaissance du propriétaire des sommes ou de l'auteur d'une opération ayant fait l'objet d'une déclaration de soupçon l'existence de cette déclaration.

Toute indiscretion volontaire sur ce plan sera sévèrement sanctionnée.

e) Surveillance continue du dispositif de vigilance.

Une surveillance continue, dans le cadre de la complémentarité des contrôles, est seule garantie de l'efficacité du dispositif de vigilance. Cette surveillance nécessite un engagement sans réserve des entités de la Banque directement impliquées. Cet engagement est matérialisé par les obligations suivantes :

1. Entités opérationnelles (Agences, Directions et Services)

L'ensemble des entités opérationnelles sont sollicitées afin de veiller à l'application correcte des dispositions de la présente procédure ainsi que les notes y afférentes en ce sens que :

- L'ensemble des responsables doivent sensibiliser leurs collaborateurs ainsi que les nouvelles recrues, afin de les former à l'assimilation des diligences requises ;



- Veiller à la transmission, sans délai, les déclarations documentées pour toutes les opérations inhabituelles.

2. La Direction de la Conformité (DCPC)

La Direction de la Conformité a pour rôle d'assurer une vigilance relevant de la conformité veille à l'application des dispositifs de vigilance, au traitement des déclarations centralisées et à la formation du personnel de la Banque.

Elle intervient dans l'approbation préalable de tous nouveaux produits, services ou applications informatiques, par rapport aux risques de LBC/FT/FP.

La banque identifie et évalue les risques de blanchiment de capitaux ou de financement du terrorisme pouvant résulter :

- Du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution ;
- De l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants. L'évaluation des risques visée ci-dessus, doit avoir lieu avant le lancement des nouveaux produits ou des nouvelles pratiques commerciales ou avant l'utilisation de technologies nouvelles ou en développement. La banque prendra les mesures appropriées pour gérer et atténuer ces risques.

(En référence avec la fiche de fonction conformité).

3. La Direction de l'Audit Interne (DAI) :

L'aspect de vigilance et de la lutte contre le blanchiment de capitaux, financement du terrorisme et de la prolifération des armes de destruction massive est pris en compte lors de chaque mission d'audit ainsi que la revue régulière du dispositif.

Une vigilance particulière doit être également exercée à l'égard des opérations provenant d'institutions financières qui ne sont pas soumises à des obligations suffisantes en matière d'identification des clients ou de contrôle des transactions.

La Banque s'assure que les obligations sont appliquées par ses bureaux de représentation, ses succursales, ou ses sociétés filiales dont le siège est à l'étranger, à moins que la législation locale n'y fasse obstacle, auquel cas, elle en informe la CENTIF.

4. La cellule monétique

Elle est l'entité en charge de la gestion de la procédure d'EER avec les sous agents de transfert rapide. La BDU-CI surveille les opérations de transferts rapides avec les outils acquis auprès



des partenaires en conformité avec les obligations de surveillance des transactions. Aussi, elle veille sur sa relation d'affaires avec les sous agents à travers la mise en œuvre de la procédure d'entrée en relation et le manuel de conformité.

IX. CONSERVATION DES PIECES ET DOCUMENTS

Le devoir de conservation des documents et autres pièces justificatives est une diligence clairement exprimée par l'article 23 de l'ordonnance n°2023-875 du 23 novembre 2023 qui stipule que :<<Sans préjudice des dispositions prescrivant des obligations plus contraignantes, les institutions financières conservent pendant une durée de **dix ans**, à compter de la clôture de leurs comptes ou de la cessation de leurs relations avec leurs clients habituels ou occasionnels, les pièces et documents relatifs :

- a) à l'identité des clients;
- b) à la connaissance du client et de son profil de risque ;
- c) aux analyses réalisées dans le cadre de la mise en œuvre des mesures de vigilance relatives à la clientèle à l'entrée ou pendant la relation d'affaires;
- d) à toute autre information pertinente.

Elles conservent les pièces et documents relatifs aux opérations que ces clients ont effectuées, y compris les livres de comptes et les correspondances commerciales, pendant **dix ans**, après l'exécution de l'opération. Les institutions financières s'assurent que ces pièces et documents permettent la reconstitution d'opérations individuelles.

Les archives doivent être tenues de façon à satisfaire rapidement les demandes d'information des autorités nationales compétentes chargées de la détection et de la répression des infractions liées aux blanchiments de capitaux, au financement du terrorisme et à la prolifération des armes de destruction massive.

Une fréquence d'actualisation du KYC des relations d'affaires peut être mise en place de sorte à ce qu'elle soit adaptée au niveau de risque du client.

Communication des pièces et documents :

Les pièces et documents relatifs aux obligations d'identification prévues aux articles 16, 17, 19, 20 et 21, et dont la conservation est mentionnée à l'article 23, sont communiqués par les institutions financières, sur leur demande, aux autorités judiciaires, aux agents de l'Etat chargés de la détection des infractions de blanchiment de capitaux, de financement de terrorisme et de



la prolifération, agissant dans le cadre d'un mandat judiciaire, aux autorités de contrôle ainsi qu'à la CENTIF.

Nul ne saurait évoquer le secret professionnel pour se soustraire à cette obligation.

Si au bout de 96 heures (4jours) la Banque ne reçoit pas d'opposition de la part du juge d'instruction, il peut exécuter l'opération objet de la déclaration.

Des déclarations à posteriori doivent être faites s'il est établi que des opérations déjà traitées étaient de natures délictueuses.

X. ORGANISATION DU CONTROLE INTERNE

Le contrôle interne mis en place pour prévenir le blanchiment des capitaux, le financement du terrorisme et la prolifération des armes de destruction massive est organisé autour des trois lignes de défense comme suit :

a) 1ère ligne de défense

Celle ligne de défense est composée des métiers opérationnels qui mettent en œuvre les procédures et politiques de la Banque. L'identification et la connaissance de la clientèle est de la responsabilité des exploitants qui les exécutent suivant la procédure en la matière. De même, pour le traitement des opérations de guichet et de virement, des diligences sont mise en œuvre afin de vérifier la provenance et la destination des fonds, l'identité du bénéficiaire, l'identité du donneur d'ordre, etc.

b) 2e ligne de défense

Les fonctions de conformité LBC/FT/FP et de contrôle interne ainsi que la fonction de conformité plus étendue et des départements des ressources humaines et informatiques constituent la seconde ligne de défense. Le Responsable de la cellule LBC/FT/FP est responsable du contrôle permanent de conformité en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et la prolifération des armes de destruction massive y compris la vérification d'échantillons et l'analyse des rapports d'exceptions, qui permettront le signalement d'anomalies et d'autres problématiques à la Direction et si nécessaire au Conseil d'Administration. Il est le point de contact de toutes les problématiques de LBC/FT/FP vis-à-vis des autorités internes et externes et endosser la responsabilité des déclarations des transactions suspectes.



Les responsabilités d’Auditeur interne et de protection des données ne doivent pas être confiées au responsable conformité chargé de la lutte contre le blanchiment des capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive.

c) 3^{ème} ligne de défense

Elle est représentée par la fonction d’Audit Interne qui évalue le dispositif LBC/FT/FP de la banque au moins une fois l’année et rapporte au Comité d’Audit et de Contrôle Interne (CACI). La fréquence des audits est basée sur les risques. La fonction d’Audit Interne doit être assurée par un personnel qualifié possédant un savoir-faire dans ce domaine.

d) Structure d’appui et de conseil : La Direction Juridique et du recouvrement (DJR)

Elle apporte son assistance, d’une manière générale lorsque la tentative de blanchiment à pour fait générateur des documents et instructions présentant à l’analyse une certaine complexité et d’une manière spécifique lorsque le blanchiment consommé devra donner lieu à une poursuite judiciaire. Le service juridique aidera alors le service de la conformité pour la suite de la procédure.

XI. GESTION DE LA CONFORMITE AUX DISPOSITIONS DE LA PRESENTE ORDONNANCE ET DES TEXTES PRIS EN APPLICATION

La Banque De l’Union Côte d’Ivoire s’est engagée à respecter toutes les normes en vigueur applicables aux établissements de crédit et aux compagnies en établissant une politique de conformité conformément à la Circulaire N° 05-2017/CB/C relative à la gestion de la conformité aux normes en vigueur par les établissements de crédit et des compagnies financières de l’UMOA.

XII. PROTECTION DES DONNEES

Dans le cadre de notre politique de Lutte contre le Blanchiment de Capitaux, le Financement du Terrorisme et de la Prolifération des armes de destruction massive, la protection des données personnelles est une priorité essentielle.



Nous nous engageons à respecter les principes de protection des données tels que définis par la loi n°2023-450 du 19 juin 2013 relative à la protection des données à caractère personnel :

- **Collecte de Données** : La collecte des données personnelles est effectuée uniquement à des fins explicites et déterminées, en lien direct avec nos obligations de LBC/FT/FP. Nous veillons à minimiser la quantité de données collectées et à éviter toute collecte excessive.
- **Consentement et Transparence** : Le traitement des données repose sur le consentement des personnes concernées, et est réalisé de manière loyale et transparente. Les individus sont informés de la finalité de la collecte et de l'utilisation de leurs données.
- **Exactitude et Sécurité** : Nous nous assurons que les données collectées sont exactes et mises à jour régulièrement. Des mesures de sécurité appropriées sont mises en place pour protéger les données contre tout accès non autorisé, perte ou divulgation.
- **Conservation Limité** : Les données personnelles sont conservées uniquement pour la durée nécessaire aux fins pour lesquelles elles ont été collectées, conformément aux exigences légales et réglementaires
- **Droits des Personnes** : Nous respectons les droits des individus en matière de protection des données, y compris le droit d'accès, de rectification, de suppression et d'opposition au traitement de leurs données personnelles

Ces principes permettent de concilier nos obligations réglementaires avec le respect des droits et libertés des individus.

XIII. RECRUTEMENT, FORMATION CONTINUE ET L'INFORMATION ET LA SENSIBILISATION DU PERSONNEL

a) Recrutement

Le recrutement du personnel doit prendre en compte les aspects d'identification et de connaissance liés à lutte contre le blanchiment des capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive en incluant les vérifications de références, des contrôles antécédents et potentiellement des évaluations psychologiques pour les postes sensibles. De même qu'une fiche KYC est nécessaire à la connaissance du client, l'établissement d'un fiche KYE (Know Your Employee) est indispensable pour la connaissance du personnel.



b) Formation continue

La Banque doit assurer la formation continue des membres du personnel y compris les membres de l'organe délibérant en vue de les doter des aptitudes nécessaires pour détecter et appliquer les mesures requises pour les opérations et les agissements susceptibles d'être liés au blanchiment de capitaux, au financement du terrorisme et de la prolifération des armes de destruction massive. Le Programme de formation annuelle de banque doit tenir compte du programme de formation de la conformité en matière de LBC/FT/FP.

c) Information et sensibilisation

La banque doit disposer de canaux de communication interne efficaces (intranet, newsletter, réunion, etc.) pour diffuser les informations et les sensibiliser sur la LBC/FT/FP de manière régulière. Les informations et les sensibilisations à communiquer aux membres du personnel sont établies selon une analyse des besoins et sur une approche par les risques découlant des constats des contrôles.

XIV. RESPECT DES SANCTIONS INTERNATIONALES ET EMBARGOS

Le respect des sanctions fait référence à la politique du respect des sanctions et embargo de la banque.

a) Définitions et normes

La notion 'Sanctions Internationales' désigne les sanctions économiques ou financières ciblées telles que les Embargos, Gels des avoirs, sanctions visant certains secteurs économiques et d'autres restrictions pesant sur les transactions avec les cibles de sanctions.

Les Sanctions Internationales sont émises, administrées ou mises en application par le Conseil de sécurité de l'ONU, l'Union européenne, les États-Unis (incluant l'OFAC et le Département d'État américain) et par des autorités locales compétentes.

On distingue alors :

- **L'Embargo** qui désigne une interdiction officielle portant sur les échanges commerciaux avec un pays, un territoire, un gouvernement ou une juridiction.
- **Le Gel des avoirs** qui consiste en l'identification de toute possession sujette à un blocage ou un gel et l'interdiction de toute utilisation ou transfert des avoirs de quelque façon que ce soit sous réserve de l'approbation d'une autorité officielle compétente.



La BDU-CI s'engage à respecter les dispositions législatives et réglementaires relatives aux Sanctions nationales et internationales, a minima celles définies par :

- Organisation des Nations Unies ;
- Union européenne ;
- États-Unis (OFAC et autres).

Lorsque cela est nécessaire, BDU-CI peut être amenée à bloquer les comptes et autres avoirs des gouvernements, entités et individus soumis à des Sanctions et à refuser ou rejeter les transactions impliquant des pays, gouvernements, entités et individus faisant l'objet de Sanctions.

b) Les bonnes pratiques

Pour vérifier si des transactions spécifiques sont prohibées ou permises, les informations détaillées de chaque transaction doivent être analysées au cas par cas. Les éléments à analyser sont notamment les parties concernées (donneur d'ordre, bénéficiaire, banques intervenantes), les intermédiaires et autres intervenants le cas échéant, les pays concernés (du donneur d'ordre, du bénéficiaire, de l'intermédiaire et autres intervenants), les compagnies de transport, les lieux de chargement et déchargement de la marchandise, la devise, l'origine, la destination et la nature des biens, services et activités et l'objectif économique de la transaction sous-jacente.

- **Les équipes commerciales et autres fonctions ne doivent pas tenter d'interpréter elle-même les sanctions internationales.**

Tout doute sur une transaction doit être rapidement reporté aux équipes de la conformité.

La responsabilité d'interprétation des lois et règlements ainsi que le conseil aux équipes du front incombe exclusivement à la Conformité, assistée le cas échéant par le Juridique.

- **Utilisation des cartes monétiques dans les jeux d'argent.**

Les jeux de hasard en ligne et la loterie sont considérés comme étant des secteurs d'activités à haut risque par la banque. Aussi les sites internet sur les jeux de hasard sont généralement associés à un trafic important et à des volumes de transactions élevés. Cette industrie du jeu est particulièrement vulnérable à la fraude d'où une exposition à des risques de dommages pour les consommateurs. **Par conséquent, la banque interdit formellement l'utilisation de nos cartes monétiques afin de jeux de hasard et de loterie.** 



c) Catégories des sanctions internationales

Les Sanctions Internationales peuvent être regroupées dans les deux catégories suivantes :

- **SANCTIONS GLOBALES VISANT UN PAYS (EMBARGO LOURD)** : il s'agit d'un programme de Sanctions qui interdit, à de rares exceptions, toute transaction avec un pays ou territoire spécifiques.
 ⇒ **La règle de base étant qu'aucune transaction ne peut être autorisée avec ces pays. Toute opération qui se présenterait devra être portée à la connaissance de la Direction Conformité.**
- **SANCTIONS PARTIELLES VISANT UN PAYS OU GLOBALES BASEES SUR DES LISTES** : il s'agit d'un programme de sanctions qui interdit toute transaction avec les Cibles de Sanctions figurant sur une liste de sanctions et, dans certains cas, avec les entités qu'elles détiennent ou contrôlent. Il peut s'agir aussi de Sanctions contenant des interdictions plus limitées et généralement plus spécifiques visant une région ou un gouvernement précis, des Cibles de Sanctions et, dans certains cas, les entités qu'elles détiennent ou contrôlent, certains produits, ou des Personnes appartenant à certains secteurs économiques (ex. sanctions sectorielles).
 ⇒ **Il faut s'assurer lors de l'initiation de toute opération, impliquant l'un des pays sous sanctions ciblées, que l'objet ou la nature de la transaction envisagée ne figure pas parmi les opérations interdites ou frappées de restrictions avec ces pays. La Direction de la conformité doit être saisie de façon systématique si des opérations impliquant ces contreparties se présentaient.**

La BDU-CI a mis en place une politique de conformité aux sanctions nationales et internationales qui détaille les engagements du groupe BDM dans le respect des sanctions internationales et embargos.

Fait à Abidjan, le 05 Août 2025

Directeur Général

Idrissa Wélé DIALLO



