Publication de juillet 2021

de la Revue de l'ACPR

# Premier bilan de l'enregistrement des PSAN

**La loi PACTE du 22 mai 2019 prévoit que les prestataires de services sur actifs numériques (PSAN) sont enregistrés par l'Autorité des marchés financiers (AMF) sur avis conforme de l'ACPR. Depuis l'entrée en vigueur de ce régime, l'ACPR a émis une vingtaine d'avis favorables à l'enregistrement de PSAN.**

**Deux ans après la loi PACTE, retrouvez dans cet article les points importants à faire figurer dans les dossiers de candidature.**

## Le rôle de l'ACPR en matière d'enregistrement des prestataires de services sur actifs numériques

La loi PACTE du 22 mai 2019 impose aux PSAN offrant (i) un service de conservation pour le compte de tiers d'actifs numériques ou d'accès à ces actifs ou (ii) un service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal d'être enregistrés par l'AMF avant le démarrage de leurs activités. Depuis l'ordonnance n° 2020-1544 du 9 décembre 2020[1], les PSAN proposant le service d'échange entre actifs numériques ou exploitant une plateforme de négociation d'actifs numériques doivent également être enregistrés par l'AMF.

Conformément à l'article L. 54-10-3 du code monétaire et financier (CMF), l'AMF enregistre les PSAN après avoir recueilli l'avis conforme de l'ACPR. Avant qu'un avis formel soit rendu et pour fluidifier la procédure, les services de l'AMF et de l'ACPR échangent sur tous les aspects d'un dossier de candidature et désignent pour chaque dossier une équipe composée d'analystes des deux autorités.

À cette fin, l'AMF et l'ACPR vérifient que les dirigeants et bénéficiaires effectifs du prestataire possèdent l'honorabilité et la compétence nécessaires à l'exercice de leurs fonctions. Plusieurs dirigeants de sociétés candidates ont dû, pour répondre à ces exigences, suivre des formations sur la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) et sur les risques de blanchiment de capitaux et de financement du terrorisme (BC-FT) liés aux actifs numériques, avant de bénéficier de l'enregistrement. Il est important que toutes les personnes n'ayant pas occupé de fonctions en lien avec la LCB-FT suivent une formation dans ce domaine. Cette formation doit être d'une durée suffisante et adaptée à l'activité des PSAN. Par ailleurs, pour apprécier la compétence, l'ACPR prend en considération, au vu des interactions avec le candidat, sa capacité à prendre

[1] Ordonnance n°2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques.

effectivement en compte les risques de BC-FT lors de la conception ou de la modification du modèle d'affaires.

Dans la mesure où l'ACPR est, après l'enregistrement, l'autorité en charge du contrôle du respect de la réglementation LCB-FT, elle examine tout particulièrement cet aspect du dossier afin de rendre son avis à l'AMF. L'ACPR vérifie la mise en place d'une organisation et de procédures propres à assurer le respect des obligations du PSAN en la matière : elles doivent être adaptées à la taille, à la nature des activités et des services fournis ainsi qu'aux risques de BC-FT identifiés par le prestataire.

## Identification des risques de blanchiment de capitaux et de financement du terrorisme et classification des risques

Le PSAN doit identifier et évaluer les risques de BC-FT auxquels il est exposé et mettre en place une politique adaptée à ces risques. À cette fin, il doit élaborer une classification des risques en fonction de la nature des produits ou 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 (article L. 561-4-1 du CMF).

L'expérience des dossiers examinés montre l'importance de soumettre aux autorités d'enregistrement des classifications complètes (couvrant l'ensemble des risques) et tenant compte les spécificités du modèle d'activité de chaque prestataire.

L'ACPR s'est ainsi assurée que les classifications des risques des prestataires prenaient en compte, conformément à l'article 2 de l'arrêté du 6 janvier 2021[2], les analyses nationale[3] et sectorielle des risques[4], les typologies de blanchiment de capitaux et de financement du terrorisme mentionnées dans les rapports de Tracfin[5] ainsi que les indicateurs de risques liés aux actifs virtuels figurant dans le rapport du GAFI de septembre 2020[6]. D'autres documents peuvent également nourrir la classification des risques des PSAN comme l'analyse supranationale des risques de la Commission européenne[7] ou l'analyse des risques de l'Autorité bancaire européenne[8].

L'Autorité a vérifié que la classification des risques des prestataires prenait en compte de façon aussi complète que possible les risques de BC-FT auxquels leurs activités les exposaient, y compris les risques spécifiques aux actifs numériques comme les rançongiciels (*ransomwares*)[9], en les déclinant dans les axes pertinents de la classification.

À titre d'exemple, un client exerçant son activité dans un secteur à risque, l'utilisation par ce dernier d'un VPN ou d'un navigateur de type Tor doivent figurer comme indicateurs de risques dans l'axe

---

[2] Arrêté du 6 janvier 2021 relatif au dispositif et au contrôle interne en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et de gel des avoirs et d'interdiction de mise à disposition ou d'utilisation des fonds ou ressources économiques.

[3] Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France du COLB, septembre 2019.

[4] Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme en France de l'ACPR, décembre 2019.

[5] Tracfin diffuse des typologies de blanchiment de capitaux ou de financement du terrorisme dans ses rapports d'activité et dans ses rapports d'analyse (consultables ici).

[6] *FATF Report – Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, septembre 2020.

[7] *Supranational risk assessment (SNRA)* de la Commission européenne, juillet 2019.

[8] *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector,* mars 2021.

[9] V. sur ce point l'analyse sectorielle des risques de l'ACPR, §5.2., p. 58.

« caractéristiques des clients » de la classification des risques. De même, le PSAN doit distinguer dans l'axe « nature des produits ou des services offerts » de sa classification les risques de BC-FT liés aux différents actifs numériques proposés, les *privacy coins* et les *anonymity-enhanced cryptocurrencies* (AEC) qui reposent sur des *blockchains* non traçables étant par nature plus risqués en raison de leurs fonctions d'anonymisation qui ne permettent pas de connaître avec certitude l'origine et la destination de ces actifs.

L'axe « conditions de transactions » doit notamment permettre de distinguer les risques de BC-FT liés à l'utilisation des différents modes de paiement (virement SEPA, carte bancaires, espèces, etc.). Enfin, les prestataires doivent veiller à ce que l'axe « pays ou territoire d'origine ou de destination des fonds » prenne notamment en compte les listes figurant à l'article 2 de l'arrêté du 6 janvier 2021 ainsi que, le cas échéant, d'autres facteurs de risque géographiques (risques associés à l'existence de zones de conflits, etc.).

Dans le cadre de l'instruction, les services de l'ACPR se sont également assurés que la classification des risques permettait de déterminer un profil de risque pour chaque relation d'affaires ainsi que les mesures de vigilance associées. Cette note de risque de chaque relation d'affaires doit être suffisamment discriminante pour permettre d'assurer une vigilance adaptée selon une approche par les risques. Elle ne saurait conduire à classer la quasi-totalité des clients ou des opérations en risque faible et doit avoir une influence sur l'intensité des mesures de vigilance mises en œuvre, tant en ce qui concerne la connaissance actualisée de la clientèle qu'en ce qui concerne la surveillance des opérations.

## Identification, vérification d'identité et connaissance de la relation d'affaires

L'identification et la vérification d'identité des clients en relation d'affaires par l'utilisation des modes de vérification d'identité admis par la réglementation (articles R. 561-5-1 à R. 561-5-2 du CMF) est un point-clé dans le cadre de l'enregistrement. Pour que la conformité à ces dispositions des demandes d'enregistrement soit suffisamment anticipée par les prestataires, ils sont invités à consulter les lignes directrices de l'ACPR sur ce sujet.

Les PSAN sont désormais tenus d'identifier et de vérifier l'identité de tous leurs clients, y compris leurs clients occasionnels, conformément au décret n° 2021-387 du 2 avril 2021 relatif à la lutte contre l'anonymat des actifs virtuels[10].

Lorsque l'activité d'un prestataire le conduit à avoir une clientèle en relation d'affaires et des clients occasionnels (notamment les services hors conservation), l'ACPR a veillé à ce que les critères retenus pour identifier ces deux types de clientèle soient suffisamment précis, adaptés au modèle d'affaires et conformes à l'article L. 561-2-1 du code monétaire et financier, afin de mettre en œuvre des vigilances adaptées, notamment au titre de la connaissance actualisée des relations d'affaires.

À cet égard, l'Autorité a veillé à ce que les PSAN disposent d'informations suffisamment précises, notamment, sur la profession, le secteur d'activité et les revenus du client. Ces informations sont en effet indispensables à l'exercice de la vigilance constante et à la surveillance des opérations.

[10] Décret n°2021-387 du 2 avril 2021 relatif à la lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme modifiant l'article R. 561-10 du CMF.

## Dispositif de surveillance des opérations

Les risques identifiés dans la classification doivent être pris en compte dans le dispositif de surveillance des opérations. En particulier, il appartient au prestataire de définir des scénarios et seuils d'alerte ou d'autres mesures de détection permettant couvrir l'ensemble des risques, notamment pour identifier les opérations devant faire l'objet d'un examen renforcé au sens de l'article L. 561-10-2 du CMF.

Le degré d'approfondissement des obligations de vigilance est fonction du niveau de risque de la relation d'affaires ou du type d'actifs numériques tel qu'il apparaît dans la classification des risques et les scénarios. En tout état de cause, le PSAN doit être en mesure d'analyser les flux de transactions, en amont et en aval, ainsi que l'adresse publique d'envoi et de réception des actifs numériques. À cette fin, il a souvent paru nécessaire que les PSAN se dotent d'un outil d'analyse transactionnelle de la *blockchain* dont des travaux de place ont souligné l'utilité dans un dispositif de LCB-FT[11]. L'utilisation d'un outil d'analyse transactionnelle permet aux PSAN d'avoir une meilleure visibilité sur les flux d'actifs numériques, en amont et en aval. À titre d'illustration, ces outils permettent de mettre en œuvre, par la technique du « *clustering* », des typologies de blanchiment de type « *many-to-one* » ou « *one-to-many* » dans le cadre de la surveillance des opérations.

Dans des conditions particulières, l'enregistrement a pu être délivré à un PSAN qui, sans recourir à un outil d'analyse transactionnelle de *blockchain,* mettait en œuvre d'autres mesures garantissant une vigilance adaptée aux risques (en particulier, vente d'un seul type d'actif numérique sur une *blockchain* publique, recours à un explorateur en ligne de *blockchain* permettant à l'organisme assujetti de connaître la provenance et de s'assurer de l'absence de mouvement des actifs numériques de la part du client, etc.).

Au titre du risque géographique (article L. 561-4 du CMF), l'ACPR est attentive à la prise en compte d'une gamme large de facteurs, y compris la nationalité, l'adresse du client, la résidence fiscale, la localisation des numéros de téléphone ou adresses IP utilisées en cas de relation à distance, la source ou la destination de fonds (s'agissant par exemple des comptes ou cartes utilisés par le client pour payer un achat ou recevoir le prix d'une vente).

En raison des risques de BC-FT plus importants qui leur sont associés, les candidats doivent mettre en place des mesures de vigilance renforcées lorsqu'ils fournissent des services liés à des *privacy coins* ou à des AEC[12]. L'Autorité a par exemple admis le dispositif LCB-FT d'un PSAN qui prévoyait notamment le déclenchement systématique d'un examen renforcé en cas de vente par un client d'un *privacy coin* ou d'un AEC, impliquant le recueil auprès du client de documents permettant d'assurer la traçabilité de ces actifs numériques (justificatifs, factures ou autres preuves d'achat, motif économique motivant l'acquisition ou la vente du produit, recueil d'éléments sur l'origine ou la destination de l'actif numérique conformément à l'article L. 561-10-2 du CMF), ainsi que des vérifications complémentaires par l'utilisation d'un outil d'analyse transactionnelle de *blockchain* quand cette analyse reste possible.

## Déclaration de soupçon à Tracfin

Dans les cas prévus par l'article L. 561-15 du CMF, les PSAN doivent adresser une déclaration de soupçon à Tracfin. L'ACPR a vérifié que les PSAN avaient mis en place un dispositif assurant notamment

[11] V. le rapport du groupe de travail du Forum Fintech ACPR-AMF sur l'application des règles de LCB-FT au secteur des crypto-actifs, juillet 2020.

[12] Sur ce point, v. l'analyse sectorielle des risques de l'ACPR, §5.2, p. 58 ainsi que le rapport « Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme 2017-2018 » p. 58. V. également les *Red Flag Indicators* du GAFI p. 9.

la continuité de l'activité déclarative en cas d'absence du déclarant Tracfin ou en cas d'urgence, ainsi que la confidentialité des déclarations de soupçon.

## Mise en œuvre des mesures de gel des avoirs

Conformément à l'article L. 562-4 du CMF, les PSAN sont tenus d'appliquer sans délai les mesures de gel et les interdictions de mise à disposition et d'en informer immédiatement le ministre de l'économie. Dans le cadre de l'instruction des demandes d'enregistrement, l'ACPR vérifie que le dispositif du candidat permet de satisfaire à cette exigence. Les candidats sont invités à se référer aux lignes directrices conjointes de l'ACPR et de Tracfin sur la mise en œuvre des mesures de gel des avoirs.

Le dispositif de gel des avoirs du prestataire, qui doit prendre en compte les listes française et européenne de sanction, doit permettre de détecter toute personne faisant l'objet d'une mesure de gel des avoirs ou d'interdiction de mise à disposition selon des modalités qui en assure l'efficacité (critères de correspondance orthographique, fréquence du filtrage, etc.)

Par ailleurs, en cas de transfert d'actifs numériques vers une adresse publique dont le PSAN n'assure pas la conservation au sens du 1° de l'article L. 54-10-2 du CMF, l'ACPR s'est assurée que le PSAN recueillait des éléments sur l'adresse publique de destination des actifs numériques et le bénéficiaire du transfert. Ces diligences doivent être effectuées avant le transfert d'actifs numériques vers l'adresse publique dont le PSAN n'assure pas la conservation afin de permettre, le cas échéant, la mise en œuvre de la mesure d'interdiction de mise à disposition.

L'enregistrement par l'AMF sur avis conforme de l'ACPR est prononcé sur la base des éléments transmis aux deux autorités. Une fois enregistrés, il appartient aux établissements d'adapter leurs dispositifs de LCB-FT et de gel des avoirs à toute évolution de leur activité, telle qu'une augmentation du nombre de clients ou d'opérations, une modification des produits proposés, de la clientèle ciblée, des canaux de distribution, etc. L'adaptation de l'organisation et des procédures devra aussi tenir compte du retour d'expérience, par exemple des résultats du contrôle interne, des scénarii de détection ou des classifications de clientèle qui se révèleraient à l'usage insuffisamment pertinents, ainsi que de l'évolution des typologies de blanchiment ou des menaces de financement du terrorisme.