

Mesures de contrôle interne en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

1. Organisation interne de l'opérateur.

L'opérateur de ventes volontaires doit mettre en œuvre des mesures de contrôle interne lui permettant de satisfaire à ses obligations en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme

L'opérateur définit les modalités de contrôle que les commissaires-priseurs et les membres du personnel mettent en œuvre dans leurs relations avec les clients vendeurs et acheteurs.

Il définit également les modalités de traitement des situations anormales : mise en œuvre de mesures de contrôle renforcé, refus de réaliser la transaction, transmission des informations au responsable désigné et, en cas de doute confirmé, déclaration de soupçon à TRACFIN.

La réglementation prévoit en effet que l'opérateur désigne un « déclarant » qui est chargé de faire les déclarations de soupçon. Son identité doit être communiquée à TRACFIN à l'occasion de la première déclaration.

La réglementation prévoit également que l'opérateur désigne un correspondant qui est le contact de TRACFIN au sein de la structure pour répondre à ses interrogations et transmettre ses instructions. Le déclarant et le correspondant peuvent être une seule et même personne.

L'opérateur doit enfin organiser la conservation pour une durée de cinq ans à compter de la fin de la relation d'affaires des documents relatifs à l'identité des clients et aux opérations.

2. Vérifications préalables de l'identité du client.

La finalité des mesures de contrôle interne que doivent mettre en œuvre de manière habituelle les opérateurs est la connaissance du client vendeur ou acheteur. Ces mesures doivent être mises en œuvre avant l'entrée en relation d'affaires avec le client.

2.1. Identifier le client personne physique.

L'opérateur vérifie l'identité de ses clients, vendeur et acheteur, ainsi que leur identité bancaire.

2.1.1. Identifier le vendeur.

Pour identifier son client vendeur, l'opérateur lui demande une pièce d'identité, en cours de validité, avec photo, telle qu'une carte nationale d'identité ou un passeport. Il relève les nom, prénom, date et lieu de naissance de la personne, la nature, le lieu et la date de délivrance de la pièce justificative d'identité et les nom et qualité de la personne qui l'a délivrée ou authentifiée.

Si le client vendeur réside hors de l'Union européenne, l'opérateur se fait présenter en plus du passeport une preuve de résidence secondaire en France ou un certificat d'importation du bien concerné.

Pour l'identification bancaire du client vendeur, deux situations doivent être envisagées : si le client demande un règlement par virement, l'opérateur lui demande un Relevé d'Identité Bancaire (RIB) et il s'assure que le titulaire du compte est la même personne que le vendeur dont l'identité lui a été communiquée ; si le client vendeur sollicite un règlement par chèque, l'opérateur doit libeller celui-ci aux nom et prénom du vendeur ; la demande du vendeur d'être payé par chèque n'est réalisable qu'à cette condition.

2.1.2. Identifier l'acheteur.

Pour identifier le client acheteur, l'opérateur lui demande une pièce d'identité, en cours de validité, avec photo telle que carte nationale d'identité ou passeport. Il relève les nom, prénom, date et lieu de naissance de la personne, la nature, le lieu et la date de délivrance de la pièce justificative d'identité et les nom et qualité de la personne qui l'a délivrée ou authentifiée.

Pour l'identification bancaire du client acheteur, l'opérateur s'assure que l'identité de l'acheteur est la même que celle du titulaire du moyen de paiement.

2.2. Identifier le client agissant par voie de procuration.

Pour identifier un client agissant par personne interposée, personne physique munie d'une procuration, l'opérateur exige une procuration écrite, la photocopie de la carte d'identité du tiers mandant en cours de validité et comportant sa photographie ainsi que celle de la personne munie de la procuration. L'opérateur vérifie que les signatures du mandant figurant sur sa carte d'identité et sur la procuration sont les mêmes. Pour ce qui concerne l'identité bancaire, le Relevé d'Identité Bancaire doit être au nom du mandant. Le RIB du mandant doit être au même nom que la pièce d'identité du mandant.

2.3. Identifier le client personne morale.

Pour identifier un client personne morale, l'opérateur demande un extrait K-bis de la personne morale datant de moins de trois mois ainsi qu'une lettre d'un des représentants légaux de la personne morale autorisant la personne qui dépose le bien à agir pour le compte de la société. L'opérateur s'assure que le nom de la personne mentionnée dans cette lettre correspond à celui figurant sur la pièce d'identité de la personne physique qui dépose effectivement le bien. Pour ce qui concerne l'identité bancaire, dans le cas d'un paiement par virement, la SVV obtient un Relevé d'Identité Bancaire au nom de la personne morale.

L'opérateur doit également s'enquérir de l'identité du bénéficiaire effectif de l'opération à savoir la ou les personnes physiques qui détiennent au moins 25% du capital ou des droits de vote de la société. Il s'agit là de repérer qui chercherait à utiliser une société « écran » pour procéder à des opérations de blanchiment.

2.4. Identifier le client absent.

Lorsque l'absence physique du client empêche son identification, situation perçue par la loi comme présentant un risque élevé, l'opérateur doit mettre en œuvre, en plus des mesures susvisées, l'une des mesures de contrôle complémentaires suivantes :

- obtenir des pièces justificatives d'identité complémentaires pour confirmer l'identité du client ;
- vérification et certification des documents présentés par un tiers indépendant de la personne à identifier ;
- exiger que le 1^{er} paiement des opérations soit effectué à partir ou à destination d'un compte bancaire d'un établissement établi dans l'Union européenne ou dans un Etat partie à l'accord sur l'Espace Economique Européen ;
- obtenir une confirmation de l'identité du client par un établissement bancaire.

Cette règle concerne également les opérations qui impliquent des personnes politiquement exposées qui sont énumérées à l'article R. 561-18 du code monétaire et financier.

3. Veille complémentaire.

La loi attend de l'opérateur qu'il évalue les risques de blanchiment de capitaux et de financement du terrorisme pendant toute la durée de la relation d'affaires. A cette fin, il lui est demandé de recueillir des informations relatives « à l'objet et à la nature » de la relation d'affaires, consigner le fruit de ses investigations par écrit et conserver cet écrit pendant le délai légal de cinq ans.

Le code monétaire et financier prévoit que ces informations sont à choisir parmi les suivantes :

- pour ce qui concerne la relation d'affaires : le montant et la nature des opérations envisagées, la provenance des fonds, la destination des fonds ou encore la justification économique déclarée par le client ou le fonctionnement envisagé du compte (pourquoi vendre ; d'où viennent les fonds...).
- pour ce qui concerne la connaissance de la situation professionnelle, économique et financière du client personne physique : la justification de l'adresse du domicile à jour au moment où les éléments sont recueillis, les activités professionnelles actuellement exercées, les revenus ou tout élément permettant d'estimer les autres ressources, tout élément permettant d'apprécier le patrimoine et, s'agissant des personnes politiquement exposées, les fonctions ou tout élément permettant d'apprécier la nature des liens existant entre ces personnes ;
- pour ce qui concerne la connaissance de la situation de la personne morale : la justification de l'adresse du siège social, les statuts, les mandats et pouvoirs ainsi que tout élément permettant d'apprécier la situation financière de la personne morale.

4. Situations à risque.

En cas de doute sur une personne ou une opération, l'opérateur doit mettre en œuvre des mesures de contrôle interne complémentaires.

4.1. Absence d'identification.

La loi oblige l'opérateur qui ne peut identifier son client qu'il n'a pu identifier ou dont il n'a pu obtenir d'information sur l'objet et la nature des relations d'affaires à ne pas entrer en relation d'affaires avec lui. Si la relation est déjà établie, il doit y mettre fin.

4.2. Comportements à risque.

L'opérateur doit repérer les comportements qui présentent un risque important de blanchiment de capitaux. Il en va par exemple ainsi des comportements suivants :

- vendeur refusant de communiquer son identité et les informations exigées par l'opérateur ;
- vendeur déposant régulièrement des biens à vendre sans qu'il y ait de cohérence entre les objets déposés ;
- client désirant laisser un ordre d'achat ou enchérir par téléphone refusant de communiquer les informations exigées par la maison de ventes (identité, RIB, etc...) ;
- un enchérisseur déclaré adjudicataire refusant de communiquer son identité à l'opérateur ;
- identité de l'auteur du règlement différente de l'identité de l'adjudicataire ;
- Il en va également ainsi de l'acheteur qui souhaite régler en espèces pour un montant non conforme avec la réglementation ; il convient à cet égard de rappeler qu'en application des dispositions de l'article D. 112-3 du code monétaire et financier, le règlement en espèces est autorisé jusqu'à 3000 € pour les résidents et jusqu'à 15.000 € pour les non-résidents (sur présentation d'un justificatif de la domiciliation fiscale du client et du passeport).

4.3. Mesures de contrôle complémentaires.

Dans les situations qui, telles celles qui sont exposées ci-dessus, présentent un risque élevé de blanchiment, le code monétaire et financier attend de l'opérateur qu'il mette en œuvre l'une des mesures complémentaires suivantes :

- Rechercher l'origine des fonds et la destination des sommes versées ;
- Rechercher l'objet de la vente et de la personne qui en bénéficie.

Il lui revient de rechercher ces informations, de consigner le fruit de ses investigations sur un écrit qu'il conservera pendant le délai légal de cinq ans.

5. Déclaration de soupçon.

L'opérateur doit apprécier le risque de blanchiment au regard des informations et documents qu'il recueille. En cas de doute caractérisé, par exemple si l'identité du client ou du bénéficiaire reste douteuse en dépit des mesures d'identification ou si l'opérateur soupçonne que les biens proposés

ou les fonds proviennent d'une infraction délictuelle ou criminelle, il est tenu, sous peine de sanction disciplinaire et pénale, de faire une déclaration de soupçon à TRACFIN.

5.1. Date de la déclaration.

Cette déclaration doit intervenir avant la réalisation de l'opération afin que TRACFIN puisse, le cas échéant, exercer son droit d'opposition à la réalisation de l'opération ; à défaut d'opposition formée dans les 24h de la déclaration, l'opérateur peut réaliser la transaction.

Il appartient en tout état de cause à l'opérateur d'apprécier l'opportunité de maintenir la relation d'affaires en fonction de l'intensité de son soupçon.

L'opérateur peut néanmoins procéder à une déclaration *a posteriori* s'il ne pouvait agir autrement, si le report de la vente, de la perception du paiement ou de la délivrance du bien aurait fait obstacle à des investigations ou si la nécessité de faire une déclaration n'est ressortie qu'après réalisation de l'opération.

5.2. Modalités de la déclaration.

La déclaration peut être faite par télédéclaration sur le site de téléprocédure de TRACFIN nommé Ermes ou par courrier au moyen du formulaire de déclaration à télécharger sur le site de TRACFIN (cf. <http://www.economie.gouv.fr/tracfin/declarer>).

L'opérateur doit porter un certain nombre d'informations sur la déclaration parmi lesquelles : les sommes ou les opérations soupçonnées de provenir d'une infraction délictuelle ou criminelle ou de participer au financement du terrorisme, les éléments d'identification et de connaissance du client ou du bénéficiaire effectif, le descriptif des opérations concernées ainsi qu'une analyse argumentée étayant le soupçon.

La déclaration doit être accompagnée de toute pièce ou document justificatif utile à son exploitation par TRACFIN (copie des pièces d'identité des personnes physiques, des statuts des personnes morales, du mandat du représentant légal, des moyens de paiements (chèques, bordereaux de virements..).

Elle doit ensuite être stockée dans un dossier spécifique portant la mention « Ne peut être saisi ». Elle est confidentielle : il ne doit en être fait état ni en interne, ni à l'extérieur. La déclaration est cependant accessible au Conseil des ventes volontaires dans le cadre de son pouvoir de contrôle du respect de la réglementation anti-blanchiment.

TRACFIN accuse réception de la déclaration sauf demande contraire de l'opérateur. Ce dernier n'est pas tenu informé des suites données à la déclaration, sauf en cas de transmission à l'autorité judiciaire.

TRACFIN est le seul interlocuteur de l'autorité judiciaire pour communiquer sur la déclaration de soupçon ; l'opérateur sollicité par un service de police judiciaire ou par un magistrat l'oriente vers TRACFIN.

L'opérateur qui fait une déclaration de soupçon de bonne foi ne peut voir sa responsabilité civile engagée au titre du préjudice subi par le vendeur ou l'acheteur. Il n'encourt aucune sanction disciplinaire et ne peut être poursuivi pour dénonciation calomnieuse.

En outre, avoir fait une déclaration de soupçon lui permettra de faire valoir plus aisément son absence d'intention frauduleuse et sa bonne foi en cas de mise en cause pour des faits de fraude, blanchiment de capitaux ou financement du terrorisme.