

RÉPUBLIQUE FRANÇAISE

Autorité nationale des jeux

**DÉCISION N° 2021-154 DU 3 JUIN 2021
PORTANT PROPOSITION AU MINISTRE DE L'INTÉRIEUR ET AU MINISTRE
DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE DU CADRE DE
RÉFÉRENCE POUR LA LUTTE CONTRE LA FRAUDE ET CONTRE LE
BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME**

Le collège de l'Autorité nationale des jeux ;

Vu le code de la sécurité intérieure, notamment le 3° de son article L. 320-3 ;

Vu la loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, notamment le deuxième alinéa du X de son article 34 ;

Après avoir entendu la commissaire du gouvernement, en ses observations, et en avoir délibéré le 3 juin 2021,

DÉCIDE :

Article 1^{er} : La proposition de cadre de référence pour la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme, annexée à la présente décision est adoptée.

Elle est transmise au ministre de l'intérieur et au ministre de l'économie, des finances et de la relance en application du deuxième alinéa du X de l'article 34 de la loi du 12 mai 2010.

Article 2 : Le directeur général de l'Autorité nationale des jeux est chargé de l'exécution de la présente décision qui sera notifiée au ministre de l'intérieur et au ministre de l'économie, des finances et de la relance et publiée sur le site internet de l'Autorité.

Fait à Paris, le 3 juin 2021.

La Présidente de l'Autorité nationale des jeux

Isabelle FALQUE-PIERROTIN



Projet de cadre de référence pour la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme

03/06/2021

Table des matières

<u>INTRODUCTION : POURQUOI INSTAURER UN CADRE DE REFERENCE POUR LA LUTTE CONTRE LA FRAUDE ET CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME ?.....</u>	<u>4</u>
<u>CHAPITRE I : PLAN D’ACTIONS ANNUEL EN VUE DE LUTTER CONTRE LA FRAUDE, LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME</u>	<u>8</u>
<u>CHAPITRE II : LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME</u>	<u>11</u>
<u>PREAMBULE : DEFINITIONS.....</u>	<u>11</u>
<u>ARTICLE 1 : ELABORATION D’UNE ANALYSE DES RISQUES</u>	<u>11</u>
<u>ARTICLE 2 : ORGANISATION ET MOYENS</u>	<u>14</u>
<u>ARTICLE 3 : DISPOSITIF DE CONTROLE INTERNE</u>	<u>17</u>
<u>ARTICLE 4 : QUALITE DE L’IDENTIFICATION ET DE LA CONNAISSANCE DES JOUEURS</u>	<u>18</u>
<u>ARTICLE 5 : SUIVI ET ANALYSE DES OPERATIONS DANS LE CADRE DE L’OBLIGATION DE VIGILANCE</u>	<u>20</u>
<u>ARTICLE 6 : MESURES DE VIGILANCE COMPLEMENTAIRES OU RENFORCEES</u>	<u>21</u>
<u>ARTICLE 7 : OBLIGATIONS DECLARATIVES.....</u>	<u>25</u>
<u>ARTICLE 8 : GEL DES AVOIRS</u>	<u>29</u>
<u>CHAPITRE III : LUTTE CONTRE LA FRAUDE.....</u>	<u>32</u>
<u>ARTICLE 9 : ELABORATION D’UNE ANALYSE DES RISQUES</u>	<u>33</u>
<u>ARTICLE 10 : ORGANISATION ET MOYENS</u>	<u>35</u>
<u>ARTICLE 11 : QUALITE DE L’IDENTIFICATION ET DE LA CONNAISSANCE DES JOUEURS</u>	<u>36</u>
<u>ARTICLE 12 : PREVENTION ET LUTTE CONTRE LES MANIPULATIONS DES COMPETITIONS SPORTIVES ET HIPPIQUES</u>	<u>36</u>
<u>ARTICLE 13 : INFORMATION GENERALE DE L’ANJ.....</u>	<u>38</u>
<u>CLAUSE DE RENDEZ-VOUS.....</u>	<u>39</u>

<u>ANNEXE I : CLASSIFICATION DES RISQUES EN MATIERE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME</u>	<u>40</u>
<u>ANNEXE II : EXEMPLES PRATIQUES.....</u>	<u>45</u>
<u>ANNEXE III : SOUPÇON DE FRAUDE FISCALE</u>	<u>52</u>
<u>ANNEXE IV : PRECISIONS SUR LA PRESENTATION ET LE CONTENU DE LA DECLARATION DE SOUPÇON</u>	<u>54</u>
<u>ANNEXE V : CATEGORISATION DES RISQUES EN MATIERE DE LUTTE CONTRE LA FRAUDE.....</u>	<u>56</u>

Introduction : pourquoi instaurer un cadre de référence pour la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme ?

Le cadre de référence pour la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme est prévu au X de l'article 34 de la loi du 12 mai 2010 modifiée par l'ordonnance du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard. Il est élaboré puis proposé par l'Autorité nationale des jeux (ANJ) aux ministres de l'intérieur et de l'économie qui l'adoptent par arrêté.

Ce cadre vise à **explicitier la mise en œuvre des obligations des opérateurs de jeux en matière de la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme** ainsi qu'à promouvoir une approche innovante de la régulation sur ce sujet.

Les jeux d'argent et de hasard ne sont ni un commerce ordinaire ni un service ordinaire. Ils sont autorisés à titre dérogatoire et doivent faire l'objet d'un **encadrement strict afin de prévenir les risques d'atteinte à l'ordre public**.

La lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme constitue l'un des quatre objectifs de la politique de l'Etat en matière de jeux d'argent codifié à l'article L. 320-3 du **code de la sécurité intérieure** dont ce cadre de référence se positionne comme la déclinaison opérationnelle.

Le cadre de référence présente une déclinaison opérationnelle du cadre juridique relatif à la lutte contre la fraude et contre le blanchiment des capitaux et le financement du terrorisme au secteur des jeux d'argent et de hasard

Au-delà des règles générales qui s'appliquent à l'ensemble des professionnels soumis au dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme, **les spécificités propres au secteur des jeux nécessitent la mise en œuvre de mesures de protection complémentaires**. Il ressort en effet tant des analyses nationales¹ qu'européennes² que le secteur des jeux d'argent et de hasard, pris dans son ensemble, présente **un niveau de risques élevé**, qui diffère selon les types de jeu et les vecteurs de distribution.

Ces risques résident à titre principal dans le **dépôt et l'utilisation par un joueur de fonds provenant d'un crime ou d'un délit** lui ayant procuré un profit direct ou indirect (escroquerie, vol, abus de confiance, recel, corruption, blanchiment, trafic de stupéfiants, etc.). Ils peuvent également être liés, de manière plus spécifique, à l'activité des joueurs excessifs ou pathologiques dont l'activité de jeu peut les entraîner à commettre l'une de ces infractions.

Ces risques sont accrus par les **vulnérabilités intrinsèques** au secteur des jeux, en particulier la circulation importante d'espèces et l'anonymat des joueurs au sein du réseau physique de distribution, qui empêche de déployer une véritable politique de connaissance du client, ou encore, dans le secteur du jeu en ligne, l'utilisation croissante des nouveaux moyens de paiement qui favorise également l'anonymat (cartes prépayées notamment). De plus, certains types d'opérations de jeu sont propices aux activités de blanchiment, à l'image des paris présentant une cote très faible.

¹ « Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France », Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), septembre 2019

² REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 24/07/2019.

Pour faire face à ces risques, l'ordonnance n° 2019-1015 du 2 octobre 2019 *réformant la régulation des jeux d'argent et de hasard* a **renforcé l'exigence de mise en conformité des opérateurs de jeux** en instituant, au X de l'article 34 de la loi n° 2010-476 du 12 mai 2010, **un cadre de référence pour la lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme. Ce cadre est pris par arrêté du ministre de l'intérieur et du ministre chargé de l'économie, sur proposition de l'Autorité nationale des jeux (ANJ).**

Ce cadre de référence remplace, d'une part, **les lignes directrices du 12 décembre 2019**, définies conjointement par la Cellule de renseignement financier national (TRACFIN) et l'Autorité de régulation des jeux en ligne (ARJEL) à destination des opérateurs agréés de jeu en ligne, et, d'autre part, **celles établies par le Service central des courses et jeux (SCCJ) du ministère de l'intérieur** à l'endroit des opérateurs sous droits exclusifs.

Il s'articule avec le cadre juridique européen, qui est principalement constitué de deux directives : la directive (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (dite « *4^{ème} directive anti-blanchiment* ») et, la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 qui modifie et complète la directive de 2015 (dite « *5^{ème} directive anti-blanchiment* »). Ces normes, qui s'inscrivent dans le prolongement des actions menées à une échelle plus large encore par le **Groupe d'action financière (GAFI)** au sein duquel la France tient un rôle majeur, ont été transposées en droit français entre 2016 et 2020.

Enfin, **la mise en œuvre des règles et recommandations** figurant dans le présent cadre de référence **s'exerce dans le respect des dispositions du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et de celles de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.**

Le cadre de référence repose sur une approche inclusive et s'adresse à tous les opérateurs de jeux d'argent, à l'exception des casinos.

Le périmètre d'application du cadre de référence coïncide avec celui des opérateurs assujettis défini au 9^obis de l'article L. 561-2 du code monétaire et financier qui sont désignés sous le vocable « opérateurs » :

- les opérateurs de jeux ou de paris autorisés sur le fondement de l'article 21 de la loi n° 2010 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, à savoir **les opérateurs agréés de jeu en ligne** et leurs représentants légaux ;
- les opérateurs de jeux ou de paris autorisés sur le fondement de l'article 5 de la loi du 2 juin 1891, ayant pour objet de réglementer l'autorisation et le fonctionnement des courses de chevaux, à savoir **le GIE Pari Mutuel Urbain et les sociétés de courses hippiques** ;
- l'opérateur de jeux et de paris autorisé sur le fondement de l'article 137 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, à savoir **La Française des jeux.**

Ce cadre de référence ne **s'applique pas aux casinos et clubs de jeux qui relèvent sur ce point du ministère de l'intérieur.**

Il convient en outre de préciser que si les **personnes exploitant un poste d'enregistrement en réseau physique de distribution, parfois dénommées « détaillants » ou « mandataires », n'ont pas la qualité d'assujetti au sens de l'article L. 561-2 du code monétaire et financier**, les exploitants de ces postes **participent à la protection de l'ordre public**, et notamment, à la lutte contre le blanchiment des capitaux et le financement du terrorisme et de la fraude. Les exploitants de ces postes d'enregistrement font à ce titre l'objet de contrôles de la part des opérateurs titulaires de droits exclusifs, qui peuvent donner lieu, en cas de manquements, à des sanctions.

Le cadre de référence propose une boîte à outils pour faciliter la mise en conformité des opérateurs de jeux, laquelle constitue l'objectif prioritaire du régulateur

La priorité du régulateur réside dans l'accompagnement à la mise en conformité des opérateurs en matière de la lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme.

A cette fin, le cadre de référence doit permettre de faciliter la compréhension du cadre juridique actuel, et, chaque fois que nécessaire, de préciser l'interprétation de ses dispositions et leurs orientations de mise en œuvre. Il fournit également des recommandations opérationnelles et des exemples de bonnes pratiques. Il n'ajoute rien aux obligations légales et n'interdit pas, sous réserve du respect des règles impératives applicables, l'adoption de solutions alternatives auxquelles les opérateurs pourraient recourir.

Les plans d'actions, que les opérateurs doivent désormais soumettre chaque année à l'approbation de l'Autorité, constituent la traduction concrète de cette mise en conformité, dans une démarche d'amélioration continue. Établis dans le respect du cadre de référence, ces plans définissent, de façon opérationnelle et actualisée, les trajectoires de conformité des opérateurs, par lesquelles ces derniers rendent compte de la mise en œuvre des actions conduites l'année précédente et présentent les mesures qu'ils vont mettre en place pour maintenir ou améliorer leurs standards de contrôle.

Le cadre de référence a été conçu comme un outil de droit souple, partagé et évolutif

La légitimité et l'efficacité du cadre de référence dépendent étroitement de l'implication des acteurs concernés dans son élaboration et sa mise en œuvre. Le dialogue permanent entre le régulateur et les opérateurs constitue la condition de réussite de cet exercice.

Aussi, la phase de concertation qui a précédé l'adoption du présent cadre de référence a constitué une étape essentielle pour aboutir à une vision partagée des enjeux et des moyens à mettre en œuvre pour atteindre le meilleur niveau d'efficacité possible en matière de lutte contre la fraude, le blanchiment de capitaux et le financement du terrorisme.

Parce qu'il doit permettre d'appréhender les phénomènes émergents d'un secteur en constante mutation, ce cadre privilégie l'approche du droit souple, au plus près des réalités du terrain, en laissant d'importantes marges de manœuvre aux opérateurs pour l'application de ces normes.

Par ailleurs, le cadre de référence comprend une clause de rendez-vous afin d'intégrer les évolutions à venir, qu'elles découlent de modifications des textes applicables ou de nouveaux besoins des opérateurs qui apparaîtraient à l'occasion de l'examen des plans d'actions.

Le cadre de référence traduit une approche coordonnée des acteurs publics nationaux et internationaux.

Pour améliorer la supervision du secteur des jeux d'argent et de hasard, l'ordonnance du 2 octobre 2019 accorde une place importante à l'interrégulation, soit à la nécessaire coopération entre tous les partenaires publics concourant à la mise en œuvre de cette politique publique, en particulier la Direction générale du Trésor, TRACFIN et le SCCJ. Dans cette perspective, l'ANJ pourra diffuser, à chaque fois que nécessaire, en lien avec ces acteurs, des informations susceptibles de guider les opérateurs dans la mise en œuvre de leurs obligations.

Cette approche recouvre aussi une **dimension européenne et internationale** qui promeut la **coopération entre les Etats membres** et l'échange de bonnes pratiques. Dans ce cadre, l'Autorité peut solliciter et utiliser, pour l'accomplissement de ses missions en matière de lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme, des **informations obtenues d'autorités étrangères**.

Cette meilleure coordination des acteurs publics contribue à une meilleure lisibilité des objectifs légaux pour l'ensemble des opérateurs.

Le non-respect par les opérateurs de leurs obligations en matière de lutte contre la fraude et de lutte contre le blanchiment de capitaux et le financement du terrorisme est susceptible de fonder **l'engagement d'une procédure de sanction devant la commission nationale des sanctions ou la commission des sanctions, en fonction des circonstances.**

Un document structuré pour faciliter sa lisibilité et sa mise en œuvre

Ce cadre de référence est composé de **trois chapitres** :

- le **premier chapitre** présente le nouveau dispositif du **plan d'actions** ;
- le **deuxième chapitre** décline les différentes obligations relatives à la **lutte contre le blanchiment des capitaux et le financement du terrorisme** ;
- le **troisième chapitre** porte plus spécifiquement sur la **lutte contre la fraude**.

Chaque article du présent cadre de référence mentionne les **dispositions législatives et réglementaires** pertinentes, explicite les **principes généraux** qui s'induisent de ces textes ainsi que leurs **orientations de mise en œuvre** assorties, le cas échéant, de **recommandations et des exemples de bonnes pratiques**.

5 annexes viennent préciser et illustrer certains aspects particuliers en matière de :

- **Annexe I** : classification des risques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- **Annexe II** : exemples de démarches à mettre en œuvre relative à l'analyse et d'informations complémentaires suite à la détection d'un critère d'alerte, critères d'alertes, analyse des données bancaires collectées ;
- **Annexe III** : précisions relatives au soupçon de fraude fiscale ;
- **Annexe IV** : présentation et contenu de la déclaration de soupçon ;
- **Annexe V** : catégorisation des risques en matière de lutte contre la fraude.

Le cadre de référence a, en outre, vocation à être **complété par des publications communes à TRACFIN et à l'ANJ**, à visée pédagogique, notamment pour présenter des **cas typologiques**.

Chapitre I : Plan d'actions annuel en vue de lutter contre la fraude, le blanchiment des capitaux et le financement du terrorisme



Textes de référence :

- Articles 27, 34-X et 35-III de la loi du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;
- Article 13 du décret n° 2020-199 du 4 mars 2020 relatif à l'organisation et au fonctionnement de l'Autorité nationale des jeux ;
- Article 4 du cahier des charges de la Française des jeux tel que défini par le décret n° 2019-1060 du 17 octobre 2019 ;
- Article 3 du décret n° 2019-1061 du 17 octobre 2019 relatif à l'encadrement de l'offre de jeux de La Française des jeux et du Pari mutuel urbain.

Principes généraux

- Chaque année, les opérateurs **soumettent à l'approbation** de l'Autorité leur plan d'actions établi dans le respect du cadre de référence. Ces plans visent à évaluer le niveau de conformité des opérateurs et à définir des axes d'amélioration à mettre en œuvre.
- A cette occasion, ils rendent compte de la mise en œuvre du plan de l'année précédente ainsi que **des résultats des contrôles** qu'ils ont réalisés en matière de lutte contre les activités frauduleuses ou criminelles ainsi que le blanchiment des capitaux et le financement du terrorisme.
- L'Autorité nationale des jeux **évalue la pertinence et les résultats des actions** menées par les opérateurs en la matière, soit à l'occasion de l'examen des plans d'actions annuels, soit dans le cadre de sa mission de contrôle.
- Le collège de l'ANJ **consulte la commission de la lutte contre la fraude et contre le blanchiment des capitaux** sur les plans d'actions dans les conditions prévues par le règlement intérieur de l'Autorité.
- Il peut adresser aux opérateurs des **prescriptions**.
- Dans le cadre de l'examen du plan d'actions, les services de l'Autorité peuvent **demandier tout élément ou document complémentaire** qu'ils jugent utiles à la bonne information du collège.

Orientations de mise en œuvre

Le plan d'actions a pour objectif de permettre à l'ANJ :

- d'avoir une **meilleure connaissance** des actions réalisées par les opérateurs dans le cadre de la lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme et d'identifier les éventuelles difficultés rencontrées par ces derniers ;

- d'**évaluer** la mise en œuvre des obligations visées par le cadre de référence ;
- d'adresser, le cas échéant et au regard de cette évaluation, des **recommandations ou des prescriptions** aux opérateurs en vue d'accompagner leur mise en conformité ;
- de **capitaliser les bonnes pratiques** afin de faire évoluer le cadre de référence.

Le plan d'actions comporte s'articule autour de deux axes :

- **un bilan des actions** réalisées au cours de l'année N-1 dans le cadre de la lutte contre la fraude et contre le blanchiment des capitaux et le financement du terrorisme ainsi que **les résultats des contrôles** conduits par l'opérateur ;
- **un plan d'actions prévu pour l'année N**, qui expose **les mesures à mettre en œuvre** pour l'année à venir afin de renforcer le dispositif de lutte contre la fraude et contre le blanchiment des capitaux et le financement du terrorisme.

Les mesures d'amélioration à mettre en place sont **librement proposées** par l'opérateur, sur la base de l'évaluation qu'il fait de son niveau de conformité et de ses marges de progression. Il revient par la suite à l'Autorité de les **approuver et, le cas échéant, d'adresser des prescriptions**.

Le suivi de la mise en œuvre des mesures doit être **assuré de manière continue par l'opérateur** et fait l'objet d'un examen annuel par l'Autorité dans le cadre du plan d'actions.



Le plan d'actions comporte *a minima* les éléments suivants relatifs :

- **à la présentation et à l'organisation interne des opérateurs :**
 - présentation de l'opérateur (organigramme organisationnel et de l'actionnariat, nombre de salariés...) ;
 - détails sur l'organisation interne et les moyens humains dont dispose l'opérateur (identification des responsables, département ou service concerné par la conformité, pilotage de l'activité, ressources humaines dédiées) ;
 - nature des prestations éventuellement confiées à des tiers ;
 - formation des personnels (nombre de personnes formées, description des formations, fréquence, ciblage, modalités et évaluation...) et maîtrise de la réglementation par les éventuels prestataires.
- **à la présentation des outils utilisés pour la lutte anti-blanchiment :**
 - outils existants (moyens informatiques, outils de contextualisation) ;
 - outils en cours de développement ou à développer.
- **au bilan des actions de mise en conformité réalisées :**
 - prise en compte des évolutions du cadre législatif et réglementaire ;
 - mise en œuvre d'actions de contrôle interne ;
 - mise en œuvre des prescriptions de l'ANJ.

▪ **à la déclinaison du dispositif d'analyse des risques utilisé :**

- tendances observées lors de la dernière année et mise à jour de l'analyse des risques « fraude, blanchiment et financement du terrorisme » ;
- démarches entreprises et mesures d'atténuation des risques.

▪ **à l'activité de détection des atypismes et à l'activité déclarative de l'opérateur :**

- caractéristiques des alertes traitées : nombre et nature des alertes, nombre d'examens renforcés, délai moyen de traitement, suites données (taux de transformation des alertes en déclarations de soupçon, plaintes, informations de l'ANJ...).

Afin d'accompagner les opérateurs dans la rédaction de leur plan d'actions, l'Autorité **met à leur disposition une notice reprenant les rubriques et informations qu'elle souhaite y voir apparaître.**

Calendrier

Le plan d'actions en matière de lutte contre la fraude et le blanchiment des capitaux est **soumis** à l'approbation de l'Autorité nationale des jeux **avant le 31 janvier** de chaque année pour l'ensemble des opérateurs concernés :

- ✓ **les opérateurs sous droits exclusifs ;**
- ✓ **les opérateurs agréés** de jeu en ligne ;
- ✓ **les sociétés de courses.**

Chapitre II : Lutte contre le blanchiment des capitaux et le financement du terrorisme

Préambule : Définitions

Le blanchiment des capitaux est défini par l'article 324-1 du code pénal comme :

- le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect ;
- ou le fait **d'apporter un concours** à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou délit.

Il se déroule en trois phases :

- ✓ Le **placement**, qui permet d'introduire dans le système financier des fonds provenant d'opérations délictueuses ;
- ✓ **L'empilage**, aux fins de dissimulation de leur origine économique réelle par la multiplication d'opérations bancaires ou financières successives faisant intervenir divers comptes, établissements, personnes, produits et pays ;
- ✓ **L'intégration**, consistant à investir les fonds d'origine frauduleuse dans les circuits légaux de l'économie et en tirer des bénéfices.

Le financement du terrorisme est défini par l'article 421-2-2 du code pénal comme le fait de fournir ou de participer, directement ou indirectement, à la collecte de fonds susceptibles d'être utilisés pour financer des terroristes, des organisations terroristes ou commettre un acte terroriste.

Article 1 : Elaboration d'une analyse des risques

Textes de référence :

- Article L. 561-4-1 du code monétaire et financier ;
- Article 3 du décret n° 2020-1349 du 4 novembre 2020 relatif aux modalités de régulation de l'Autorité nationale des jeux.



Section 1.1 Principes généraux

- Les opérateurs doivent définir et mettre en place des dispositifs **d'identification et d'évaluation des risques** de blanchiment des capitaux et de financement du terrorisme auxquels ils sont exposés.
- Ils élaborent une **classification des risques** documentée en fonction de la nature des services offerts, des conditions de transaction proposées, des canaux de distribution utilisés, des caractéristiques des clients, ainsi que du pays ou du territoire d'origine ou de

destination des fonds en fonction desquels ils appliquent les mesures de vigilance appropriées.

- Ils définissent les éventuelles **mesures d'atténuation** en fonction des risques identifiés.
- **Pour les hippodromes** dans lesquels la gestion des paris n'est pas assurée par le GIE PMU, les sociétés de courses peuvent établir une classification des risques commune au niveau de la Fédération nationale des courses hippiques. L'Autorité peut toutefois demander à chaque société de course la transmission de tout document complémentaire ou information lui permettant d'apprécier le respect de ses obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.
- Sur la base de cette analyse et de cette classification, l'opérateur met en œuvre une **politique de détection, de prévention et de correction** adaptée de ces risques.

Section 1.2 Orientations de mise en œuvre

La compréhension des risques de blanchiment des capitaux et/ou de financement du terrorisme que présente une activité constitue le fondement d'un dispositif efficace de maîtrise et de gestion de ces risques. A cette fin, les opérateurs doivent **mettre en place un ensemble de mesures organisationnelles et techniques destinées à identifier, classer et détecter de manière pertinente les personnes ou les opérations à risques**.

L'évaluation et la gestion des risques doit comporter **trois volets** :

- **une identification des risques (1) ;**
 - **une appréciation de leur criticité permettant de les classer (2) ;**
 - **la présentation des mesures visant, le cas échéant, à les gérer et à les atténuer (3).**
- > Le volet « **identification des risques** » constitue la première étape primordiale d'une analyse de risques. A cette occasion, et en amont de toute analyse, les opérateurs doivent recenser tous les facteurs de risques en lien avec leur activité, qu'il s'agisse des services proposés, des transactions réalisées ou des caractéristiques des clients intéressés par de tels services.

Ils mènent ce travail à partir de leur expertise et de leur connaissance du secteur ainsi que des différentes sources d'informations qu'ils ont à leur disposition telles que l'évaluation supranationale des risques effectuée par la Commission européenne et l'analyse nationale des risques précédemment évoquées, les informations communiquées par l'Autorité et/ou par TRACFIN (rapports, alertes, typologies) ou encore les informations librement accessibles, le tout dans le respect des règles relatives à la protection des données à caractère personnel.

- > Le volet **classification des risques**, deuxième étape de l'analyse des risques, vise à établir une échelle des risques auxquels l'opérateur est exposé au regard de ses activités et aboutit à l'établissement d'une « *cartographie des risques* ».

Pour établir cette classification, les opérateurs doivent prendre en compte l'ensemble des éléments relatifs à la **nature des services offerts, aux conditions de transaction proposées, aux canaux de distribution utilisés, aux caractéristiques des clients concernés ainsi qu'aux pays ou territoires d'origine et de destination des fonds**. Une attention particulière doit ainsi être apportée :

- aux risques liés à la connaissance du client, en veillant notamment à pouvoir identifier en amont les personnes politiquement exposées (PPE), les clients à haute valeur commerciale (bénéficiant souvent de programme « VIP ») et les titulaires de points de vente ;

- aux risques liés aux services ou opérations de jeux proposés par l'opérateur, notamment en fonction des degrés de vulnérabilité qu'ils présentent ;
- aux risques liés aux transactions et aux données financières du client.

Un exemple de classification des risques à prendre en compte est présenté **en annexe I**.

- > Le volet **stratégique**, troisième et dernière étape de l'analyse, décrit les mesures de prévention, d'atténuation et de correction ainsi que les procédures à mettre en œuvre, en réponse aux risques préalablement identifiés.

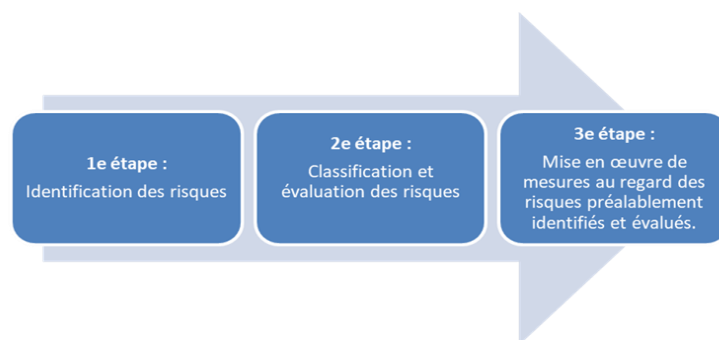
Le système d'évaluation et de gestion des risques d'un opérateur doit faire l'objet d'une **actualisation régulière** et notamment :

- préalablement au lancement de nouveaux services, suite notamment à une évolution du cadre juridique ou réglementaire autorisant la fourniture de nouveaux jeux ou types de paris hippiques ou sportifs, ou de nouvelles pratiques ;
- à l'occasion de modifications législatives ou réglementaires en matière de lutte contre la fraude et contre le blanchiment des capitaux.

En pratique, l'ensemble du dispositif d'analyse des risques doit être **formalisé dans un document écrit** qui reprend :

- > l'identification et la classification des risques auxquels l'opérateur est exposé ;
- > la définition des mesures destinées à prévenir et à gérer ces risques ;
- > l'organisation des travaux à mener.

La démarche que les opérateurs doivent suivre en la matière se schématise comme suit :



L'évaluation des résultats issus de la mise en œuvre des mesures préventives et de gestion des risques doit permettre à l'opérateur, le cas échéant, d'**adapter sa cartographie** des risques.

Focus réseau physique de distribution

Les points de distribution en réseau physique **doivent également faire l'objet d'une cartographie des risques** effectuée par les opérateurs en fonction notamment de leur localisation, de leur activité (part des paris sportifs, variation d'activité, présence de joueurs à forte activité...) et de leurs modalités d'exploitation (modification du statut juridique, changement de gérant, etc.).

Il en va de même pour les sociétés de courses, en fonction de l'activité et de la clientèle des hippodromes.

Exemples de bonnes pratiques



En cartographiant ses risques, l'opérateur **crée les conditions d'une plus grande connaissance et donc d'une meilleure maîtrise des risques** auxquels il est confronté.

- La cartographie des risques se présente généralement comme une nomenclature, dressée par l'opérateur, des situations dans lesquelles il peut avoir affaire à une opération et/ou une personne physique qui présentent des risques au regard de la réglementation LCB/FT.
- Le lieu et le support de la prise de jeu ainsi que son mode de paiement sont également à passer en revue.

Article 2 : Organisation et moyens

Textes de référence :



- Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission ;
- Articles L. 561-32-I, L. 561-33 et L. 561-34 du code monétaire et financier ;
- Articles R. 561-29, R. 561-38 et R. 561-38-1 du code monétaire et financier ;
- Articles 30 et 31 du décret n° 2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.

Section 2.1 Principes généraux

- Les opérateurs disposent **d'une organisation** qui tient compte de la classification des risques mentionnée ci-dessus ainsi que **de moyens humains et matériels** permettant de lutter contre la fraude, le blanchiment de capitaux et le financement du terrorisme.
- Ces moyens sont **adaptés à la taille** de l'opérateur, à la **nature** de ses activités ainsi qu'aux **risques** identifiés. Ils permettent une mise en œuvre effective des mesures de vigilance.
- Lorsqu'un opérateur fait partie d'un groupe, l'organisation et les procédures peuvent être définies et mises en œuvre au **niveau du groupe**.
- Les opérateurs **élaborent des procédures** applicables en la matière et les **formalisent par écrit**.
- Dans le cadre du **recrutement de leur personnel**, les opérateurs prennent en compte les risques que présentent les personnes recrutées au regard de la lutte contre le blanchiment de capitaux et le financement du terrorisme.
- Les opérateurs assurent la **formation et l'information** de leur personnel.
- L'opérateur qui confie à un tiers l'exécution de ses obligations en matière de LCB-FT **demeure responsable du respect de cette dernière** à l'égard de l'ANJ. L'externalisation à laquelle l'opérateur procède donne lieu à la conclusion d'un écrit avec le prestataire,

décrivant précisément le contenu des obligations mises sa charge. Ce contrat est communiqué sans délai à l'Autorité.

- Les opérateurs conservent pour une durée de **cinq ans** à compter de la clôture des comptes les documents et informations relatifs à leurs relations d'affaires (relations avec leurs joueurs) et aux mesures de vigilance mises en œuvre (sans préjudice du délai de 6 ans applicable à certaines données).

Section 2.2 Orientations de mise en œuvre

Les opérateurs doivent mettre en place une organisation et des procédures internes pour lutter efficacement contre le blanchiment des capitaux et le financement du terrorisme.

La mise en œuvre de ces dispositions se traduit notamment par la **nomination d'un responsable qualifié** de la lutte contre le blanchiment des capitaux et le financement du terrorisme qui dispose d'un niveau hiérarchique suffisamment élevé.

En outre, les opérateurs doivent désigner auprès de TRACFIN au moins un déclarant et un correspondant TRACFIN selon les modalités précisées à l'article 7 du présent cadre de référence.

Moyens humains et matériels

Les opérateurs mettent à disposition du personnel en charge de la lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme **les moyens matériels ainsi que les outils nécessaires à l'exercice de leur mission**. Ils en justifient auprès de l'Autorité à tout moment.

Des dispositifs adaptés et spécifiques de recrutement, de formation et d'information des personnels doivent être mis en place. Pour chaque fonction en lien avec la lutte contre la fraude ou le blanchiment des capitaux, les opérateurs documentent notamment :

- > les conditions d'aptitude et d'honorabilité requises ;
- > l'expérience et la qualification nécessaires ;
- > les modalités de formations adaptées ;
- > les modalités selon lesquelles toutes les informations nécessaires à l'exercice de leurs fonctions sont portées à leur connaissance.

Les vérifications effectuées dans le cadre du processus de recrutement sont **proportionnées** aux risques présentés par chaque type de poste, compte tenu des fonctions, des activités et de la position hiérarchique qui leur sont associées, au regard du dispositif de lutte contre le blanchiment des capitaux et de financement du terrorisme. Les opérateurs s'assurent en particulier que les personnes recrutées ne sont pas soumises à des mesures de gel des avoirs.

Les opérateurs dispensent ou font dispenser une formation **régulière et adaptée** à leurs collaborateurs (réglementation applicable, techniques de blanchiment et de fraude). Que la formation soit conduite en interne ou par le recours à un organisme tiers, l'opérateur doit s'assurer que le formateur dispose des **compétences requises** pour dispenser ce type de formation. Doivent être prévues une formation initiale et une formation continue, chacune étant adaptée en termes de fréquence et de contenu au degré d'exposition du personnel au risque de blanchiment des capitaux et de financement du terrorisme. Ces formations doivent également bénéficier aux membres des organes de direction de ces sociétés.

L'obligation d'information s'apprécie notamment par la mise à la disposition effective du personnel de toutes les informations utiles et par le fait que celui-ci en a pris formellement connaissance.

Mise en place de procédures formalisées

L'ensemble des procédures mises en œuvre pour lutter contre le blanchiment des capitaux et le financement du terrorisme est formalisé **par écrit**.

Les opérateurs doivent pouvoir **justifier** à tout moment de **l'existence**, de la **permanence et de l'efficacité des procédures mises en place, notamment par la conservation de tout document utile**.

Appartenance à un groupe

Lorsqu'un opérateur fait partie d'un groupe, l'organisation et les procédures peuvent être mises en œuvre au niveau du groupe mais **doivent tenir compte des spécificités propres à l'activité de chaque entité**. Ces procédures prévoient également le partage des informations au sein du groupe, la protection des données à caractère personnel ainsi que les mesures de contrôle interne.

Recours à des prestataires

Les opérateurs peuvent recourir à des tiers pour mettre en œuvre les mesures leur permettant de remplir leurs propres obligations (par exemple, s'agissant de la vérification de l'identité de leurs clients). Ils **restent cependant seuls responsables de leurs obligations en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme**.

Par ailleurs, **la gouvernance et le pilotage du dispositif anti-blanchiment ainsi que la déclaration de soupçon ne peuvent être externalisés**.

Dans le cas du recours à un prestataire, **un contrat écrit** est systématiquement conclu entre l'opérateur et le fournisseur du service externalisé. Il prévoit que celui-ci agit au nom et pour le compte de l'opérateur qui définit contractuellement les procédures à mettre en place. Le contrat comporte le descriptif des services fournis par l'agent, rappelle que la responsabilité liée à la réalisation des obligations de lutte contre la fraude, le blanchiment des capitaux et le financement du terrorisme pèse en tout état de cause sur l'opérateur et ne peut être transférée à l'agent fournissant le service externalisé, et décrit les modalités du contrôle exercé sur l'agent pour vérifier la bonne exécution par ce dernier de ses obligations contractuelles.

Enfin, **l'obligation de formation et de qualification** des personnels aux problématiques anti-blanchiment trouve également à s'appliquer à l'égard du personnel du fournisseur du service externalisé, l'opérateur devant être en mesure d'en justifier.

Conservation des informations

Les opérateurs doivent conserver **pendant cinq ans après la clôture du compte joueur ou la cessation de la relation** :

- > les éléments relatifs à l'identité des clients ;
- > les éléments relatifs aux opérations réalisées par ceux-ci ;
- > les documents relatifs aux mesures de vigilance mises en œuvre à leur égard ;
- > les documents consignant les caractéristiques des opérations pour lesquelles des mesures de vigilance renforcées ont été mises en œuvre.

Ce délai est porté à 6 ans après la clôture du compte joueur pour les données visées à l'article 31 du décret n°2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.

Article 3 : Dispositif de contrôle interne

Textes de référence :

- Articles L. 561-32-II, L. 561-33 et L. 561-34 du code monétaire et financier ;
- Articles R. 561-38-3 et R. 561-38-9 du code monétaire et financier ;
- Article 20 du décret n° 2019-1061 du 17 octobre 2019 relatif à l'encadrement de l'offre de jeux de La Française des jeux et du Pari mutuel urbain.



Section 3.1 Principes généraux

- Pour veiller au respect de leurs obligations, les opérateurs mettent en place des **mesures de contrôle interne** visant à s'assurer de la bonne mise en œuvre des procédures.
- Les résultats des contrôles donnent lieu, le cas échéant, à des **mesures correctrices**.

Section 3.2 Orientations de mise en œuvre

Les opérateurs doivent apprécier **l'effectivité et l'efficacité de leurs mesures** et procédures de prévention, d'atténuation et de correction des risques identifiés ainsi que des mesures de vigilance exécutées par la mise en place de procédures de contrôle interne. Ces contrôles sont adaptés à la taille, à la structure et au degré d'exposition aux risques de l'opérateur ainsi qu'aux défaillances précédemment relevées. Ils comprennent :

- > un dispositif de contrôle permanent réalisé par des opérationnels ou du personnel dédié ;
- > et, lorsque cela est approprié, un dispositif de contrôle périodique, éventuellement réalisé par des personnes dédiées et indépendantes.

Les dispositifs de contrôle interne permettent ainsi de s'assurer, d'une part, que les procédures mises en place permettent de **satisfaire aux différentes obligations** de lutte contre le blanchiment des capitaux et le financement du terrorisme et, d'autre part, qu'elles sont **correctement appliquées**. L'appréciation de l'efficacité des procédures internes inclut notamment les délais de réalisation des différentes diligences à accomplir.

Lorsque de nouveaux risques ou des défaillances supplémentaires sont détectés à l'occasion de ces contrôles internes, des **mesures correctrices sont alors mises en œuvre** (modification de la documentation, actions de formation complémentaires voire avertissements ou sanctions). Ces nouveaux risques peuvent résulter de la fourniture par l'opérateur d'un nouveau type de jeux ou de paris.

Les résultats de ces contrôles internes sont **portés à la connaissance du représentant légal** de l'entreprise. **Ils sont en outre présentés dans la partie bilan du plan d'actions. A ce titre, les opérateurs doivent être en mesure de justifier à tout moment de la mise en œuvre de ce contrôle interne** et tenir l'intégralité des rapports et des documents y afférents à la disposition permanente de l'Autorité.

Focus réseau physique de distribution

L'opérateur titulaire de droits exclusifs doit veiller à ce que les personnes exploitant pour lui un poste d'enregistrement contribuent effectivement à la lutte contre le blanchiment des capitaux et le financement du terrorisme et la fraude. Cet opérateur doit donc contrôler et, le cas échéant, sanctionner ces exploitants. Sa défaillance l'expose à l'ouverture d'une procédure de sanction à son encontre.

A cet égard, l'article 20 du décret n° 2019-1061 du 17 octobre 2019 relatif à l'encadrement de l'offre de jeux de La Française des jeux et du Pari mutuel urbain dispose : « I. - La Française des jeux est tenue de s'assurer que les contrats qu'elle conclut avec les personnes autorisées à exploiter un poste d'enregistrement de jeux de loterie ou de paris sportifs conformément aux dispositions des articles R. 322-18-1 à R. 322-18-3 et des articles R. 322-22-1 à R. 322-22-3 du code de la sécurité intérieure mettent à la charge de celles-ci les obligations de prendre les mesures et d'accomplir les diligences nécessaires à la réalisation des objectifs mentionnés à l'article L. 320-4. Elle veille à ce que le non-respect de ces obligations donne lieu à des sanctions proportionnées. / II. - La société notifie à l'Autorité nationale des jeux tout projet d'évolution des obligations mentionnées au I, telles que stipulées dans les contrats conclus avec les personnes autorisées à exploiter des postes d'enregistrement. Elle rend compte chaque année de la mise en œuvre éventuelle de sanctions en cas de manquement de ces personnes à ces obligations ».

Le contrat liant l'exploitant du poste d'enregistrement à l'opérateur titulaire de droits exclusifs est l'outil juridique adéquat par lequel celui-ci s'assure que celui-là participe à la protection de l'ordre public. Il est également l'instrument juridique approprié pour déterminer les conséquences juridiques d'un manquement de l'exploitant à ses obligations, notamment les sanctions (clauses pénales par exemple) qui sont susceptibles de devoir lui être infligées.

En tant que de besoin, il est rappelé aux opérateurs titulaires de droits exclusifs que, en application du onzième alinéa du II de l'article 38 de la loi du 12 mai 2010 modifiée, il leur appartient de saisir l'Autorité nationale des jeux pour que celle-ci « *approuve les clauses-types des contrats passés entre les opérateurs titulaires de droits exclusifs et les personnes privées exploitant un poste d'enregistrement de jeux de loterie, de jeux de paris sportifs et de paris hippiques* ».

Article 4 : Qualité de l'identification et de la connaissance des joueurs

Textes de référence :

- Articles L. 561-2-1, L. 561-5, L. 561-5-1 et L. 561-8 du code monétaire et financier ;
- Article 17 de la loi n° 2010-476 du 12 mai 2010 ;
- Articles R. 561-5, R. 561-5-1, R. 561-5-3, R. 561-6, R. 561-10, R. 561-11, R. 561-12, et R. 561-22-2 du code monétaire et financier ;
- Articles 2 et 4 du décret n° 2010-518 du 19 mai 2010 ;
- Article 11 du décret n° 2019-1061 du 17 octobre 2019.



Section 4.1 Principes généraux

- **L'ouverture d'un compte joueur auprès d'un opérateur est subordonnée au recueil par ce dernier des informations et documents lui permettant de vérifier l'identité de**

chaque nouveau joueur, son âge, son adresse ainsi que la titularité du compte de paiement sur lequel sont reversés ses avoirs.

- Les opérateurs peuvent vérifier l'identité de leurs clients sur comptes en recourant à certains moyens d'identification électronique.
- Les opérateurs vérifient également l'identité de leurs clients, lors d'une opération ou de plusieurs opérations liées de jeu hors compte joueur en réseau physique de distribution, **lorsqu'un joueur mise ou gagne des sommes égales ou supérieures à 2 000 euros par transaction**.
- En cas de doute sur l'identité d'un de leurs clients ou sur l'exactitude des éléments de vérification obtenus, les opérateurs procèdent à une **nouvelle vérification de l'identité dudit client**. S'ils n'y parviennent pas, ils mettent alors fin à la relation d'affaires avec la possibilité, le cas échéant, de transmettre une déclaration de soupçon à TRACFIN.
- Les opérateurs analysent et mettent à jour les éléments d'identification et d'informations qu'ils détiennent sur leurs clients et qui leur permettent de **disposer de la connaissance nécessaire à l'entrée en relation d'affaires et à la poursuite de celle-ci**. La nature et le périmètre des informations collectées ainsi que la fréquence de leur mise à jour et l'étendue des analyses menées sont adaptés aux risques de blanchiment des capitaux et de financement du terrorisme que présentent les activités concernées. Les opérateurs sont en mesure de justifier auprès de l'Autorité de la mise en œuvre de ces mesures et de leur adéquation aux risques préalablement identifiés.

Section 4.2 Orientations de mise en œuvre

En premier lieu, en application de l'article L. 320-16 du code de la sécurité intérieure, « *Nul tiers personne morale ne peut prendre part aux jeux d'argent et de hasard autorisés par l'article L. 320-6, ni effectuer de prise de jeu au nom et pour le compte des personnes physiques* ».

Dès lors, dans le secteur des jeux d'argent et de hasard, les obligations énoncées par le code monétaire et financier et relatives à **l'identification des clients ne concernent que des personnes physiques** et les problématiques relatives à la recherche du bénéficiaire effectif d'une opération ne trouvent donc pas à s'appliquer.

De la même façon, **les joueurs détenant un compte** sont tous considérés comme **des « relations d'affaires »**, au sens des textes applicables en matière de lutte contre le blanchiment des capitaux, et ce, quelle que soit l'intensité de leur activité. Ces derniers peuvent également être désignés, au sein du présent cadre de référence, sous le vocable de « **clients non occasionnels** ».

Si les opérateurs ne recourent pas à **un des moyens d'identification électronique** prévus par l'article R. 561-5-1 du code monétaire et financier, ils doivent exercer un **contrôle rigoureux** de la concordance des données personnelles avec celles fournies par le joueur et s'assurer de la validité et de l'authenticité des documents produits. A cette fin, le personnel dédié à leur recevabilité et à leur contrôle devra détenir les **compétences nécessaires** en matière de détection de documents falsifiés ou contrefaits et d'usurpation d'identité.

La connaissance du client doit être actualisée en fonction du profil de risque présenté par celui-ci. Pour l'ensemble des joueurs identifiés, les opérateurs mettent en place des moyens adaptés assurant la conservation et la sécurisation des données enregistrées.

Nota : Le dispositif spécifique d'identification des personnes politiquement exposées est évoqué à l'article 6.

Recommandations



- L'Autorité recommande aux opérateurs de recourir à **un des moyens d'identification électronique** prévus par l'article R. 561-5-1 du code monétaire et financier. En effet, ces moyens limitativement énumérés par le code monétaire et financier garantissent l'identité du joueur tout en dispensant, d'une part, ce dernier de l'envoi de sa pièce d'identité et, d'autre part, l'opérateur de la vérification de celle-ci.
- Les opérateurs sont invités à prendre l'attache des services de l'Autorité lorsqu'ils entendent mettre en place des solutions de paiement facilitant l'approvisionnement ou le reversement des avoirs des joueurs.

Focus réseau physique de distribution

Les opérateurs sous droits exclusifs sont **tenus d'identifier et de vérifier l'identité de leurs clients occasionnels, lors d'une opération ou de plusieurs opérations liées de jeu hors compte, lorsqu'un joueur mise ou gagne des sommes égales ou supérieures à 2 000 euros par transaction.**

Ils enregistrent alors les nom, prénoms, adresse, date et lieu de naissance des joueurs ainsi que le montant des sommes mises et gagnées par ces derniers dans un registre spécifique. Ces informations doivent être conservées pendant 5 ans.

En outre, pour l'offre de jeux de loterie et de paris sportifs en réseau physique de distribution, en cas de demande de **paiement unique de plusieurs lots ou gains** dont le montant total est **supérieur à 300 euros**, le gagnant de ces lots ou gains est identifié et son identité vérifiée dans les mêmes conditions.

Exemples de bonnes pratiques



Afin de mettre en œuvre des mesures leur permettant de **détecter les opérations fractionnées**, l'Autorité recommande, par exemple, d'implémenter une alerte spécifique permettant de repérer les mises placées par un même joueur dans un espace-temps rapproché, dans un même point de vente et dépassant le seuil précédemment cité en plusieurs prises de jeu. Une autre alerte peut cibler les cas où le parieur, se présentant avec un récépissé de gains supérieur à 2 000 euros, souhaite recourir au chèque pari ou demande au point de vente un paiement en espèces. La récurrence de l'encaissement de gains par chèque ou par virement bancaire pour des montants inférieurs au seuil par un même joueur peut également constituer un autre signal d'alerte.

Article 5 : Suivi et analyse des opérations dans le cadre de l'obligation de vigilance

Textes de référence :



- Articles L. 561-6 et L. 561-13 du code monétaire et financier ;
- Articles R. 561-12-1 et R. 561-22-2 du code monétaire et financier ;
- Articles 2 et 4 du décret n° 2010-518 du 19 mai 2010 modifié.

Section 5.1 Principes généraux

- Les opérateurs exercent **une vigilance constante sur le déroulement de leurs relations d'affaires au titre de leurs obligations de lutte contre le blanchiment des capitaux et pratiquent à ce titre un examen attentif des opérations effectuées.**

Section 5.2 Orientations de mise en œuvre

Les opérateurs de jeux doivent exercer **une vigilance constante sur l'activité de leurs clients, afin de prendre en compte tout élément de nature à en modifier le profil de risque.** La connaissance du client doit être **régulièrement actualisée** par l'opérateur.

À cette fin, les opérateurs mettent en place un **dispositif adapté de suivi et d'analyse** des opérations qui doit permettre de définir des critères d'identification des risques en matière de lutte contre le blanchiment des capitaux et de financement du terrorisme.

Les opérateurs apprécient le risque, au regard notamment :

- > des modalités d'alimentation du compte joueur ou de paiement des prises de jeu ;
- > du profil du titulaire du compte joueur ou des éléments en leur possession relatifs aux parieurs et joueurs ;
- > des prises de jeux effectuées ;
- > de la destination des gains éventuels ;
- > des atypismes dans les prises de paris sportifs et hippiques ;
- > des cas de collusion dans les parties de jeux de cercle offertes ;
- > de la possibilité de détention et d'utilisation d'informations privilégiées ;
- > des atypismes dans l'activité des joueurs susceptibles de révéler l'utilisation de robots informatiques ou d'autres moyens susceptibles d'affecter la transparence et l'intégrité du jeu.

Article 6 : Mesures de vigilance complémentaires ou renforcées

Textes de référence :

- Articles L. 561-10, L. 561-10-1 et L. 561-10-2 du code monétaire et financier ;
- Articles R. 561-18, R. 561-20-2, R. 561-20-4, R. 561-20-5 et R. 561-22 du code monétaire et financier.



Section 6.1 Principes généraux

- Les opérateurs appliquent des **mesures de vigilance complémentaires** en présence d'une **personne politiquement exposée** ou domiciliée dans **un pays tiers à haut risque** ou encore lorsque l'offre ou l'opération présente, par sa nature, un **risque particulier** de blanchiment des capitaux ou de financement du terrorisme, notamment lorsqu'elles favorisent l'anonymat.
- Lorsque le risque de blanchiment des capitaux et de financement du terrorisme présenté par une relation d'affaires, une offre ou une opération apparaît élevé, les opérateurs

mettent en place des **mesures de vigilance renforcées** qui consistent principalement à améliorer la connaissance de la clientèle et exercer une surveillance accrue des opérations de jeux.

- Les opérateurs effectuent un **examen renforcé de toute opération particulièrement complexe ou qui présenterait un montant inhabituellement élevé ou paraîtrait dépourvue de justification économique ou d'objet licite**. Dans ce cas, les opérateurs se renseignent auprès du client sur l'origine des fonds et la destination de ces sommes. Les résultats de cet examen renforcé sont consignés par écrit et conservés pendant cinq ans à compter de la clôture du compte joueur pour un joueur sur compte ou à compter de la demande de renseignement pour un autre joueur identifié.

Section 6.2 Orientations de mise en œuvre

En premier lieu, les opérateurs définissent et mettent en œuvre des procédures permettant de déterminer si leur client est une **personne politiquement exposée** ou le devient au cours de la relation d'affaires.

Lorsque le client est une personne politiquement exposée, les opérateurs appliquent **les mesures de vigilance complémentaires suivantes** :

- > ils s'assurent que la décision de **nouer ou maintenir** une relation d'affaires avec cette personne ne peut être prise que par un membre de l'organe exécutif ou toute personne habilitée par lui à cet effet ;
- > ils recherchent, pour apprécier les risques, **l'origine des fonds** impliqués dans la relation d'affaires ou la transaction ;
- > ils renforcent les mesures de vigilance relatives à la **cohérence des opérations** avec les activités professionnelles du joueur, son profil de risque et, si nécessaire, selon l'appréciation du risque, l'origine et la destination des fonds concernés par les opérations.

L'ensemble des mesures d'identification et de gestion de la relation d'affaires avec ces personnes peut s'appliquer jusqu'à un an après la cessation de l'activité exposée à des risques particuliers en raison de fonctions politiques, administratives ou juridictionnelles.

Qui sont les « personnes politiquement exposées » au sens de l'article R. 561-18 du CMF ?

Une personne politiquement exposée est **une personne qui exerce ou a cessé d'exercer depuis moins d'un an l'une des fonctions suivantes** :

- 1° Chef d'Etat, chef de gouvernement, membre d'un gouvernement national ou de la Commission européenne ;
- 2° Membre d'une assemblée parlementaire nationale ou du Parlement européen, membre de l'organe dirigeant d'un parti ou groupement politique soumis aux dispositions de la loi n° 88-227 du 11 mars 1988 ou d'un parti ou groupement politique étranger ;
- 3° Membre d'une cour suprême, d'une cour constitutionnelle ou d'une autre haute juridiction dont les décisions ne sont pas, sauf circonstances exceptionnelles, susceptibles de recours ;
- 4° Membre d'une cour des comptes ;
- 5° Dirigeant ou membre de l'organe de direction d'une banque centrale ;
- 6° Ambassadeur ou chargé d'affaires ;

7° Officier général ou officier supérieur assurant le commandement d'une armée ;

8° Membre d'un organe d'administration, de direction ou de surveillance d'une entreprise publique ;

9° Directeur, directeur adjoint, membres du conseil d'une organisation internationale créée par un traité, ou une personne qui occupe une position équivalente en son sein.

Sont considérées comme des **personnes réputées être des membres directs de la famille** d'une personne politiquement exposée :

1° Le conjoint ou le concubin notoire ;

2° Le partenaire lié par un pacte civil de solidarité ou par un contrat de partenariat enregistré en vertu d'une loi étrangère ;

3° Les enfants, ainsi que leur conjoint, leur partenaire lié par un pacte civil de solidarité ou par un contrat de partenariat enregistré en vertu d'une loi étrangère ;

4° Les ascendants au premier degré.

III. – Sont considérées comme des **personnes étroitement associées** aux personnes mentionnées au I :

1° Les personnes physiques qui, conjointement avec la personne mentionnée au I, sont bénéficiaires effectifs d'une personne morale, d'un placement collectif, d'une fiducie ou d'un dispositif juridique comparable de droit étranger ;

2° Les personnes physiques qui sont les seuls bénéficiaires effectifs d'une personne morale, d'un placement collectif, d'une fiducie ou d'un dispositif juridique comparable de droit étranger connu pour avoir été établi au profit de la personne mentionnée au I ;

3° Toute personne physique connue comme entretenant des liens d'affaires étroits avec la personne mentionnée au I.

Un arrêté du ministre chargé de l'économie fixe la liste des fonctions auxquelles correspondent au plan national celles énumérées ci-dessus.

En second lieu, des mesures complémentaires sont mises en œuvre lorsque les joueurs sont **domiciliés dans un pays considéré comme à risques**.

A cet égard, il convient de rappeler que le GAFI identifie des États qui présentent des vulnérabilités afin de protéger le système financier international : **certains sous surveillance (liste grise) et certains à hauts risques (liste noire)**. Ces listes sont accessibles à l'adresse : <https://www.tresor.economie.gouv.fr/tresor-international/lutte-contre-la-criminalite-financiere/lutte-contre-le-blanchiment-de-capitaux>.

En présence de joueurs présentant ce profil, les opérateurs appliquent, le cas échéant, au moins l'une des mesures suivantes en se fondant sur une approche par les risques :

- des éléments supplémentaires de vigilance renforcée ;
- la mise en place de mécanismes renforcés de suivi ou de signalements destinés notamment au responsable de la mise en œuvre du dispositif de lutte contre le blanchiment et le financement du terrorisme ;
- la limitation des relations d'affaires ou des transactions, ce qui implique notamment que l'opérateur puisse limiter le nombre et le montant des mises d'une personne politiquement exposée.

De plus, l'opérateur doit mettre en place des **mécanismes d'analyse, de surveillance et de recueil d'information** lui permettant d'appréhender les risques identifiés lors de l'analyse prévue à l'article 1^{er} du présent cadre.

Par ailleurs, l'opérateur se livre à un **examen renforcé** afin de lever un doute relatif à une opération de jeu sur la base des informations qu'il a recueillies. Un examen renforcé est appliqué notamment en présence :

- > d'une opération particulièrement complexe ;
- > d'une opération d'un montant inhabituellement élevé ;
- > d'une opération ne paraissant pas avoir de justification économique ou d'objet licite.

Les résultats des examens renforcés, consignés et conservés par écrit, doivent pouvoir être présentés à l'Autorité à sa demande pour lui permettre d'apprécier la matérialité et la pertinence des investigations.

Si l'opérateur conclut avec certitude à la licéité de l'opération, il clôt l'examen renforcé. En revanche, si un doute subsiste après l'examen renforcé, il doit **adresser une déclaration de soupçon à TRACFIN**.

Le délai de recherche et d'approfondissement nécessaire à l'analyse effectuée au titre de la vigilance renforcée ne saurait justifier le refus de **versement d'un solde créditeur ou d'inscription d'un gain au crédit** d'un compte joueur. En effet, les articles 9 et 15 du décret n° 2010-518 du 19 mai 2010 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux prévoient le **versement immédiat** des avoirs du joueur en cas de clôture ou à la demande de celui-ci. A titre exceptionnel, l'opérateur peut légèrement **différer l'inscription d'un gain au crédit du solde du compte joueur et le versement de ce solde sur le compte de paiement du joueur**, mais seulement le temps qui lui est nécessaire pour accomplir la déclaration prévue à l'article L. 561-15 du code monétaire et financier à laquelle il doit procéder, en tout état de cause, dans un bref délai.

Recommandations

- Il est recommandé aux opérateurs de mettre en place des **dispositifs informatiques automatisés** afin d'enrichir leur connaissance des clients nécessitant des mesures de vigilance complémentaires ou renforcées grâce aux informations disponibles dans des bases ouvertes ou auprès de prestataires spécialisés, dans le respect des règles relatives au traitement des données à caractère personnel.
- S'agissant des personnes politiquement exposées, il est recommandé de mettre en œuvre ce dispositif le plus fréquemment possible en fonction de l'évolution des listes disponibles.
- La réception d'une réquisition judiciaire, d'un droit de communication ou d'un appel à vigilance de TRACFIN doit nécessairement conduire l'opérateur **à adapter sa vigilance en conséquence et à réévaluer sa connaissance client**. Dans le cadre du traitement de cette réquisition, les opérations inhabituelles, non identifiées au préalable et non concernées par le champ de la réquisition judiciaire doivent faire l'objet d'une déclaration de soupçon, qui fait mention de l'existence de la réquisition judiciaire ou administrative en indiquant dans la mesure du possible les références et coordonnées du service émetteur.

Des **exemples de démarches** à mener dans le cadre de la mise en œuvre des mesures de vigilance figurent en **annexe II**.

Article 7 : Obligations déclaratives

Textes de référence :

- Articles L. 561-15, L. 561-16, L. 561-22, L. 561-25 et L. 561-30-2 du code monétaire et financier ;
- Articles R. 561-23, R. 561-24, R. 561-27, R. 561-31, R. 561-37 et D. 561-32-1 du code monétaire et financier ;
- Décret n° 2010-518 du 19 mai 2010 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux, art. 9 et 15.

Section 7.1 Principes généraux

- Les opérateurs sont tenus de déclarer au service TRACFIN les sommes inscrites dans leurs livres ou les opérations portant sur des **sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner** qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an, d'une fraude fiscale ou sont liées au financement du terrorisme.
- Les opérateurs doivent s'abstenir d'effectuer toute opération jusqu'à ce qu'elles aient fait la déclaration mentionnée à l'article L. 561-15 du code monétaire et financier. Si l'opération a néanmoins été réalisée, les opérateurs doivent sans délai en informer **TRACFIN**.
- La déclaration, établie **par écrit**, est accompagnée, le cas échéant, de toute pièce utile à son exploitation et comporte les éléments suivants :
 - la fonction de la personne qui effectue la déclaration ;
 - les éléments d'identification et les coordonnées du déclarant désigné ;
 - le type de cas mentionné à l'article L. 561-15 du CMF ;
 - les éléments d'identification du joueur ;
 - un descriptif de l'opération et les éléments d'analyse qui ont conduit à effectuer la déclaration ;
 - lorsque l'opération n'a pas encore été exécutée, son délai d'exécution.
- Toute information de nature à confirmer ou infirmer les éléments d'une déclaration de soupçon précédente est transmise sans délai à TRACFIN.
- La déclaration est **confidentielle** : à l'exception de l'autorité de contrôle, il est interdit de divulguer à un tiers l'existence et le contenu d'une déclaration ainsi que de communiquer tout élément d'information sur les suites réservées à cette déclaration.
- **Aucune action pénale, civile ou disciplinaire** ne peut être engagée à l'encontre des personnes ayant effectué de **bonne foi** des déclarations de soupçons.
- Les opérateurs doivent faire droit aux demandes de communication de documents, informations ou données de TRACFIN dans les délais que ce service fixe.
- Les opérateurs communiquent à l'Autorité et à TRACFIN **l'identité de leurs dirigeants ou préposés habilités à procéder aux déclarations (déclarant) ou de répondre aux**

demandes du service TRACFIN (correspondant). Tout dirigeant ou préposé d'un opérateur doit pouvoir, en situation d'urgence, prendre l'initiative de déclarer lui-même au service TRACFIN, dans des cas exceptionnels une opération suspecte. Cette déclaration est confirmée, dans les meilleurs délais, par la personne habilitée.

- Les opérateurs veillent à ce que les fonctions de correspondant soient assurées avec la **continuité nécessaire** pour être en mesure de répondre, dans les délais impartis, aux demandes de TRACFIN.
- Les correspondants et les déclarants désignés échangent les informations portées à leur connaissance par TRACFIN ainsi que les demandes qui en émanent et répondent à ses sollicitations.

Section 7.2 Orientations de mise en œuvre

Les opérateurs sont tenus de déclarer à TRACFIN les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent :

- d'une infraction passible d'une peine privative de liberté supérieure à un an ;
- d'une fraude fiscale lorsqu'il y a présence d'au moins un critère défini par arrêté.

La liste de ces critères figure en [annexe III](#).

Portée de l'obligation déclarative

La déclaration de soupçon n'est pas un acte anodin car elle entraîne un traitement de l'information déclarée par TRACFIN et peut donner lieu à des investigations complémentaires voire à une transmission à l'autorité judiciaire ou aux administrations mentionnées à l'article L. 561-31 du CMF.

Le champ de la déclaration de soupçon porte sur **toutes les infractions sous-jacentes sanctionnées d'une peine d'emprisonnement supérieure à un an**. Il s'agit notamment du trafic de stupéfiants, de la corruption et du trafic d'influence commis par des personnes exerçant une fonction publique, de l'abus de biens sociaux, de la contrefaçon, de l'escroquerie, de l'abus de confiance, de l'abus frauduleux de l'état d'ignorance ou de la situation de faiblesse, du travail dissimulé, de l'escroquerie.

Les opérateurs n'ont pas à qualifier une infraction sous-jacente, il suffit qu'ils soupçonnent ou aient de « bonnes raisons » de soupçonner qu'elle existe. Ils présentent des faits et l'analyse qui les conduit à effectuer la déclaration de soupçon voire, dans l'hypothèse où ils ont recueilli des éléments leur permettant d'être plus précis, de caractériser le soupçon.

S'agissant plus spécifiquement du **blanchiment de fraude fiscale**, une déclaration n'est envisageable que dans la mesure où au moins l'un des seize critères visés à l'annexe III est rempli. Les éléments d'analyse ayant conduit à retenir au moins l'un des critères doivent être précisés dans la déclaration de soupçon. Il convient de préciser qu'un certain nombre de ces critères **ne peuvent trouver à s'appliquer** au secteur des jeux du fait de l'interdiction du jeu des personnes morales.

Les **tentatives** d'opérations suspectes font également l'objet d'une déclaration à TRACFIN.

Les opérateurs ont une **obligation de réactivité** qui les contraint à veiller à ce que, quelle que soit leur organisation, et à chaque stade du processus conduisant à une déclaration, les diligences soient menées le plus rapidement possible. Ainsi, les opérateurs assujettis veillent à ne prendre que le temps strictement nécessaire aux investigations et à l'analyse faisant suite à l'alerte : lorsque celles-ci sont de nature à justifier le soupçon, les opérateurs rédigent et transmettent la déclaration **sans délai**.

A la suite d'une déclaration de soupçon, l'opérateur peut être amené à établir une **déclaration complémentaire**. Cette déclaration complémentaire doit être effectuée dans les cas où l'opérateur a

connaissance de nouvelles informations de nature à infirmer, conforter ou modifier les éléments contenus dans la déclaration de soupçon initiale. Cette nouvelle déclaration doit être adressée sans délai à TRACFIN.

Rôle des déclarant(s) et des correspondant(s)

Les opérateurs communiquent à l'Autorité et à TRACFIN **l'identité de leurs dirigeants ou préposés habilités à procéder aux déclarations (déclarants)** ou à répondre aux demandes de TRACFIN (correspondants) au moyen d'un document spécifique joint à l'appui de la première déclaration, disponible sur le site internet du service <http://www.economie.gouv.fr/tracfin/declarer>. Tout changement concernant les personnes habilitées doit également être signalé.

Dans les cas exceptionnels, notamment pour un motif d'urgence, tout dirigeant ou préposé d'un opérateur peut prendre l'initiative de déclarer lui-même à TRACFIN. Cette déclaration est confirmée, dans les meilleurs délais, par la personne habilitée.

TRACFIN peut demander que tous documents, informations ou données lui soient communiqués directement dans les délais qu'il fixe, dans le but de reconstituer un ensemble d'opérations liées ou de renseigner ses homologues étrangers.

Les correspondants et déclarants désignés par un opérateur se communiquent les informations portées à leur connaissance par TRACFIN et se tiennent informés des demandes qui en émanent.

Modalités et délais de transmission

Le déclarant peut adresser les déclarations de soupçon à TRACFIN via la plate-forme de télé-déclaration ERMES³, accessible depuis le site Internet de TRACFIN : <https://www.economie.gouv.fr/TRACFIN/declarer>.

Si la télé-déclaration ne revêt pas de caractère obligatoire, la plate-forme ERMES est garante d'un haut niveau de sécurité et de confidentialité. Elle offre en outre l'assurance d'une déclaration recevable et doit donc être privilégiée. Le cas échéant, le déclarant peut également établir une déclaration papier (obligatoirement dactylographiée et signée), à l'aide du formulaire en ligne accessible depuis le site de TRACFIN : <https://www.economie.gouv.fr/TRACFIN/declarer>, à renvoyer par courrier à TRACFIN.

La déclaration **doit en principe être transmise préalablement à l'exécution de la transaction** afin, le cas échéant, de permettre à TRACFIN d'exercer son droit d'opposition. Dans cette hypothèse, la déclaration indique le délai d'exécution de la transaction.

Toutefois, il convient de souligner que **la possibilité pour TRACFIN de s'opposer à l'exécution d'une transaction ne saurait justifier un refus ni même un différé de l'inscription d'un gain au crédit du compte joueur ou du reversement d'un solde de celui-ci sur le compte de paiement du joueur. En effet**, les articles 9 et 15 du décret n° 2010-518 du 19 mai 2010 modifiée relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux posent **un principe d'immédiateté du paiement**. L'opérateur peut seulement « différer » cette inscription et ce paiement le temps nécessaire pour procéder sans délai à la déclaration de soupçon.

Motifs de la déclaration

La déclaration de soupçon est le fruit d'une **analyse des faits en cause par les services de l'opérateur**. Elle ne peut se fonder uniquement sur les résultats d'un traitement automatisé quand bien même celui-ci peut y concourir.

Ainsi, seules des opérations considérées comme suspectes doivent être déclarées à TRACFIN, les opérateurs de jeux et paris n'étant pas soumis à une obligation de déclaration de toutes les opérations

⁴ Mode d'emploi ERMES disponible sur le lien https://www.economie.gouv.fr/files/files/directions_services/tracfin/ERMES_082020.pdf

inhabituelles de leurs clients. Les opérateurs effectuent une déclaration quand le soupçon est établi au terme de l'analyse c'est-à-dire lorsqu'ils n'ont pas obtenu, au regard des informations recueillies auprès du client, une assurance raisonnable de la licéité des fonds utilisés par le joueur.

Facteurs d'alerte

- Doivent notamment constituer des critères d'alertes :
 - la progression forte et inexpliquée, sur une courte période, des sommes créditées sur les comptes nouvellement ouverts ou sur des comptes jusque-là peu actifs ou inactifs, liée le cas échéant à une augmentation importante du nombre et du volume des opérations ;
 - le recours inexpliqué à un ou plusieurs comptes utilisés comme des comptes de passage ou par lesquels transitent de multiples opérations tant au débit qu'au crédit, alors que les soldes des comptes sont souvent proches de zéro ;
 - le refus du client de produire des pièces justificatives relatives à la provenance des fonds ;
 - le dépôt par un joueur de fonds sans rapport avec ses ressources et revenus.
- Au titre des éléments susceptibles de justifier de la transmission d'une déclaration complémentaire, il est notamment possible de mentionner :
 - l'intensification de la pratique de jeux ;
 - la modification des modalités d'alimentation ou de retrait du compte joueur (changement de références de compte de reversement, intensification des alimentations par nouveaux moyens de paiement permettant l'intégration massive d'espèces etc.) ;
 - l'obtention de nouveaux éléments de connaissance client ;
 - l'obtention de documents justificatifs permettant d'infirmer le soupçon initial ;
 - l'identification de comptes joueurs fonctionnant en lien avec le compte ayant fait l'objet d'une déclaration préalable ;
 - la poursuite du rachat de tickets gagnants, etc.

Points de vigilance

- Les déclarations de soupçon ne peuvent avoir pour seul motif :
 - l'activité professionnelle du client, son adresse ou son pays de résidence/naissance (éléments toutefois susceptibles de constituer un faisceau d'indices) ;
 - le montant élevé d'une opération ;
 - le fait que la personne en cause est une PPE.

Contenu de la déclaration

La déclaration expose **l'analyse des faits ayant conduit au soupçon à l'origine du signalement et reprend synthétiquement l'ensemble des éléments** conduisant à sa transmission.

La clarté et la concision de la rédaction présentant les éléments d'information établis dans la déclaration de soupçon sont essentielles pour l'efficacité du dispositif.

Le déclarant transmet, à l'appui de la déclaration, l'ensemble des pièces et données mobilisées lors de la phase d'analyse et notamment, les données financières du compte joueur, les éléments de connaissance du client (*Know your customer, KYC*) ainsi que les données de jeux.

Les données transmises par le déclarant sont susceptibles de faire l'objet d'un retraitement par les enquêteurs de TRACFIN. Par conséquent, il convient de privilégier leur transmission sous format Excel afin de faciliter ce travail d'analyse (ou à défaut, un format .pdf convertible).

L'annexe IV présente les éléments clés que doit comporter une déclaration de soupçon.

Confidentialité et conséquences juridiques de la déclaration

La **confidentialité** de la déclaration de soupçon porte tant sur son existence même que sur son contenu. Elle s'applique également aux suites qui lui sont données. Les informations recueillies à ce titre doivent donc être conservées dans des conditions permettant le respect de cette exigence de confidentialité et sont couvertes par le secret professionnel.

Le caractère confidentiel des déclarations implique que **seuls le(s) correspondant(s) et le(s) déclarant(s) habilités auprès de TRACFIN sont autorisés à détenir des informations relatives à ces déclarations**. Le non-respect de ce principe est sanctionné d'une amende de 22 500 euros (article L. 574-1 du CMF).

En contrepartie de l'obligation légale d'effectuer une déclaration de soupçon à TRACFIN, le professionnel bénéficie d'une **immunité civile, pénale et disciplinaire**. Cela signifie qu'une déclaration de soupçon réalisée de bonne foi exonère le professionnel (article L. 561-22 du CMF) :

- de toute responsabilité pénale, civile et professionnelle pour dénonciation calomnieuse ;
- de toute responsabilité pénale en cas de risque de mise en cause comme auteur ou complice du délit (par exemple de trafic de stupéfiants, de recel, de blanchiment, ou de financement du terrorisme).

La seule **exception à cette exigence de confidentialité vise l'autorité de contrôle** qui peut demander la communication des déclarations effectuées à TRACFIN.

Suite donnée à une déclaration de soupçon

TRACFIN accuse réception de la déclaration.

Dans le cas où la déclaration n'est pas adressée *via* la plateforme de télé-déclaration ERMES et qu'elle ne satisfait pas à l'une des conditions de forme prévues, TRACFIN invite le déclarant à la **régulariser** dans le délai d'un mois en l'informant qu'à défaut de régularisation, elle ne pourra être prise en compte. A défaut de régularisation, le service notifie au déclarant une décision d'irrecevabilité.

La déclaration peut conduire TRACFIN à un **signalement au procureur de la République**, ce dont le déclarant est informé par tout moyen. En cas de risque d'exposition du déclarant, aucune information n'est communiquée.

Les notes d'information transmises à l'autorité judiciaire contiennent diverses informations susceptibles d'avoir été transmises par plusieurs assujettis, de sorte que leur contenu ne permet pas d'identifier le déclarant.

Article 8 : Gel des avoirs

Textes de référence :

- Articles L. 562-1 à L. 562-10 du code monétaire et financier ;
- Articles R. 562-1 à R. 562-4 du code monétaire et financier.



Section 8.1 Principes généraux

- Les opérateurs qui détiennent ou reçoivent des fonds ou des ressources économiques pour le compte d'un client sont tenus d'appliquer **sans délai les mesures de gel et les interdictions de mise à disposition ou d'utilisation** prévues au chapitre II du livre V du code monétaire et financier. Ils en informent immédiatement le ministre chargé de l'économie.
- L'organisation, les procédures mises en place et le contrôle interne évoqués précédemment intègrent la nécessité du respect de cette interdiction.

Section 8.2 Orientations de mise en œuvre

Les pouvoirs publics **peuvent décider, pour une durée déterminée, le gel des fonds et ressources économiques** qui appartiennent à des auteurs ou complices d'actes terroristes en application de dispositions nationales, européennes et internationales (ONU).

Afin de permettre aux opérateurs de satisfaire à leurs obligations, il est établi un **registre national** des personnes et entités faisant l'objet d'une mesure de gel. Ce registre recense l'ensemble des personnes et entités visées par des mesures de gel des avoirs sur le territoire français.

Les opérateurs sont tenus **d'appliquer sans délai les mesures de gel et les interdictions** de mise à disposition ou d'utilisation de ressources des joueurs qui seraient visés par un arrêté de gel des avoirs indépendamment des caractéristiques de l'activité des joueurs concernés.

Le gel des fonds est défini au 5° de l'article L. 562-1 du CMF comme toute action tendant **à empêcher un changement de leur volume, montant, localisation, propriété, possession, nature, destination** ou toute autre modification qui pourrait permettre leur utilisation.

En matière de jeux d'argent et de hasard, cela signifie qu'une mesure de gel empêche l'opérateur :

- d'ouvrir un compte joueur au nom de la personne visée par la mesure ;
- d'enregistrer une mise.

En revanche, une mesure de gel :

- n'entraîne pas la clôture du compte ouvert auprès de l'opérateur ;
- n'empêche pas de déposer des fonds sur un compte joueur préalablement gelé dès lors que les fonds versés sont immédiatement gelés. L'opérateur informe immédiatement la Direction générale du Trésor de toute opération effectuée ainsi au crédit du compte joueur. »
- n'empêche pas l'inscription d'un gain généré par une mise antérieure à la mesure de gel au crédit du compte joueur, le solde de ce compte demeurant gelé.

Enfin, les opérateurs peuvent, en application de l'article L. 562-7 du CMF, transférer des fonds appartenant à une personne visée par une mesure de gel vers un compte préalablement gelé. Les opérateurs s'assurent du fait que le compte destinataire est préalablement gelé en demandant à la Direction générale du Trésor l'autorisation d'effectuer l'opération.

Afin de remplir leur obligation de gel des avoirs, les opérateurs doivent **mettre en place un outil de détection des personnes** désignées par arrêté dans la base de données clientèle. Le paramétrage du dispositif, la fréquence de filtrage (qui doit en tout état de cause correspondre aux mises à jour du registre national des personnes et entités faisant l'objet d'une mesure de gel) et le délai de traitement des alertes doivent permettre de remplir efficacement cette obligation de gel des avoirs.

Ce dispositif doit notamment permettre aux opérateurs :

- lors de **l'entrée en relation d'affaires**, de détecter les personnes dont le nom, le prénom ou l'alias sont identiques ou se rapprochent, avec un taux raisonnable de concordance, des éléments d'identification d'une personne figurant sur les listes publiées au *Journal officiel* ;
- en **cours de relation d'affaires**, dans les mêmes conditions, de détecter en permanence dans leur base clientèle la présence des personnes qui feraient l'objet d'une telle mesure ;
- de réaliser des recherches sur les bases ouvertes disponibles afin de vérifier la concordance d'identité.

Dès qu'ils ont connaissance d'une mesure de gel affectant un joueur, les opérateurs **en informent immédiatement le ministre chargé de l'économie**⁴.

De même, en cas d'impossibilité d'écarter une homonymie, ils soumettent une déclaration d'homonymie à la Direction générale du Trésor⁵.

Le cas échéant, ils déclarent sans délai au service TRACFIN les opérations susceptibles d'être liées au financement du terrorisme.

Le non-respect par les opérateurs de leurs obligations en matière de gel des avoirs est susceptible de fonder l'engagement d'une procédure de sanction devant la commission nationale des sanctions, qui peut prononcer l'une des sanctions prévues par les dispositions de l'article L. 561-40 du code monétaire et financier. Par ailleurs, l'opérateur qui contribuerait sciemment et volontairement à apporter des fonds à une personne ayant fait l'objet d'une mesure de gel des avoirs est passible des peines prévues à l'article 459 du code des douanes.

Recommandations



- Le registre national des gels est accessible à l'adresse : <https://gels-avoirs.dgtresor.gouv.fr/>
- L'ONU et le Conseil de l'Union européenne peuvent adopter des mesures restrictives financières ou commerciales à l'encontre de personnes physiques, morales ou d'autres entités. Ces mesures prennent la forme de sanctions économiques, il est recommandé aux opérateurs de consulter la page : <https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques>
- Afin de disposer des dernières mises à jour du registre (nouveaux gels, modifications, radiations), les opérateurs sont invités à s'abonner au « Flash Info gel » soit via un lien direct sur cette même page soit en envoyant un message à info-gel-subscribe@listes.finances.gouv.fr avec pour objet « abonnement à la liste info-gel ».
- Les modalités d'utilisation d'une API sont également précisées sur cette page.

⁴ Adresses fonctionnelles : liste-nationale@dgtresor.gouv.fr (terrorisme) ou sanctions-gel-avoirs@dgtresor.gouv.fr (Sanctions)

⁵ <https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/signaler-un-cas-d-homonymie>

Chapitre III : Lutte contre la fraude

Prise dans son acception classique, la fraude comporte deux éléments :

- un **élément matériel**, en premier lieu, consistant en l'usage de moyens légaux (alimentation du compte joueur au moyen d'un instrument de paiement anonyme et demandes fréquentes de reversement associées à une faible activité de jeu) ou illégaux (falsification d'un document d'identité pour jouer), permettant à son auteur de bénéficier d'un droit ou d'un avantage en vertu d'une règle à l'application de laquelle il ne peut normalement prétendre ;
- un **élément intentionnel**, en second lieu, résidant dans la volonté de celui qui emploie ces moyens de bénéficier d'un droit ou d'un avantage auquel il sait ne pas pouvoir normalement prétendre. Le plus souvent, l'élément intentionnel se déduit de l'élément matériel.

Il importe de préciser que la caractérisation d'une fraude suppose le recueil d'éléments probants et que l'opérateur ne saurait refuser le paiement d'un gain ou le reversement d'une partie ou de la totalité du solde d'un compte sur la base de simples soupçons, sauf à porter atteinte au principe de la force obligatoire du contrat de jeu. En tout état de cause, l'opérateur informe sans délai l'Autorité de son refus de payer un joueur et expose à cette occasion les circonstances de fait et de droit qui le motive.

Le présent cadre de référence **n'a pas vocation à appréhender la totalité des cas de fraude envisageables**. Il appartient aux opérateurs de faire preuve de vigilance, en accordant un soin particulier aux opérations de jeu ou de compte qui, prises isolément ou ensemble, sont susceptibles de révéler une pratique frauduleuse pour en déceler éventuellement les nouvelles formes. C'est aussi par ce biais que, conformément aux dispositions de l'article L. 320-4 du code de la sécurité intérieure, les opérateurs « *concourent* » à la réalisation de l'objectif défini au 3° de l'article L. 320-3 du même code consistant à « *prévenir les activités frauduleuses* ». Différentes hypothèses sont abordées dans ce cadre.

Les conflits d'intérêt et le détournement des services de l'entreprise

Sont visés les manquements aux dispositions du I de l'article 32 de la loi du 12 mai 2010 modifiée et aux dispositions communes relatives à la probité : le propriétaire, les dirigeants, les mandataires sociaux et le personnel d'un opérateur de jeux ou de paris en ligne titulaire d'un agrément délivré par l'ANJ ne peuvent engager, à titre personnel, directement ou par personne interposée, des mises sur des jeux ou des paris proposés par cet opérateur. Sont également visées, pour l'ensemble des opérateurs, l'utilisation des biens et services de l'opérateur à d'autres fins que celles prévues à son objet social (abus) ou que son intérêt économique.

La fraude au jeu résultant de l'utilisation d'un robot informatique

L'alinéa 4 de l'article 2 du décret n° 2016-1326 du 6 octobre 2016 relatif aux catégories de jeux de cercle mentionnées au II de l'article 14 de la loi n° 2010-476 du 12 mai 2010 interdit le jeu assisté par un robot informatique et fait obligation à l'opérateur de garantir la sincérité des jeux.

La fraude au jeu par entente ou collusion

Il résulte de la combinaison du 2° et 3° de l'article 320-3 du code de la sécurité intérieure, de l'article L. 320-4 du même code et du troisième alinéa de l'article 18 de la loi du 12 mai 2010 modifiée que l'opérateur doit garantir la sincérité des opérations de jeux et concourir à la lutte contre les activités frauduleuses et criminelles, obligation rappelée pour le poker à l'alinéa 4 de l'article 2 du décret du 6 octobre 2016.

L'atteinte à l'intégrité des compétitions sportives ou hippiques

Il résulte de la combinaison du 3° de l'article L. 320-3 du code de la sécurité intérieure, de l'article L. 320-4 du même code et du troisième alinéa de l'article 18 de la loi du 12 mai 2010 modifiée que l'opérateur doit concourir à la lutte contre les activités frauduleuses et criminelles, ce qui implique qu'il contribue à la **prévention et à la lutte contre les manipulations sportives** dans la mesure de ses moyens et des informations et documents en sa possession.

En revanche, il convient de préciser que **la fraude visant à exploiter d'éventuelles failles de sécurité des systèmes d'information n'est pas visée** en l'espèce dès lors que les dispositifs à mettre en œuvre et les échanges y afférents avec l'ANJ sont précisés dans les exigences techniques définies en application du VIII de l'article 34 de la loi du 12 mai 2010.

Article 9 : Elaboration d'une analyse des risques



Textes de référence :

- Articles 17, 18 et 32 de loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;
- Article 2 du décret n° 2016-1326 du 6 octobre 2016 relatif aux catégories de jeux de cercle mentionnées au II de l'article 14 de la loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;
- Article 4 du cahier des charges de la Française des jeux tel que défini par le décret n° 2019-1060 du 17 octobre 2019 relatif aux modalités d'application du contrôle étroit de l'Etat sur la société La Française des jeux ;
- Article 11 du décret n° 2019-1061 du 17 octobre 2019 relatif à l'encadrement de l'offre de jeux de La Française des jeux et du Pari mutuel urbain.

Section 9.1 Principes généraux

- L'opérateur met en place des procédures et des moyens adaptés pour prévenir et lutter contre la fraude, ce qui implique notamment la mise en place **d'un système d'alertes et de détection des atypismes** fondé sur une identification et un suivi de qualité de l'activité des joueurs, dans le respect des règles relatives à la protection des données à caractère personnel.
- Au-delà des hypothèses de fraude visées par le cadre de référence, les opérateurs doivent prendre **toutes les mesures utiles pour prévenir d'autres types de manœuvres frauduleuses**.
- Les **propriétaires, dirigeants, mandataires sociaux et le personnel des opérateurs agréés de jeu en ligne ne peuvent engager, à titre personnel, directement ou par personne interposée, des mises sur des jeux** ou des paris de cet opérateur.
- Dans l'hypothèse de **comptes tests nécessaires à l'activité**, une procédure et un plan de contrôle de la **bonne utilisation** des comptes joueurs des personnels sont définis par écrit.

Section 9.2 Orientations de mise en œuvre

Conflit d'intérêts et détournement des outils et services de l'entreprise

Les opérateurs titulaires d'un agrément de jeu en ligne s'assurent, sous le contrôle de l'Autorité, que leur organisation et leurs moyens permettent de **faire obstacle à des prises de pari ou à la participation à leurs jeux à des fins personnelles, directes ou indirectes, par leur propriétaires, dirigeants, mandataires sociaux et personnels.**

Ils mettent également en place un fonctionnement et une organisation ayant pour objet d'interdire l'utilisation des biens, pouvoirs ou voix de la société à d'autres fins que celles prévues par leur objet social.

Les personnes pouvant avoir un intérêt personnel direct ou indirect dans un événement support de paris, notamment en matière de paris hippiques, doivent en informer leur employeur au moyen d'une déclaration formalisée transmise ensuite à l'Autorité.

Recommandations



- En matière de lutte contre les conflits d'intérêts et de fraude interne, **la mise en place d'un dispositif de gestion des risques, le déploiement d'une procédure *ad hoc* de contrôle des opérations de jeu ou de pari et l'insertion de clauses pénales dans le contrat de travail** sont recommandées.
- L'opérateur prend toute mesure pour empêcher que l'exploitation des comptes tests porte atteinte à la sincérité des opérations de jeux et aux intérêts des joueurs.

Systèmes automatisés de jeu

Les opérateurs **mettent en place des outils permettant de détecter et de faire obstacle à l'utilisation de moyens informatiques assistant ou se substituant** aux joueurs.

Exemples de bonnes pratiques



- Les opérateurs mettent en place **des outils de détection et d'obstruction à l'utilisation de robots informatiques** combinant la détection statistique et comportementale en temps réel.
- Ces outils visent à identifier **les incohérences de jeu ou le fonctionnement anormal d'un compte joueur** à partir d'indicateurs tels que le temps de réaction du joueur, le positionnement des clics de la souris, l'analyse comportementale de jeu ou encore les temps de jeu effectif.
- Les opérateurs peuvent également définir dans leurs conditions générales d'utilisation quels types de dispositifs d'aide peuvent ou non être utilisés.

Jeu en équipe

Les opérateurs mettent en œuvre une politique générale et des moyens **afin de prévenir, quelle qu'en soit la cause, les ententes de joueurs, notamment sur les tables de poker, l'utilisation de plusieurs comptes joueurs depuis le même ordinateur, le partage de compte** et les faits pouvant s'apparenter à des « prêts » entre joueurs.

Dans le cadre de jeu sous la forme mutuelle, et particulièrement du poker, les opérateurs sont tenus de garantir la sincérité des opérations de jeux en assurant notamment **un suivi étroit, dans le respect des dispositions légales applicables en matière protection de la vie privée, des communications** entre les joueurs.



Exemples de bonnes pratiques

- Une vigilance constante est portée sur l'activité des joueurs jouant régulièrement ensemble.

Lancement d'une nouvelle offre ou évolution de l'offre existante

Avant le lancement d'une nouvelle offre de jeu ou de pari ou à l'occasion de modification apportée à une offre existante, l'opérateur procède à une **évaluation spécifique des risques qu'elle suscite** et, le cas échéant, met en place des mesures pour les prévenir ou les atténuer.



Recommandations

- L'Autorité recommande aux opérateurs de mettre en place des seuils de mise, notamment pour les nouveaux jeux ou à l'occasion de l'introduction de nouvelles modalités de l'offre (par exemple : nouvelle variante de poker, nouveau type de pari hippique).

Article 10 : Organisation et moyens

Textes de référence :

- Articles 17, 18, 21, 27 et 34-X de la loi n° 2010-476 du 12 mai 2010 modifiée.

Section 10.1 Principes généraux

- La mise en place d'une **bonne gouvernance en matière de lutte contre la fraude** participe à la protection de l'ordre public.
- A cette fin, les opérateurs se dotent **d'une organisation et de procédures adaptées aux enjeux de lutte contre la fraude** ainsi que de procédures de **contrôle interne**.
- Le dispositif de lutte contre la fraude inclut notamment des indicateurs de suivi pertinents et les opérateurs doivent être en capacité permanente d'en rendre compte à l'Autorité.

Section 10.2 Orientations de mise en œuvre

Les opérateurs mettent en place une organisation **adaptée afin de prévenir et lutter contre la fraude**.

L'ensemble des procédures est **formalisé par écrit** et l'effectivité de leur mise en œuvre doit faire l'objet de **contrôles internes**.

Les opérateurs **doivent pouvoir justifier** à tout moment de l'existence et de la permanence des procédures mises en place et de l'adéquation du soutien matériel et financier au service en charge de la lutte contre la fraude.

Article 11 : Qualité de l'identification et de la connaissance des joueurs



Textes de référence :

- Article 17 de la loi n° 2010-476 du 12 mai 2010 ;
- Décret n° 2010-518 du 19 mai 2010.

- L'organisation mise en place doit permettre de **vérifier l'identité de chaque nouveau joueur**, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont reversés ses avoirs. L'approvisionnement du compte joueur par son titulaire doit être conditionné au respect de la nature et de la domiciliation des moyens de paiement.

Au-delà des obligations définies par le CMF, la **qualité de l'identification** permet également de lutter contre les tentatives de contournements des joueurs interdits de jeux ou bénéficiant d'une mesure d'auto-exclusion. Aussi, dans un objectif d'efficacité de lutte contre la fraude documentaire, les mesures d'identification évoquées plus haut trouvent ici pleinement à s'appliquer.

Points d'attention



En complément des mesures recommandées en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, l'Autorité préconise :

- la mise en œuvre de mesures spécifiques complémentaires au dispositif prévu à l'article 22 du décret n° 2010-518 du 19 mai 2010 visant à **empêcher les personnes inscrites sur les fichiers des interdits de jeu** de participer à des jeux d'argent et de hasard ;
- la mise en place par les opérateurs de mesures de contrôle adaptées permettant **d'identifier des tentatives d'inscription par des personnes bénéficiant d'une mesure d'auto-exclusion**.

Ces mesures ont pour objectif de contrer les tentatives de contournement des dispositifs de protection en mettant en place une procédure de détection des personnes dont le nom, les prénoms ou l'alias sont identiques ou proches, avec un taux raisonnable de concordance, des éléments d'identification d'une personne désignée. Il convient notamment d'empêcher la création de nouveaux comptes, y compris provisoires, en procédant à des comparaisons des éléments mentionnés par les joueurs (incluant, mais ne se limitant pas, à l'adresse, le numéro de téléphone, le courriel, les adresses IP ou les coordonnées bancaires). Le cas échéant, la procédure d'inscription devra être suspendue de façon à interroger la personne concernée sur son homonymie ou tout autre élément similaire à plusieurs joueurs.

Article 12 : Prévention et lutte contre les manipulations des compétitions sportives et hippiques

Textes de référence :

- Articles 12 et 34 de loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;

▪ Article 4 du cahier des charges annexé au décret n° 2019-1060 du 17 octobre 2019 relatif aux modalités d'application du contrôle étroit de l'Etat sur la société La Française des jeux.

Section 12.1 Principes généraux

- Dans le cadre de la mission de surveillance des opérations de jeux d'argent et de hasard qui lui est conférée par l'article 34 de la loi n° 2010-476 du 12 mai 2010 modifiée **l'Autorité nationale des jeux reçoit, centralise, analyse pour la plateforme nationale de lutte contre les manipulations sportives les signalements relatifs aux paris atypiques et suspects** pris sur des compétitions sportives organisées ou ouvertes aux paris sur le territoire français.
- **La liste des compétitions ou manifestations sportives et des types de résultats** sur lesquels des paris sportifs sont autorisés, en tout ou partie, **est tenue par l'Autorité nationale des jeux au regard notamment des risques de manipulation** que les compétitions ou manifestations sportives présentent.
- La présidente de l'Autorité nationale des jeux peut, **s'il existe des indices graves et concordants de manipulation d'une compétition ou manifestation sportive** inscrite sur la liste ci-dessus, **interdire, pour une durée qu'elle détermine**, tout pari sur celle-ci. L'organisateur de la compétition ou manifestation sportive peut la saisir à cette fin.
- Les opérateurs **détectent et informent sans délai l'Autorité nationale des jeux des atypismes dans les prises de paris offerts**.

Section 12.2 Orientations de mise en œuvre

La lutte contre la manipulation de compétitions sportives ou d'épreuves hippiques fait partie intégrante de la lutte contre la fraude à laquelle participent les opérateurs agréés ou sous droits exclusifs. Le périmètre de la lutte contre la fraude sportive et hippique **couvre les manipulations de compétitions sportives ou de courses hippiques en lien avec les paris**.

Les opérateurs **prennent les mesures de veille nécessaires à la détection de manœuvres pouvant avoir pour objet ou pour effet de modifier le résultat ou le déroulement d'une compétition sportive ou d'une course hippique**.

Lorsqu'ils détectent une anomalie ou une opération suspecte, ils **en informent sans délai l'Autorité**.

Exemples de bonnes pratiques



- La mise en place d'un **dispositif de gestion des risques relatifs à la manipulation des compétitions sportives** ou hippiques est fortement recommandée. Les indices de fraude sur lesquels les opérateurs doivent se fonder peuvent être notamment :
 - la constatation de déréférencements des offres et cotations sur une compétition ;
 - le montant atypique des mises enregistrées (notamment sur les paris dérivés pris avant le début des rencontres sportives) ;

- la nature atypique des paris (proportion de paris suspecte, prévalence de paris portant sur un résultat très précis, cotes/rapport élevés, chiffre d'affaires anormal sur un événement/une course au regard de l'historique des paris) ;
 - le mouvement inexplicable d'une cote ou d'un rapport ;
 - une information détenue par l'opérateur, de quelque nature que ce soit, qui permettrait de soupçonner une manipulation de compétition ;
 - la concentration géographique des mises par compte joueur ou par points de vente s'agissant de l'offre en réseau physique ;
 - la connaissance d'un détaillant/partenaire entretenant des liens avec un acteur de compétition.
- Les opérateurs de paris sportifs sont invités à **prévoir dans leur règlement de jeu l'anéantissement des paris portant sur une compétition ou manifestation sportive ayant fait l'objet d'une décision d'interdiction** des paris prise par la présidente de l'ANJ en application du V de l'article 12 de la loi du 12 mai 2010 modifiée.
 - Afin de **faciliter les échanges avec l'ANJ**, les opérateurs sont invités à désigner un ou des **interlocuteurs dédiés** afin que les services de l'Autorité puissent les informer de décisions d'interdiction et permettre leur mise en œuvre dans le délai le plus bref.

Article 13 : Information générale de l'ANJ

Section 13.1 Principes généraux

- Toute **constatation ou suspicion d'une fraude nouvelle, lorsqu'elle revêt un niveau suffisant de gravité, est portée à la connaissance de l'Autorité**, par écrit.
- Une **analyse générale des fraudes ou tentatives de fraudes** dont l'opérateur a pu faire l'objet durant l'année est réalisée dans le cadre du plan d'actions.

Section 13.2 Orientations de mise en œuvre

Les opérateurs doivent **informer l'Autorité de la survenance d'une fraude, de sa nature et des moyens qui l'ont permise ainsi que des mesures correctrices envisagées ou mises en place.**

L'analyse des fraudes contenue dans le plan d'actions s'attache à distinguer, le cas échéant, les différents types de fraude dont l'opérateur a fait l'objet, en mettant en évidence les fraudes les plus remarquables (soit par leur volume, soit par leur caractère inhabituel ou novateur).



Clause de rendez-vous

Afin d'assurer la légitimité et l'efficacité des lignes directrices qu'il dessine, le cadre de référence doit s'inscrire au cœur des réalités du secteur et des pratiques du jeu, lesquelles sont en mutation constante.

Par ailleurs, afin de mieux appréhender la diversité des situations concrètes du secteur, les orientations de ce cadre doivent pouvoir faire l'objet d'adaptations sans pour autant porter atteinte à la stabilité et la prévisibilité du cadre de régulation applicable.

Compte tenu de ces remarques, le cadre de référence doit pouvoir évoluer dans son contenu.

L'ANJ dressera un premier bilan de la mise en œuvre du cadre de référence, de façon concertée avec les opérateurs et l'ensemble des parties prenantes, **un an après son entrée en vigueur**. Elle proposera les modifications qui s'avèreraient nécessaires pour renforcer la réalisation des objectifs en matière de lutte contre la fraude et contre le blanchiment de capitaux et le financement du terrorisme qui constitue sa raison d'être.

Annexe I : Classification des risques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

Exemples

Risques liés à la personne

- ✓ personne politiquement exposée ;
- ✓ personne faisant l'objet d'une mesure de gel des avoirs ;
- ✓ personne faisant l'objet d'une demande d'informations provenant d'une autorité publique ;
- ✓ profil de joueur atypique au regard de la clientèle type de l'opérateur ;
- ✓ exploitant d'un poste d'enregistrement en réseau physique de distribution bénéficiant de gains de façon régulière ;
- ✓ similitudes de comportements entre plusieurs comptes joueurs ou, en poker, informations permettant de mettre le compte en relation avec d'autres comptes joueurs (compte de reversement/adresse postale/adresse mail/numéro de téléphone/adresse IP, device).

Risques liés aux données de connexion

- ✓ cohérence des données de connexion : connexion depuis l'étranger, multiplication des machines utilisées, utilisation d'un VPN.

Risques liés aux données financières

Alimentation

- ✓ dépôts par un moyen de paiement adossé à un compte de paiement domicilié en dehors du territoire national ;
- ✓ tentatives d'alimentation rejetées ;

	<ul style="list-style-type: none"> ✓ dépôts par un nouveau moyen de paiement ou favorisant l'anonymat (monnaie électronique, tickets et codes pré payés) ; ✓ fragmentation des opérations de dépôt ; ✓ alimentation du compte joueur par cartes de paiement multiples ; ✓ absence de cohérence entre les données relatives au titulaire du compte joueur et le document mentionnant l'identité du titulaire du moyen de paiement ; ✓ opérations d'alimentation faisant suite à des retraits (absence de recyclage des gains) ; ✓ alimentation d'un montant important au regard de l'historique du compte ; ✓ monétisation de carte de paiement volée ; ✓ poursuite des alimentations sur un solde élevé ; ✓ alimentation par des récépissés gagnants (opérateurs titulaires de droits exclusifs) ; ✓ série de mises dans un laps de temps très court ; ✓ même moyen de paiement (CB, code prépayé ...) utilisé pour alimenter plusieurs comptes joueurs.
Retrait	<ul style="list-style-type: none"> ✓ retraits effectués sur un compte de paiement ouvert auprès d'un prestataire établi hors de France ; ✓ retraits réguliers à partir d'adresses IP étrangères ; ✓ retraits de montants importants ; ✓ tentatives de retraits de sommes n'ayant pas ou peu fait l'objet d'enjeux ; ✓ absence de recyclage des gains ; ✓ clôture d'un compte avec un solde important ; ✓ modifications fréquentes de comptes de reversement ;

	<ul style="list-style-type: none"> ✓ retraits sous forme de petits lots cumulés ou de chèques inférieurs au seuil des 2 000 euros (opérateurs titulaires de droits exclusifs) ; ✓ retraits par rachat de tickets gagnants par un joueur collecteur de reçus ou d'individus manifestement associés (opérateurs titulaires de droits exclusifs) ; ✓ consultations multiples d'un ticket gagnant avant le paiement.
--	---

Risques liés au service (jeux)

- ✓ type de jeu (expertise/hasard) ;
- ✓ principe (répartition/contrepartie) ;
- ✓ taux de retour joueur théorique ;
- ✓ taux de retour joueur réel ;
- ✓ facilité à se procurer des preuves de gains.

Risques liés aux opérations de jeu

Paris sportifs	<ul style="list-style-type: none"> ✓ prises de paris sportifs importantes sur des cotes très faibles ; ✓ prises de paris sportifs sur l'ensemble des issues possibles d'une compétition ; ✓ arbitrages effectués entre les différentes offres du marché afin d'obtenir un retour sur investissement en spéculant sur les TRJ (« surebet ») ou sur les cotes ; ✓ prises de jeux récurrentes sur des offres de paris annulées ; ✓ prises de paris sportifs très diversifiées ne permettant pas de déterminer un profil joueur et permettant de suspecter un rachat de tickets gagnants.
-----------------------	--

<i>Jeu de cercle</i>	<ul style="list-style-type: none"> ✓ opérations de jeu réalisées sur des tables dont les « blinds » sont élevées ; ✓ opérations de jeu entre joueurs fréquemment présents sur les mêmes tables ; ✓ opérations de jeu réalisées en duel (« heads-up ») ; ✓ transfert illicite de jetons d'un joueur à un autre lors d'une partie (« chip dumping ») ; ✓ inscriptions à des tables puis sorties sans avoir effectué d'opérations de jeu.
<i>Paris hippiques</i>	<ul style="list-style-type: none"> ✓ prises de paris hippiques très diversifiées ne permettant pas de déterminer un profil joueur et permettant de suspecter un rachat de tickets gagnants ; ✓ mises importantes sur un cheval favori ; ✓ mises importantes sur un rapport final s'avérant être très faible (atteignant le seuil limite de rapport minimum autorisé).
<i>Loterie</i>	<ul style="list-style-type: none"> ✓ incohérence dans les informations fournies par le gagnant.

Risques liés au réseau de distribution

- ✓ forte augmentation soudaine du chiffre d'affaires de l'exploitant d'un poste d'enregistrement ;
- ✓ concentration géographique de paiements de tickets gagnants ;
- ✓ fréquence des paiements composés d'opérations de paris enregistrées simultanément à divers endroits ;
- ✓ positionnement du poste d'enregistrement de vente dans une zone sensible ;
- ✓ rachat de reçus gagnants par le détaillant ;
- ✓ horaire d'enregistrement atypique des prises de jeu ou de paiement des gains (au moment de l'ouverture ou de la fermeture du point de vente) ;

- ✓ fréquence de cession d'un point de vente ;
- ✓ présence de machines-à-sous ;
- ✓ détaillant ayant des liens avec le sport (entraîneur, président de club, etc...) ;
- ✓ repérage d'un ensemble de postes d'enregistrement en lien avec le même atypisme sur des prises de pari ;
- ✓ nombreux gains perçus par le détaillant ;
- ✓ distance géographique entre l'adresse du détaillant et l'adresse déclarée par le joueur.

Annexe II : Exemples pratiques

1. Exemples de mise en œuvre d'une démarche d'analyse suite à la détection d'un critère d'alerte

Exemple 1
Identification d'une alerte liée aux modalités d'alimentation du compte joueur
<p>Critère d'alerte justifiant un examen renforcé de la relation d'affaires</p> <p>M. X, 23 ans, détenteur d'un compte depuis 2 ans, enregistre depuis quelques mois une progression significative de ses enjeux, qui se matérialise notamment par une fréquentation quasi-quotidienne du site de l'opérateur.</p> <p>Les montants engagés justifient une analyse destinée à s'assurer de l'adéquation des sommes engagées avec le profil du client.</p> <p>Recherches effectuées sur les éléments de connaissance client</p> <p>Le client se situe dans le profil type de la clientèle de l'opérateur.</p> <p>Le client ne dispose pas d'antériorité dans la base client. Aucune information le concernant n'est disponible en bases ouvertes.</p> <p>Analyse des opérations de jeux</p> <p>Le client se distingue par une stratégie très agressive en matière de paris sportifs, engageant ponctuellement des sommes importantes sur des paris à cote élevée. Son taux de retour joueur se situe en dessous de la moyenne, le conduisant à des pertes conséquentes. Également actif sur le poker, le client démontre un niveau d'expertise convenable et fréquente ponctuellement des tables à <i>blind</i> élevées.</p> <p>Analyse des éléments financiers</p> <p>L'alimentation du compte joueur s'effectue exclusivement par carte bancaire, via 4 CB différentes sur 2 ans.</p> <p>Les recherches effectuées sur la base du code INN des CB permettent de constater que trois de ces cartes sont adossées à des établissements estoniens ayant fait l'objet de sanctions par leur autorité de contrôle.</p> <p>Résultat de l'analyse</p> <p>Le client se distingue par une pratique de jeux non conforme à sa surface financière supposée. La détention de comptes à l'étranger par une jeune personne physique constitue un critère d'alerte additionnel.</p> <p>L'opérateur sollicite auprès du joueur des justificatifs concernant l'origine des sommes mises. Le joueur indique développer une activité de prestataire informatique à la suite d'une première expérience professionnelle en Estonie. Il fournit dans ce cadre des bulletins de salaire français et estoniens. Les revenus mentionnés sur ces documents sont de nature à justifier les sommes engagées sur le site de l'opérateur.</p> <p>La procédure de placement sous vigilance renforcée de la relation d'affaires prend fin. L'opérateur considère qu'une déclaration de soupçon ne se justifie pas à ce stade. En revanche, un accompagnement au titre de la lutte contre l'addiction s'avère nécessaire.</p>

Exemple 2

Identification d'une alerte liée aux prises de jeux

Critère d'alerte justifiant un examen renforcé de la relation d'affaires

L'opérateur identifie dans ses bases de données une cliente de 45 ans, Mme X, sollicitant à de nombreuses reprises des remboursements à la suite de prises de jeux concernant des événements sportifs non avendus. Cette technique concerne par exemple des prises de jeux concernant le 3ème set d'une rencontre de tennis *a priori* destinée à se dérouler en deux sets, car déséquilibrée.

La conjonction des atypismes liée au profil atypique du client et à ses modalités de jeux (paris susceptibles d'être annulés ou dont les cotes sont très faibles) justifie un examen renforcé de la relation d'affaires.

Recherches effectuées sur les modalités de fonctionnement du compte joueur

La première année, le compte se caractérise par une très faible activité de jeux. Les alimentations portent sur des montants significativement plus élevés les années suivantes. Il est essentiellement alimenté par des tickets pré payés, et dans une moindre mesure par des cartes bancaires.

L'opérateur identifie 26 CB, dont 7 ont effectivement abouti à des paiements ; 4 de ces CB sont émises dans un pays frontalier de la France.

La cliente procède par ailleurs à de fréquents changements de compte de reversement des gains : en 7 mois, 6 comptes sont successivement désignés, dont 4 sont étrangers (pays distincts de celui des CB utilisées pour l'alimentation du compte) et un adossé à un établissement de monnaie électronique⁸.

Une de ces CB est également utilisée pour l'alimentation du compte joueur d'un autre client de l'opérateur, M. Y.

Recherches effectuées en base ouverte et sur demandes de justification

Mme X est aide-soignante dans un EHPAD. Les montants engagés sur le compte joueur par cartes pré payées représentent l'équivalent d'une année de salaire moyen de cette profession. Son activité ne justifie pas la détention de comptes bancaires dans 4 pays étrangers. Enfin, aucun élément ne permet de justifier les liens entre Mme X et M. Y, ce dernier résidant à plusieurs centaines de kilomètres de Mme X.

Résultat de l'analyse

Mme X ne semble pas s'inscrire dans une pratique ludique. Les montants engagés semblent sans rapport avec la surface financière supposée du client. Par ailleurs, l'utilisation de nombreuses CB par une personne physique exerçant ses fonctions au sein d'établissements favorisant un contact avec une population vulnérable permet de soupçonner un potentiel abus de faiblesse.

La détention d'un nombre élevé de comptes étrangers, ainsi que les liens non justifiés avec un autre compte joueur conduisent l'opérateur à la transmission d'une déclaration de soupçon, suite à une tentative de prise de contact infructueuse avec les joueurs.

Exemple 3

Identification d'une alerte liée au compte de reversement des gains

Critère d'alerte justifiant un examen renforcé de la relation d'affaires

M. X procède, en cours de relation d'affaires, à la désignation d'un nouveau compte de reversement des gains. Lors d'un contrôle de routine, il apparaît que l'IBAN transmis désigne un compte adossé à un portefeuille de monnaie électronique.

Contactée par les services commerciaux de l'opérateur, la personne physique indique « ne pas vouloir laisser de traces sur son compte bancaire », sans plus de précision.

Suite à ces échanges, l'opérateur effectue une analyse de la relation d'affaires.

Recherches effectuées sur les éléments de connaissance client

Les éléments transmis par le client lors de l'ouverture du compte joueur permettent de dresser un profil *a priori* du client : il s'agit d'une jeune personne physique (23 ans), habitant un arrondissement central de Paris. Les recherches effectuées sur internet sur la base de l'adresse communiquée permettent d'identifier un immeuble bourgeois.

Les recherches effectuées dans la base client permettent de constater que le client a successivement détenu 6 comptes joueurs, dont certains n'ont jamais fait l'objet de validation. Ces comptes sont adossés à 4 adresses postales distinctes.

La consultation des bases ouvertes met en évidence la gestion par M. X de nombreuses sociétés, la plupart radiées après une période d'activité de quelques mois. Les secteurs d'activités concernés présentent une sensibilité en matière fiscale : société de commerce de produits électroniques sur internet, société de conseil pour les affaires et conseil de gestion, etc.

Analyse des opérations de jeux

Le client est exclusivement actif sur les paris sportifs. Il place des mises élevées sur des cotes faibles. Très occasionnellement, des enjeux mineurs sont effectués sur des cotes élevées.

Analyse des éléments financiers

Le client alimente son compte joueur exclusivement par cartes et tickets pré payés. Fait notable, les alimentations se poursuivent lorsque le client dispose d'un solde élevé sur son compte joueur.

Par ailleurs, les sommes ayant fait l'objet d'enjeux sont immédiatement retirées, le joueur procédant par la suite à de nouvelles alimentations (absence de recyclage des gains).

L'analyse des comptes précédemment créés par le joueur met en évidence de fréquents changements de domiciliation bancaire. En effet, par-delà le portefeuille de monnaie électronique récemment désigné par le joueur, 4 comptes adossés à des établissements bancaires distincts ont successivement été désignés par le client.

Identification de critères d'alerte additionnels en cours d'analyse

L'instabilité bancaire du client laisse présager de difficultés rencontrées avec ses établissements bancaires successifs.

Démarche entreprise par l'opérateur

L'opérateur contacte le client afin d'obtenir des justificatifs de l'origine des fonds (bulletin de salaire, avis d'imposition, etc.). Ce dernier indique ne pas être en mesure de justifier l'origine des fonds, s'agissant d'argent liquide versé en guise de pourboire.

Résultat de l'analyse

L'origine des fonds est indéterminée.

Le client alimente son compte joueur par des nouveaux moyens de paiement, susceptible de favoriser l'intégration d'espèces.

Les sommes engagées semblent conséquentes au regard du profil client : ce dernier, relativement jeune, n'exerce pas d'activité stable permettant de justifier d'une activité de jeu significative.

Le client ne semble pas s'inscrire dans une pratique ludique.

Les fréquentes opérations liées aux alimentations et retraits successifs sur le compte joueur, ainsi que les prises de jeux effectuées sur des rencontres sans réelle incertitude ne correspondent pas à une pratique ludique.

L'ensemble de ces éléments conduit l'opérateur à transmettre une déclaration de soupçon.

Exemple 4

Identification d'une tentative de retrait sans enjeux liée à une problématique d'usurpation d'identité

Critère d'alerte justifiant un examen renforcé de la relation d'affaires

Les équipes de l'opérateur consultent l'outil de *reporting* permettant l'identification des comptes joueurs objet de tentatives de retraits sans enjeux.

Un examen rapide des résultats permet l'identification de caractéristiques communes à 4 de ces comptes :

- une localisation commune (ville de résidence) ;
- l'ensemble de ces comptes a été créé la même semaine, dont deux le même jour ;
- l'essentiel des approvisionnements s'effectue par cartes pré payées ;
- les adresses mails indiquées lors de la création du compte présentent des similitudes (adossées au même opérateur internet peu utilisé en France, l'identifiant de ces adresses présente par ailleurs une base identique).

A ce stade, il est possible de s'interroger sur le possible recours à des identités d'emprunt. En conséquence, le déclarant effectue une analyse élargie à l'ensemble de sa base client, afin de détecter d'autres comptes impliqués dans une tentative de dissimulation.

Recherches effectuées sur les éléments de connaissance client

- Adresses postales :
 - deux rues de la ville identifiée concentrent respectivement 18 et 13 titulaires de comptes, dont une part déterminante à une adresse identique. Au total, 32 comptes joueurs sont logés dans la même commune, ouverts sur un intervalle de deux mois (concentration des ouvertures à certaines dates) ;
 - une facture d'électricité transmise à des fins de justificatif de domicile présente une police non conforme à celle traditionnellement utilisée par l'opérateur électrique. Ce dernier, contacté par l'opérateur de jeux, confirme le caractère frauduleux du document ;
- Adresses mail : parmi les 32 comptes joueurs, 30 présentent une adresse mail avec une extension identique, dont 17 présentent un identifiant partiellement identique (x.x00@).
- Anomalies dans les documents justificatifs transmis lors de la création des comptes joueurs initialement non détectés :

- aucune pièce d'identité ne mentionne une adresse identique à celle déclarée par les joueurs lors de l'ouverture de leur compte ;
- deux comptes joueurs alimentés par la même CB (cf. *supra*) ont transmis des pièces d'identité faisant figurer des états civils différents mais une photo identique.

Analyse des éléments financiers

- Compte de reversement des gains : parmi les 32 comptes, 28 ont communiqué des RIB adossés à un établissement bancaire identique. Cet opérateur, acteur récent du marché bancaire, entretient une relation d'affaires à distance avec ses clients qui présente une vulnérabilité liée aux emprunts d'identité.
- Modalités d'alimentation : 15 comptes joueurs ont été alimentés par 46 CB distinctes. 5 de ces comptes partagent des alimentations effectuées par une même CB (4 CB concernées). Un 33^{ème} compte en lien est identifié par ce biais. L'analyse des opérations d'alimentation par cartes pré payées met par ailleurs en évidence des opérations d'un montant identique, réalisées le même jour, sur des comptes adossés à des titulaires différents.

Résultat de l'analyse

Les titulaires des comptes ne s'inscrivent pas dans le profil type de la clientèle de l'opérateur (âge, genre). De nombreux éléments permettent de présager une usurpation d'identité.

Les modalités de fonctionnement des comptes permettent de présager une démarche d'intégration d'espèces d'origine indéterminée (cartes pré payées, absence de réelle opération de jeux).

L'ensemble des éléments collectés permet d'identifier 33 comptes fonctionnant en lien (éléments de connaissance client, éléments financiers).

Le déclarant transmet sans délai une déclaration de soupçon.

2. Exemples d'informations complémentaires à demander suite à la détection d'un critère d'alerte

Critères d'alerte	Mesures de vigilance
Alimentations successives du compte joueur par cartes et codes pré payés, portant sur un total élevé	Sollicitation d'une copie des tickets avec référence visible (élément permettant de s'assurer que le titulaire du compte a effectivement acheté les tickets) Sollicitation d'un extrait de compte bancaire faisant apparaître un achat de tickets ou cartes pré payés
Alimentations portant sur des montants importants	Sollicitation d'un justificatif de revenus
Doute concernant l'identité du titulaire du compte joueur (problématique d'usurpation d'identité)	Sollicitation d'une photo webcam présentant une caractéristique particulière (portrait accompagné de la présentation d'une pièce d'identité par exemple)
Tentative de retrait sans enjeux	Demander des explications concernant la motivation de l'opération

3. Exemples de critères d'alertes associés aux principaux risques dans le secteur des jeux en ligne

Le transfert de sommes de compte à compte par le biais d'un compte joueur (éventuellement par l'alimentation du compte par un/des tiers)
<p>L'article 17 de la loi n° 2010-476 du 12/05/2010 précise que le compte joueur ne peut être alimenté que par son titulaire. Toutefois, dans les faits, l'opérateur ne dispose pas d'éléments lui permettant de s'assurer du respect de cette disposition. Ainsi, rien ne garantit que les codes pré payés utilisés dans le cadre de l'alimentation d'un compte joueur ont effectivement été achetés par le titulaire du compte, ni que les opérations d'alimentation par carte bancaire sont effectuées par une CB adossée à un compte bancaire au nom du titulaire du compte joueur.</p> <p>Cette limite favorise le transfert de sommes de compte à compte dans une optique de blanchiment, notamment lors de la phase d'empilage.</p> <p><u>Les critères d'alerte associés à ce risque sont notamment :</u></p> <ul style="list-style-type: none">– les dépôts effectués par des moyens de paiement favorisant l'anonymat ;– l'alimentation du compte joueur par de multiples CB ;– les changements fréquents de comptes de reversement ;– les retraits effectués au bénéfice d'un compte domicilié dans un établissement de crédit en dehors du territoire national, l'absence de recyclage des gains, etc.

L'usurpation d'identité / le recours à un titulaire d'emprunt
<p>Les opérateurs de jeux en ligne sont particulièrement exposés au risque d'usurpation d'identité et de création de comptes joueurs adossés à des titulaires d'emprunt, en raison de l'entrée en relation d'affaires à distance.</p> <p><u>Les critères d'alerte associés à ce risque sont notamment :</u></p> <ul style="list-style-type: none">– l'identification d'informations permettant de faire le lien avec d'autres comptes joueurs de la base client de l'opérateur (compte de reversement, adresse postale, adresse mail, numéro de téléphone, adresse IP, device) ;– les données de connexion incohérentes (localisation de l'adresse IP différente de l'adresse postale) ;– l'absence de cohérence entre le titulaire du compte joueur et les informations transmises concernant le titulaire du moyen de paiement ;– les retraits réguliers à partir d'adresses IP étrangères, le reversement des gains sur un compte adossé à un établissement bancaire entretenant des relations d'affaires à distance.

L'intégration d'espèces dans le système bancaire
<p>Certains moyens de paiement, autorisés par la réglementation européenne, sont susceptibles de favoriser l'intégration d'espèces d'origine illicite dans le système bancaire.</p> <p><u>Les critères d'alerte associés à ce risque sont notamment :</u></p> <ul style="list-style-type: none">– les dépôts par nouveau moyen de paiement ou favorisant l'anonymat ;

- la fragmentation des opérations de dépôt ;
- l’absence de recyclage des gains ;
- la poursuite des alimentations sur un solde élevé ;
- la clôture d’un compte avec un solde important ;
- la prise de paris sportifs importantes sur un concurrent/équipe favorite ;
- des prises de jeux récurrentes sur des offres de paris annulées ;
- les mises importantes sur un cheval favori.

4. Exemples d’analyse des données bancaires collectées

L’évaluation de la sensibilité LCB-FT des données bancaires nécessite de déterminer la provenance des fonds, leur destination, et de s’interroger sur un éventuel différentiel entre ces données.

Analyse des informations liées à l’alimentation du compte joueur					
<p>Les numéros de cartes bancaires sont encadrés par une norme internationale (ISO/IEC 7812) fixant leur nombre total à 18 chiffres. Les huit premiers chiffres sont propres à l’établissement émetteur de la carte et constituent le code IIN (<i>Issuer Identification Number</i>).</p> <p>Des moteurs de recherche spécialisés, disponibles en bases ouvertes, permettent sur cette base de déterminer l’établissement émetteur du moyen de paiement, ainsi que son pays d’établissement.</p>					
Analyse des informations liées aux opérations de retrait des gains					
<p>La structure des codes IBAN présent sur les RIB transmis par les joueurs à des fins de reversement des gains, permet la mise en œuvre de recherches similaires.</p> <p>Des moteurs de recherche spécialisés, disponibles en bases ouvertes, permettent également la collecte de plus amples informations concernant l’établissement bancaire concerné.</p>					
Code ISO pays	Clef de contrôle	RIB			
		Code banque	Code guichet	Numéro de compte	Clé du RIB
FR	33	3002	00550	0000157841Z	25
<p>La confrontation des données issues de l’analyse des références des cartes bleues utilisées dans le cadre de l’alimentation du compte et de l’IBAN de reversement des gains permet ainsi d’éclairer le comportement financier du joueur : transfert de sommes de compte à compte, alimentation du compte par un tiers, utilisation de moyens de paiement étrangers, etc.</p>					

Annexe III : Soupçon de fraude fiscale

L'article L. 561-15 II du code monétaire et financier prévoit un **traitement particulier pour la fraude fiscale**.

Lorsqu'un opérateur sait, soupçonne ou a de bonnes raisons de soupçonner que les sommes ou opérations suspectes proviennent d'une fraude fiscale, **il ne déclare à TRACFIN** ces sommes ou opérations que lorsqu'il y a **présence d'au moins un des 16 critères** ci-dessous, étant précisé que **certains ne peuvent trouver à s'appliquer** notamment du fait de l'interdiction du jeu des personnes morales.

- ✓ utilisation de sociétés écran, dont l'activité n'est pas cohérente avec l'objet social ou ayant leur siège social dans un État ou un territoire qui n'a pas adhéré à la norme relative à l'échange de renseignements sur demande à des fins fiscales, ou à l'adresse privée d'un des bénéficiaires de l'opération suspecte... ;
- ✓ réalisation d'opérations financières par des sociétés dans lesquelles sont intervenus des changements statutaires fréquents non justifiés par la situation économique de l'entreprise ;
- ✓ recours à l'interposition de personnes physiques n'intervenant qu'en apparence pour le compte de sociétés ou de particuliers impliqués dans des opérations financières ;
- ✓ réalisation d'opérations financières incohérentes au regard des activités habituelles de l'entreprise ou d'opérations suspectes dans des secteurs sensibles aux fraudes à la TVA de type carrousel, ... ;
- ✓ progression forte et inexpliquée, sur une courte période, des sommes créditées sur les comptes nouvellement ouverts ou jusque-là peu actifs ou inactifs, liée le cas échéant à une augmentation importante du nombre et du volume des opérations ou au recours à des sociétés en sommeil ou peu actives dans lesquelles ont pu intervenir des changements statutaires récents ;
- ✓ constatation d'anomalies dans les factures ou les bons de commande lorsqu'ils sont présentés comme justification des opérations financières, telles que l'absence du numéro d'immatriculation au registre du commerce et des sociétés, du numéro SIREN, du numéro de TVA, de numéro de facture, d'adresse ou de dates ;
- ✓ recours inexpliqué à des comptes utilisés comme des comptes de passage ou par lesquels transitent de multiples opérations tant au débit qu'au crédit, alors que les soldes des comptes sont souvent proches de zéro ;
- ✓ retrait fréquent d'espèces d'un compte professionnel ou leur dépôt sur un tel compte non justifié par le niveau ou la nature de l'activité économique ;
- ✓ difficulté d'identifier les bénéficiaires effectifs et les liens entre l'origine et la destination des fonds en raison de l'utilisation de comptes intermédiaires ou de comptes de professionnels non financiers comme comptes de passage, ou du recours à des structures sociétaires complexes et à des montages juridiques et financiers rendant peu transparents les mécanismes de gestion et d'administration ;
- ✓ opérations financières internationales sans cause juridique ou économique apparente se limitant le plus souvent à de simples transits de fonds en provenance ou à destination de l'étranger notamment lorsqu'elles sont réalisées avec des États ou des territoires visés plus haut ;
- ✓ refus du client de produire des pièces justificatives quant à la provenance des fonds reçus ou quant aux motifs avancés des paiements, ou l'impossibilité de produire ces pièces ;

- ✓ transfert de fonds vers un pays étranger suivi de leur rapatriement sous la forme de prêts ;
- ✓ organisation de l'insolvabilité par la vente rapide d'actifs à des personnes physiques ou morales liées ou à des conditions qui traduisent un déséquilibre manifeste et injustifié des termes de la vente ;
- ✓ utilisation régulière par des personnes physiques domiciliées et ayant une activité en France de comptes détenus par des sociétés étrangères ;
- ✓ dépôt par un particulier de fonds sans rapport avec son activité ou sa situation patrimoniale connue ;
- ✓ réalisation d'une transaction immobilière à un prix manifestement sous-évalué.

Annexe IV : Précisions sur la présentation et le contenu de la déclaration de soupçon

1) L'exposé de la déclaration de soupçon

Partie 1 : phrase introductive de synthèse

Cette partie doit permettre une compréhension rapide du signalement et consiste à synthétiser l'ensemble des éléments fondant le soupçon.

Partie 2 : présentation des personnes physiques faisant l'objet du soupçon

Rappel des informations détenues par le déclarant sur les personnes physiques objet du soupçon.

Personnes physiques :

- situations personnelle et professionnelle connues ;
- adresse postale déclarée ;
- historique de la relation d'affaires (date d'entrée en relation d'affaires, rappel de l'historique des comptes joueurs successivement ouverts auprès de l'opérateur).

Le déclarant mentionne dans cette partie, le résultat des recherches effectuées en base ouverte concernant le client (réseaux sociaux, bases commerciales, etc.).

Partie 3 : présentation des opérations

- synthèse des opérations et des mouvements suspects ;
- développement des faits concernant ces opérations ;
- précision sur l'origine et la destination (certaine ou présumée) des fonds sur lesquels porte le soupçon.

L'analyse effectuée par le déclarant porte conjointement sur les données financières (modalités d'alimentation et de retrait des gains du compte joueur), sur le comportement du joueur manifestant une volonté d'obtenir des preuves de gains pour ensuite justifier l'origine des fonds arrivant sur son compte bancaire, la méthodologie de jeu (notamment au regard de la prise de risques), les éventuels liens entretenus avec d'autres comptes joueurs, le taux de retour joueur, le rapport au risque du joueur, etc.

Partie 4 : caractérisation du soupçon

Cette partie restitue le fait à l'origine du soupçon ayant conduit au signalement, expose clairement le soupçon du déclarant à l'appui des éléments figurant supra.

- En quoi cette opération est-elle suspecte ?
- Pourquoi l'origine des fonds peut paraître suspecte ?
- Démarches entreprises par le déclarant pour lever le doute ?
- En quoi les explications ou justifications apportées sont-elles peu convaincantes ou crédibles ?

2) Les pièces jointes à la déclaration de soupçon

- Documents récapitulatifs des éléments de connaissance client :

- copie de la pièce d'identité du client ;
- copie des RIB associés au compte joueur ;
- tableau récapitulatif de l'ensemble des éléments de connaissance client (adresse postale, mail, adresse IP, numéro de téléphone, etc.) ;
- tableau récapitulatif des adresses IP de connexion associées au compte joueur (idéalement réparties par nombre de connexion).

- Document de synthèse des données financières faisant figurer, par année :

- les approvisionnements ventilés par type de prestataire de paiement ;
- sur ce point, si plusieurs cartes bancaires sont utilisées par le joueur, ventiler les alimentations par CB.
- les retraits par compte destinataire ;
- les enjeux par offre de jeux (paris hippiques/jeux de cercle/paris sportifs).

- Document présentant le détail des opérations financières :

Un document détaillant l'ensemble des opérations d'alimentation et de retrait sera également joint (y figureront, le cas échéant : la date de l'opération, le moyen de paiement [vecteur de paiement ou marque liée au prestataire de service de paiement], le montant de l'opération, l'adresse IP de connexion, l'adresse MAC, les informations nécessaires liées à l'opération [référence liée au prestataire de paiement, référence CB, référence du ticket pré payé, etc.]).

- Document présentant le détail des opérations en matière de paris sportifs et hippiques :

Montant de la prise de jeux, cote associée, résultat de la prise de jeu et événement sportif / hippique concerné.

- Documents attestant de la pratique de rachats de tickets gagnants :

Lorsque les comptes joueurs déclarés sont alimentés de manière significative par des codes et tickets pré payés, il convient de faire figurer dans les pièces jointes dédiées le numéro d'identification de ces derniers. Cette information permet aux enquêteurs TRACFIN d'adresser des droits de communication à leur éditeur, dans l'objectif d'obtenir de plus amples informations concernant les modalités de commercialisation des tickets et codes pré payés utilisés.

Annexe V : Catégorisation des risques en matière de lutte contre la fraude

Exemples

Risques liés aux jeux

- ✓ prise de paris sur des événements sportifs ou hippiques sur lesquels existent des forts soupçons de manipulation ;
- ✓ opérations de jeu réalisées entre des participants sur lesquels existent de forts soupçons de collusion ;
- ✓ opérations de jeu sur lesquels il existe de forts soupçons d'utilisation de robots informatiques.

Risques liés aux moyens de paiement ou à l'utilisation de documents d'identité

- ✓ ouvertures de comptes/justification d'identité à l'aide des documents sur lesquels existent un fort soupçon de contrefaçon, d'usurpation ou de falsification ;
- ✓ dépôt/paiement avec un moyen de paiement sur lequel existe un fort soupçon de vol ou d'usage abusif.

Risques internes

- ✓ opérations de jeu ou de pari effectuées par le propriétaire, les dirigeants, les mandataires sociaux et le personnel d'un opérateur ;
- ✓ gestion des comptes joueurs en conflit avec l'intérêt de l'entreprise ;
- ✓ détection de l'activité atypique d'un membre du personnel de l'opérateur.