Novembre 2022

Principes d'application sectoriels relatifs aux prestataires de services sur actifs numériques (PSAN)

Document de nature explicative

Sommaire

Introduction

1. Les présents principes d'applications sectoriels (PAS) élaborés par l'ACPR, en lien avec Tracfin et la DG Trésor, répondent à une demande des organismes financiers[1] soumis à son contrôle en vue de la mise en œuvre des obligations de vigilance en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) et de gel des avoirs.

2. Il s'agit d'un document explicatif qui n'a pas de caractère contraignant en lui-même. Il vise à faciliter l'élaboration et la mise en place par les prestataires de services sur actifs numériques (PSAN) de leur système préventif LCB-FT et de leur dispositif de gel des avoirs.

3. Les présents principes d'applications sectoriels précisent la mise en œuvre de la réglementation en matière de LCB-FT et de gel des avoirs dans le contexte spécifique lié aux actifs numériques. Ils complètent les lignes directrices de l'ACPR, qui leur sont applicables[2].

4. Les présents principes d'applications sectoriels se fondent notamment sur les dispositions législatives et réglementaires issues notamment de la transposition de la directive (UE) 2015/849 du 20 mai 2015 révisée (dite « 5e directive LCB-FT ») et de l'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 (ci-après « arrêté du 6 janvier 2021 »). Ils tiennent également compte des décisions de la Commission des sanctions de l'ACPR.

5. Les PAS sont publics. Ils ont fait l'objet d'une concertation préalable à leur adoption au sein de la Commission consultative Lutte contre le blanchiment et le financement du terrorisme (CCLCBFT) instituée par l'ACPR en application de l'article L. 612-14 du code monétaire et financier (CMF).

6. Les dispositions législatives et réglementaires mentionnées dans les PAS sont celles du code monétaire et financier, sauf précisions contraires.

[1] Les organismes financiers sont les personnes mentionnées aux 1° à 7° bis de l'article L. 561-2 du Code monétaire et financier, à l'exclusion des personnes mentionnées au 5° et des organismes soumis au contrôle de l'AMF mentionnés au 6° dudit article.

[2] En particulier, les lignes directrices relatives au pilotage consolidé du dispositif de LCB-FT des groupes, les lignes directrices conjointes de la Direction Générale du Trésor et de l'Autorité de contrôle prudentiel et de résolution sur la mise en œuvre des mesures de gel des avoirs, les lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, les lignes directrices conjointes de l'ACPR et de TRACFIN sur les obligations de déclaration et d'information à TRACFIN, les lignes directrices relatives aux personnes politiquement exposées (PPE), les lignes directrices relatives à la notion de gestion de fortune.

1. Identification et classification des risques de blanchiment de capitaux et de financement du terrorisme

7. Les PSAN identifient et évaluent les risques de blanchiment de capitaux et de financement du terrorisme (BC-FT) auxquels ils sont exposés et mettent en place des politiques internes, une organisation et des procédures adaptées à ces risques. À cette fin, ils élaborent 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).

8. L'efficacité du dispositif de LCB-FT dépend notamment de l'élaboration d'une bonne classification des risques, qui est prise en compte pour la mise en place de l'organisation du dispositif de LCB-FT et des procédures internes, y compris en qui concerne les mesures de vigilance à appliquer (I de l'article L. 561-32 du CMF).

1.1 Sources prises en compte pour identifier et évaluer les risques

9. Les PSAN documentent l'identification, l'évaluation et la classification des risques (article 2 de l'arrêté du 6 janvier 2021). En particulier, ils prennent en compte les informations suivantes :

- les recommandations de la Commission européenne mentionnées dans son analyse supranationale des risques[3], fondée notamment sur l'avis de l'Autorité bancaire européenne sur les risques de BC-FT affectant le système financier[4] ;
- les facteurs de risque mentionnés aux annexes II et III de la 5e directive LCB-FT[5] ;
- l'analyse nationale des risques élaborée dans le cadre du Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB)[6], ainsi que l'analyse sectorielle de l'ACPR[7], qui en est la déclinaison dans le secteur financier ;
- les informations diffusées par le ministre chargé de l'économie[8] ;
- les informations diffusées par Tracfin[9], en particulier ses rapports d'activité et d'analyse ;
- les informations diffusées par le Groupe d'action financière (GAFI), telles que le rapport du GAFI sur les typologies de blanchiment de capitaux et de financement du terrorisme impliquant des actifs virtuels[10] ;
- les publications de l'Organisation de coopération et de développement économique (OCDE) et de l'Union européenne.

Ces informations comprennent notamment :

- Les listes des juridictions à haut risque ou sous surveillance établies par le GAFI ;
- Les listes des pays tiers à haut risque établies par la Commission européenne en application de l'article 9 de la directive (UE) 2015/849 du 20 mai 2015 susvisée ;

[3] La Commission européenne a publié sa première analyse supranationale des risques en 2017 (annexes 1 et 2), sa deuxième en 2019 (avec son annexe) et sa troisième en 2022 (avec son annexe).
[4] Les autorités européennes de surveillance ont publié un premier avis conjoint sur les risques de BC-FT affectant le secteur financier de l'Union européenne en 2019. L'ABE a publié un avis sur les risques de BC-FT en 2021.
[5] 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.
[6] Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France.
[7] Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme en France.
[8] Telles que des informations publiées sur le site internet du ministère chargé de l'économie ou des communiqués de presse.
[9] V. par exemple la lettre d'information n°20 de Tracfin sur les PSAN de mars 2022.
[10] V. le document *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*.

- Les listes publiées par l'OCDE et par l'Union européenne relatives aux juridictions non coopératives en matière fiscale ou adoptées en application de l'article 238-0 A du code général des impôts.

10. Lorsque, pour des motifs liés à la spécificité de leur activité ou de leur clientèle, les PSAN s'écartent des recommandations prévues dans ces documents et informations, ils sont en mesure de justifier leur analyse auprès de l'ACPR.

11. Ils peuvent également prendre en compte les éléments pertinents provenant d'autres sources, telles que les orientations de l'Autorité bancaire européenne sur les facteurs de risque de blanchiment de capitaux et de financement du terrorisme[11] ou les rapports d'Europol[12], ainsi que les éléments typologiques mentionnés dans les rapports des sociétés spécialisées dans l'analyse de *blockchains*.

1.2 Classification des risques

12. Les PSAN élaborent une classification des risques de BC-FT auxquels leur activité les expose 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.

13. Cette classification couvre l'ensemble des risques auxquels le prestataire est exposé par son activité[13]. Elle couvre ainsi toutes les catégories de produits et services proposés par le prestataire (en prenant en compte l'exposition au risque résultant de chaque produit ou service commercialisé[14]), des opérations proposées[15] et des clientèles[16].

14. La plupart des risques de BC-FT qui affectent les organismes du secteur financier concernent également les PSAN. En particulier, dans le cadre de leurs activités liées aux actifs numériques, les PSAN peuvent fournir des services de change ou réaliser des activités qui s'assimilent notamment à de la gestion de fortune ou de la transmission de fonds. Ces activités présentent des risques plus élevés en matière de blanchiment, notamment de fraude sociale et fiscale ou de transactions portant sur des produits/services illicites, ou de financement du terrorisme.

Les PSAN qui offrent la possibilité d'utiliser des actifs numériques pour acheter des biens ou services sont exposés à des risques similaires à ceux des prestataires de services de paiement. Ainsi, par exemple, la fourniture du service d'achat/vente d'actifs numériques auprès de places de marché expose aux risques liés à la revente de biens volés ou contrefaits, à l'achat suivi de la revente de biens de valeur à des fins de blanchiment ou à ce que le vendeur ait une activité fictive (ou ne correspondant pas à celle affichée) pour dissimuler des activités telles que la distribution de stupéfiants ou la collecte et le transfert de fonds à des fins terroristes.

Les PSAN qui offrent la possibilité de négocier des actifs numériques peu liquides, sont plus exposés au risque de manipulation de cours pouvant par exemple servir à dissimuler des transferts de valeurs.

---

[11] ABE, *"The ML/TF Risk Factors Guidelines"*, 1er mars 2021, EBA/GL/2021/02.
[12] V. par exemple les *Internet Organised Crime Threat Assessment (IOCTA)* ou le rapport *Cryptocurrencies: tracing the evolution of criminal finances* de janvier 2022.
[13] CDS, 26 janvier 2015, n°2013-06.
[14] CDS, 26 juillet 2018, n°2017-01 ; 26 juillet 2018, n°2017-02.
[15] CDS, 26 juillet 2018, n°2017-03.
[16] CDS, 24 juillet 2015, n°2014-07 ; 16 octobre 2015, n°2014-10 ; 8 décembre 2016, n°2015-08 ; 30 juin 2017, n°2016-09 ; 8 novembre 2017, n°2016-10 ; 24 février 2021, n°2020-02.

Plus généralement, les PSAN qui acquièrent, vendent ou facilitent la négociation d'actifs numériques sont exposés au risque accru d'anonymat associé aux portefeuilles d'actifs numériques, en particulier ceux intégrant des fonctionnalités de *mixing* et de *tumbling* qui réduisent la traçabilité des transactions (*privacy wallets*), sauf à ce que les actifs numériques soient conservés par les PSAN eux-mêmes ou par des PSAN régulés de manière équivalente avec lesquels ils sont en mesure d'échanger des informations sur l'identité des donneurs d'ordre et des bénéficiaires[17].

L'ensemble de ces risques doit être pris en compte dans la classification du prestataire.

15. Par ailleurs, les PSAN sont également exposés à des risques spécifiques ou accrus liés à la nature de leur activité. Ils prêtent une attention particulière :

- Aux fonds susceptibles de provenir d'un piratage de plateformes d'achat d'actifs numériques (« *hack* »)[18], d'un vol de portefeuilles d'actifs numériques, d'un rançongiciel ou d'escroqueries (telles que des « *exit scams* ») ;
- Aux opérations réalisées sur le « *darkweb* » (achat d'armes, trafic de stupéfiants, pédopornographie, achat de faux titres d'identité, etc.)[19] ;
- Aux opérations de collecte ou de transfert de fonds à des fins de financement de terrorisme.

16. Le tableau ci-dessous présente plusieurs facteurs de risques propres à l'activité liée aux actifs numériques :

Nature des produits ou services offerts	Conditions de transaction proposées	Canaux de distribution utilisées	Caractéristiques des clients	Pays ou territoire d'origine ou de destination des fonds
○ Actifs numériques à anonymat renforcé (AEC, « *privacy coins* »)[20] , que l'anonymat soit optionnel ou non	○ Utilisation d'espèces ou d'autres modes de paiement risqués ○ Actifs numériques provenant de *mixers* ou de *tumblers*, de manière à masquer l'origine des actifs[21]. Les	○ Utilisation de distributeurs automatiques (ATM)	○ Utilisation d'un VPN, d'adresses IP différentes ou liées à Tor[23], de proxys ○ Utilisation de *privacy wallets*[24] ○ Adresse IP du client renvoyant à un pays différent de son pays de résidence ○ Utilisation de multiples adresses	○ Flux d'actifs numériques[26] ou de monnaie ayant cours légal en provenance ou à destination de pays à risque figurant sur liste de pays à risque de la France, de la Commission européenne, du GAFI ou de l'OCDE ○ Différences entre le pays de résidence du client et le pays de domiciliation

[17] Notamment dans le cadre de l'article L. 561-21 du CMF.
[18] Sur ce point, v. les *Red Flag Indicators* du GAFI p. 16.
[19] V. rapport d'activité et d'analyse de Tracfin 2021, p. 37 et en particulier le cas typologique n°4 p. 40.
[20] Les AEC désignent une catégorie d'actifs numériques conçus afin de favoriser l'anonymat de ses détenteurs en permettant aux contreparties d'une transaction d'assurer leur anonymat tout en permettant une configuration du niveau de confidentialité de la transaction. Les *privacy coins* assurent une totale intraçabilité des flux d'actifs numériques.
[21] Les mixeurs (« *mixers* ») et mélangeurs (« *tumblers* ») sont des services permettant de renforcer l'anonymat d'actifs numériques en mélangeant plusieurs flux d'un même type d'actif numérique traçable issus de plusieurs adresses publiques en vue de les renvoyer vers d'autres adresses publiques, entraînant une rupture de la chaîne de traçabilité de ces actifs numériques dans l'historique de détention des différents portefeuilles.
[23] Les navigateurs Tor exploitent le réseau informatique décentralisé Tor favorisant une navigation anonymisée des ressources sur le web.
[24] Les *privacy wallets* sont des logiciels permettant à une personne de conserver elle-même ses actifs numériques, tout en intégrant des fonctionnalités permettant de combiner les transactions de plusieurs personnes en un même transfert ce qui réduit la visibilité sur ces flux d'actifs numériques.
[26] Il s'agit d'un facteur de risque qui doit être pris en compte dans la classification des risques. Il doit donner lieu à des mesures de vigilances lorsque le PSAN identifie une origine ou une destination à risque.

	comptes « omnibus » d'un PSAN[22] ne faisant pas l'objet d'une régulation et d'une supervision équivalentes peuvent aussi compliquer la traçabilité. ○ Actifs en provenance ou à destination d'un PSAN non soumis à une réglementation et/ou une supervision équivalente. ○ Utilisation d'une adresse publique connue pour être liée à des rançongiciels ou d'autres activités illicites (*marketplace* sur le *darknet*, etc.)		publiques par une seule personne (typologies de « *chain peeling* » *ou de* « *smurfing* »[25]) ○ Client effectuant des transactions en actifs numériques en utilisant des adresses publiques liées à des rançongiciels ou à d'autres activités illicites (piratage de plateformes, vol d'actifs numériques)	bancaire des comptes servant aux transactions en actifs numériques

Ce tableau n'est pas exhaustif. Il appartient aux PSAN d'adapter leur classification en fonction des risques spécifiques de BC-FT auxquels leur activité les expose.

1.3 Mise à jour de la classification des risques

17. Les PSAN mettent régulièrement à jour leur classification des risques, notamment à la suite de tout évènement externe (apparition de nouvelles menaces de BC-FT ou de vulnérabilités, évolution des listes de pays à risque, modification de la réglementation, etc.) ou interne (commercialisation de nouveaux produits ou services, nouvelles cibles de clientèle, mise en place de nouveaux canaux de distribution, etc.) affectant significativement les activités, les produits, les opérations, les canaux de distribution, les clientèles ou ses implantations.

18. En particulier, les PSAN identifient et évaluent les risques de BC-FT préalablement au lancement notamment de nouveaux produits, services ou pratiques commerciales afin de prendre des mesures appropriées propres à gérer et à atténuer ces risques (article 2 de l'arrêté du 6 janvier 2021). Ils en tiennent compte pour la mise à jour de la classification des risques.

2. Élaboration d'un profil de risque de chaque relation d'affaires

19. Les PSAN élaborent un profil de risque pour chaque relation d'affaires en fonction notamment (i) de la classification des risques et (ii) des éléments de connaissance actualisée de la relation d'affaires, notamment de l'activité et de la situation financière du client, ainsi que de la nature des opérations envisagées ou effectuées. Ils tiennent également compte de toute déclaration de

[22] Par opposition à des adresses individuelles par client.
[25] Le propriétaire d'une adresse publique détenant un montant important d'actifs numériques en envoie un petit montant à un PSAN et le reste à une autre adresse publique. Il répète ce procédé plusieurs fois de manière à faire croire que plusieurs personnes différentes déposent des actifs numériques auprès du PSAN.

soupçon transmise à TRACFIN, d'éventuels appels à vigilance reçus ou de mesure de gel des avoirs. Ce profil de risque est mis à jour à une fréquence définie selon une approche par les risques et, en tout état de cause, à chaque actualisation des éléments de connaissance de la relation d'affaires.

20. Le profil de risque détermine l'intensité des mesures de vigilance mises en œuvre à l'égard de la relation d'affaires, tant en ce qui concerne la nature, l'étendue ou la fréquence de mise à jour des informations recueillies, qu'en ce qui concerne la surveillance des opérations, conduisant, le cas échéant, au déclenchement d'alertes. Il doit être suffisamment discriminant pour permettre notamment d'identifier les relations d'affaires présentant des risques plus élevés et nécessitant une vigilance accrue[27].

21. Il appartient aux PSAN de prévoir, dans leurs procédures internes, les modalités de définition du profil de risque de chaque relation d'affaires et les mesures de vigilances requises en fonction de ce profil[28].

3. Mesures d'identification et de vérification d'identité

22. Les PSAN sont invités à consulter les lignes directrices de l'ACPR relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle.

23. Pour vérifier l'identité de leur client, ils mettent en œuvre une mesure prévue à l'article R. 561-5-1 ou deux mesures prévues à l'article R. 561-5-2[29]. Lorsqu'ils fournissent exclusivement le service d'échange d'actifs numériques contre d'autres actifs numériques, la mise en œuvre de la mesure prévue au 3° de l'article R. 561-5-2 (cf. § 24) peut par exemple consister en un versement d'une commission en monnaie ayant cours légal.

Exemple de bonne pratique pour la vérification d'identité mise en place par les PSAN

24. Le 3° de l'article R. 561-5-2 du CMF prévoit que, pour vérifier l'identité du client, un PSAN peut notamment exiger que le premier paiement des opérations soit effectué en provenance d'un compte ouvert au nom du client auprès d'un organisme financier établi dans l'Union européenne. Comme l'indiquent les lignes directrices de l'ACPR relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, « *Dans le cadre d'un paiement par carte, l'organisme financier s'assure* (…) *que le porteur de la carte est bien le titulaire du compte de paiement utilisé* »[30]. Certains PSAN recueillent, avant le paiement, une photographie d'un relevé de compte et de la carte de paiement associée au compte utilisée (avec les mentions du numéro du compte et de la carte, du nom de leur titulaire et des lignes d'opération établissant que la carte est associée au compte).

4. Connaissance de la clientèle

25. Les PSAN sont invités à consulter les lignes directrices de l'ACPR relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle.

26. Conformément aux articles L. 561-5-1 et R. 561-12 du CMF, les PSAN recueillent et analysent, avant d'entrer en relation d'affaires, les éléments d'informations nécessaires à la connaissance de

[27] CDS, 24 février 2021, n° 2020-02.
[28] Article 6 de l'arrêté du 6 janvier 2021.
[29] En particulier, pour vérifier l'identité d'un client étranger situé en-dehors de l'Union européenne ou de l'Espace économique européen, les PSAN peuvent en pratique recourir à l'ensemble des mesures permises pour les opérations à distance prévues par les articles R. 561-5-1 et R. 561-5-2 (à l'exception du moyen d'identification électronique mentionné au 1° de l'article R. 561-5-1).
[30] Lignes directrices de l'ACPR relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, cf. § 46.

l'objet et de la nature de celle-ci, en vue d'établir un profil de risque et d'exercer une vigilance constante sur les opérations et leurs relations d'affaires.

27. Il leur appartient ainsi de collecter, selon une approche par les risques, des informations, voire des documents, pertinents :

- sur chacune des parties à la relation d'affaires ;

- et sur le fonctionnement envisagé de cette relation d'affaires (montant et nature des opérations envisagées, provenance et destination des fonds, justification économique déclarée par le client, fonctionnement envisagé de la relation d'affaires). Dans le cas de clients ayant, grâce à l'appréciation de la valeur ou à la négociation d'actifs numériques, accumulé une épargne importante en actifs numériques sans rapport avec le niveau de leur revenu, leur âge ou leur profession, les PSAN, dès lors qu'ils n'ont pas eux-mêmes assuré la conservation des actifs numériques concernés, recueillent, selon une approche par les risques, des informations et des justificatifs sur l'origine et les modalités de constitution de cette épargne. L'analyse de la *blockchain* peut-être une source utile, mais celle-ci doit être complétée par des informations permettant de relier les actifs épargnés au client.

28. Les PSAN recourent, selon une approche par les risques, aux outils d'analyse transactionnelle pour enrichir leur connaissance de la clientèle à l'entrée en relation d'affaires. À cet effet, ils tiennent compte du fait que ces outils peuvent reposer sur des méthodes probabilistes, notamment concernant l'attribution des adresses publiques à un détenteur. Cependant, la connaissance de la clientèle ne saurait uniquement se fonder sur les outils d'analyse transactionnelle.

29. Pendant toute la durée de la relation d'affaires, ils recueillent, mettent à jour et analysent les éléments d'informations qui permettent de conserver une connaissance appropriée, selon une approche par les risques, et actualisée de leurs relations d'affaires.

5. Vigilance constante

30. Les PSAN sont invités à consulter les lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'information à Tracfin.

5.1 Dispositif de surveillance des opérations et des relations d'affaires

31. Pour assurer leur obligation de vigilance constante (article L. 561-6 du CMF), les PSAN mettent en place un dispositif de suivi et d'analyse des opérations et des relations d'affaires prévu au troisième alinéa du I de l'article L. 561-32 du CMF et à l'article 4 de l'arrêté du 6 janvier 2021. Si la réglementation n'impose pas aux PSAN de se doter d'outils automatisés, un tel dispositif est nécessaire lorsque la taille de l'organisme ainsi que la nature et le volume de ses activités ne permettent pas une surveillance manuelle adaptée des opérations.

32. Ce dispositif permet notamment de détecter les opérations atypiques ou suspectes au regard, le cas échéant, du profil de risque de la relation d'affaires, sur la base de critères, seuils de significativité, scénarios. Ces derniers sont définis selon une approche par les risques et permettent de couvrir l'ensemble des risques identifiés dans la classification du prestataire.

33. Ce dispositif porte à la fois sur les flux en actifs numériques et sur les flux en monnaie ayant cours légal.

- Sur les flux en actifs numériques

34. Les PSAN sont en mesure d'analyser, outre des adresses publiques d'envoi et de réception des actifs numériques, l'origine des flux en actifs numériques et leur destination, avec une profondeur d'analyse adaptée aux risques.

35. À cette fin, ils disposent de moyens matériels et humains leur permettant d'analyser les transactions sur la *blockchain*.

36. Ces moyens comprennent notamment les outils d'analyse transactionnelle de *blockchain* (OAT), qui permettent d'avoir une meilleure visibilité sur les flux d'actifs numériques, sur leur origine et sur leur destination, ainsi que sur les risques associés à certaines adresses publiques. L'utilisation de plusieurs OAT peut être nécessaire lorsqu'un PSAN propose des services liés à différents actifs numériques qui sont pris en charge par des outils distincts.

37. Certains actifs numériques, notamment s'ils sont de création récente, peuvent ne pas être compatibles avec les outils d'analyse transactionnelle disponibles sur le marché. Les PSAN qui fournissent des services liés à de tels actifs prennent des mesures nécessaires à réduire le risque de BC-FT lié à ces actifs. Par exemple, un PSAN fournissant les services d'échange et de conservation peut choisir de limiter les services offerts à la seule vente de ces actifs (à l'exclusion de leur achat), à condition que les actifs vendus soient conservés par le PSAN au nom et pour le compte du client et qu'ils ne puissent être transférés que vers une adresse publique dont le PSAN assure également la conservation. Un autre exemple pourrait être l'utilisation d'un explorateur en ligne de *blockchain* qui peut constituer un élément utile dans le cadre de la surveillance des opérations.

38. Il en va différemment pour les actifs numériques à anonymat renforcé, qui sont conçus pour échapper, totalement ou partiellement, à une analyse des transactions sur la *blockchain*. À cet égard, les PSAN qui acceptent de telles transactions mettent en œuvre des vigilances particulières lorsqu'ils sont amenés à réaliser des opérations impliquant ce type d'actifs (cf. § 44). En outre, les PSAN peuvent limiter l'utilisation des actifs numériques à anonymat renforcé.

39. Les OAT sont utilisés dans le cadre des dispositifs de surveillance des opérations et des relations d'affaires pour déclencher des alertes ou pour analyser des opérations dans le cadre du traitement d'une alerte. Toutefois, la surveillance des opérations et des relations d'affaires ne saurait reposer uniquement sur des outils d'analyse transactionnelle. Il appartient aux PSAN d'analyser l'ensemble des informations dont ils disposent aux fins de la vigilance constante, en particulier les informations recueillies au titre de la connaissance de la relation d'affaires ou dans le cadre d'un examen renforcé.

40. Les PSAN sont en mesure de justifier auprès de l'ACPR le paramétrage des outils utilisés, notamment le nombre de rebonds analysés selon une approche par les risques.

- Sur les flux en monnaie ayant cours légal

41. Les PSAN doivent également exercer une vigilance sur les flux en monnaie ayant cours légal. Les PSAN peuvent se référer, sur ce point, aux lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'information à Tracfin.

5.2 Examen renforcé

42. Conformément à l'article L. 561-10-2 du CMF, les PSAN effectuent un examen renforcé de toute opération particulièrement complexe ou d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite. Dans ce cas, ils se renseignent auprès du

client sur l'origine des fonds et la destination de ces sommes ainsi que sur l'objet de l'opération et l'identité de la personne qui en bénéficie.

43. Pour justifier de l'origine des fonds, ils peuvent en particulier recueillir des informations/justificatifs sur les modalités d'obtention de l'actif numérique (preuve d'achat auprès d'une plateforme située en France ou à l'étranger ou d'un particulier, obtention par du minage, du *staking*[31] ou un *airdrop*[32], souscription dans le cadre d'une offre initiale au public de jetons, relevé de compte daté délivré par un PSAN, etc.), la date d'obtention ou d'autres informations pertinentes (*hash* de transaction en cas d'échange entre actifs numériques lorsque cette information est disponible).

44. Sauf dans des cas dûment justifiés[33], les PSAN réalisent un examen renforcé lorsqu'ils effectuent une opération liée à des *privacy coins* ou à des *anonymity-enhanced cryptocurrencies* (AEC). En effet, l'utilisation de ces actifs numériques, qui ont été spécifiquement conçus pour favoriser l'anonymat de leur détenteur, conduit à s'interroger sur l'objet de l'opération.

45. Les PSAN prêtent une attention particulière aux opérations réalisées dans le cadre d'un rançongiciel (ou *ransomware*)[34], que l'opération soit réalisée par l'auteur du rançongiciel, par la victime[35] ou pour le compte de cette dernière[36]. Dans chacun de ces cas, les PSAN réalisent un examen renforcé et, lorsque l'examen ne permet pas de lever le doute, ils s'abstiennent d'effectuer l'opération et transmettent une déclaration de soupçon à TRACFIN conformément au III de l'article L. 561-15 du CMF. Les PSAN peuvent procéder à la réalisation de l'opération si Tracfin n'a pas notifié d'opposition[37], conformément aux articles L. 561-16 et L. 561-24 du CMF[38].

6. Déclaration de soupçon

46. Concernant les modalités de déclaration de soupçon, les PSAN sont invités à consulter les lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'information à Tracfin.

47. Lorsqu'un PSAN déclare une opération à Tracfin sur le fondement de l'article L. 561-15 du CMF, il lui appartient de mentionner notamment :

---

[31] L'activité de *staking* consiste à donner à des détenteurs d'actifs numériques la possibilité d'immobiliser, contre une contrepartie, une certaine quantité d'actifs numériques au sein d'un portefeuille ou d'un autre support, dans le but d'assister un dispositif d'enregistrement électronique partagé (*blockchain*) ayant un mécanisme de validation fondé sur la preuve d'enjeu (*proof of stake*) ou tout autre mécanisme de validation équivalent.

[32] Méthode de distribution d'actifs numériques dans le cadre d'une opération de promotion d'un actif numérique récemment créé.

[33] Ce peut être le cas lorsque le client réalise des opérations de « *staking* » au moyen d'actifs numériques à anonymat renforcé, dès lors que ces actifs sont exclusivement conservés par le PSAN, à l'exclusion de toute possibilité de transfert entrant ou sortant en provenance ou à destination d'une adresse publique dont le PSAN n'assure pas la conservation au sens du 1° de l'article L. 54-10-2 du CMF.

[34] Technique d'attaque de la cybercriminalité consistant en l'envoi à la victime d'un logiciel malveillant qui chiffre des données et lui demande une rançon, souvent exigée en actifs numériques, en échange du mot de passe de déchiffrement.

[35] Plusieurs facteurs permettent de détecter ce type de situation (clients différents de sa clientèle habituelle, agissant en-dehors de leur objet social - comme des petites et moyennes entreprises, des entreprises stratégiques, des collectivités territoriales ou des centres hospitaliers - et demandant à acheter rapidement un montant important d'actifs numériques, transfert au bénéfice d'un intermédiaire spécialisé dans l'accompagnement d'entreprises victimes de cyberattaques, etc.).

[36] Par exemple des sociétés spécialisées dans la cybersécurité ou des intermédiaires spécialisés dans l'accompagnement d'entreprises victimes de cyberattaques et agissant pour le compte de ces victimes.

[37] Avant le délai d'exécution indiqué conformément au 6° du III de l'article R. 561-31 du CMF.

[38] Sous réserve de leurs obligations en matière de gel des avoirs et de mesures restrictives (cf. §59 et s. du présent document).

- Les éléments d'identification du client et, le cas échéant, du bénéficiaire effectif, de connaissance de la relation d'affaires, d'identification des personnes impliquées, y compris des éléments tels que l'adresse IP, les éléments d'identification des appareils ayant servi à la connexion[39], l'adresse courriel, le numéro de téléphone, etc. ;
- Les éléments relatifs à la nature des actifs numériques concernés : la *blockchain* pertinente, le *hash* de la transaction lorsqu'il est disponible, l'adresse publique de son client et toute autre adresse publique pertinente, ainsi que tout élément technique de localisation ou d'attribution ;
- Une description des faits et l'analyse structurée du PSAN ayant conduit à la déclaration.

Par ailleurs, il convient de joindre à ces éléments toute pièce utile relative à l'opération : les relevés transactionnels y compris les opérations internes (*off-chain*), les extraits d'analyse obtenue par l'OAT, etc. En ce qui concerne les documents les plus techniques (comme des tableaux *Excel*), il convient, le cas échéant, de les accompagner des informations nécessaires à leur exploitation et à leur compréhension par Tracfin.

7. Contrôle interne

48. Conformément à l'article R. 561-38-3 du CMF, les PSAN mettent en place un dispositif de contrôle interne adapté à leur taille, à la nature, à la complexité et au volume de leurs activités. Ce dispositif est doté de moyens humains suffisants.

49. Ce dispositif, qui doit être défini dans les procédures internes de l'établissement, a notamment pour objet de vérifier que les opérations exécutées par les PSAN, ainsi que leur organisation et leurs dispositifs de LCB-FT et de gel des avoirs sont conformes aux procédures internes qu'ils ont définies et à la réglementation (article 13 de l'arrêté du 6 janvier 2021).

50. Il porte sur l'ensemble des activités du PSAN.

7.1 Organisation du dispositif de contrôle interne

51. Conformément aux dispositions de l'article R. 561-38-8 du CMF, le dispositif de contrôle interne du PSAN comprend au moins :

- Des procédures définissant les activités de contrôle interne que le PSAN accomplit pour s'assurer du respect de leurs obligations en matière de LCB-FT ;
- Un contrôle interne permanent réalisé, conformément aux procédures internes, par des personnes exerçant des activités opérationnelles (contrôle permanent de premier niveau) et, le cas échéant, en fonction de leur taille, de la complexité et du niveau de leurs activités, par des personnes dédiées à la seule fonction de contrôle des opérations (contrôle permanent de deuxième niveau) ;
- Un contrôle interne périodique réalisé par des personnes dédiées, de manière indépendante à l'égard des personnes, entités et services qu'elles contrôlent lorsque cela est approprié eu égard à la taille et à la nature des activités.

52. Les PSAN mettent en place un contrôle permanent de premier niveau.

53. Compte tenu du niveau de risque des activités liées aux actifs numériques, les PSAN mettent en place un dispositif de contrôle permanent de deuxième niveau et un dispositif de contrôle périodique adapté, notamment, à leur taille (cf. § 48). Toutefois, ils peuvent adopter une organisation différente dans des situations spécifiques, dûment justifiées auprès de l'ACPR. Ainsi, des prestataires de plus petite taille dont le nombre d'employés n'est pas suffisant pour assurer

[39] Comme des adresses MAC.

un contrôle permanent de deuxième niveau peuvent, s'ils exercent des activités limitées présentant des risques plus faibles, mettre en place seulement un contrôle périodique. Dans ce cas, la fréquence du cycle d'audit est renforcée. Elle est au moins annuelle, sauf dans des situations dûment justifiées auprès de l'ACPR.

54. Les incidents ou insuffisances identifiés par le dispositif de contrôle interne sont communiqués au responsable du dispositif LCB-FT/gel mentionné à l'article 2 de l'arrêté du 6 janvier 2021 Lorsqu'ils portent sur le dispositif de LCB-FT, ils font l'objet de mesures correctrices dans des délais raisonnables, qui tiennent compte des risques de BC-FT (article R. 561-38-8 du CMF). Lorsqu'ils portent sur le gel des avoirs, ces incidents ou insuffisances font l'objet de mesures correctrices immédiatement (article 13 de l'arrêté du 6 janvier 2021).

55. Les PSAN disposent de procédures permettant de vérifier la mise en œuvre et le suivi des mesures correctrices dans les délais impartis (article 3 de l'arrêté du 6 janvier 2021), qui font l'objet d'un contrôle interne (article 13 de l'arrêté du 6 janvier 2021).

7.2. Implication des dirigeants

56. Selon l'article 25 de l'arrêté du 6 janvier 2021, la responsabilité de s'assurer que l'organisme assujetti se conforme à ses obligations en matière de LCB-FT incombe aux dirigeants et à l'organe de surveillance, qui doivent disposer de l'ensemble des informations nécessaires à cet effet.

57. Selon l'article 26 du même arrêté, les dirigeants des PSAN évaluent et contrôlent périodiquement l'efficacité des dispositifs et des procédures mis en place pour se conformer à la réglementation LCB-FT/gel. L'organe de surveillance examine régulièrement la politique de lutte contre le blanchiment de capitaux et le financement du terrorisme mentionnée à l'article L. 561-4-1 du CMF, les dispositifs et les procédures mis en place pour se conformer à la réglementation en matière de LCB-FT et de gel des avoirs, ainsi que les mesures correctrices mentionnées ci-dessus. Ils s'assurent de leur efficacité.

58. À cette fin, les dirigeants doivent disposer de l'ensemble des informations nécessaires. L'organe de surveillance détermine la nature, le volume, la forme et la fréquence des informations qui lui sont transmises. Cette transmission d'informations peut notamment prendre la forme d'un rapport annuel de contrôle interne.

8. Mise en œuvre des mesures de gel des avoirs et des autres mesures restrictives

59. Les PSAN sont invités à consulter les lignes directrices conjointes de l'ACPR et de la DG Trésor sur la mise en œuvre des mesures de gel des avoirs.

60. Les actifs numériques sont des fonds ou ressources économiques susceptibles d'être gelés.

61. 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 ou d'utilisation. Ils doivent également déclarer immédiatement au ministre chargé de l'économie (en pratique, la DG Trésor) toutes les actions de mise en œuvre d'une mesure de gel des avoirs[40] via les points de contact dédiés :

[40] À savoir : le gel d'un compte, d'une opération ou d'un contrat, toute opération portée au crédit d'un compte dont les fonds sont gelés, la suspension de toute opération de mise à disposition de fonds ou ressources économiques au profit d'une personne ou entité désignée, le refus d'entrée en relation d'affaires, d'exécuter une opération occasionnelle au profit d'une personne ou entité désignée et les tentatives de contournement.

- Pour les mesures de gel des avoirs liées au terrorisme, qu'elles soient européennes ou nationales : liste-nationale@dgtresor.gouv.fr
- Dans tous les autres cas (autres sanctions financières) : sanctions-gel-avoirs@dgtresor.gouv.fr

62. La mise en œuvre des mesures de gel des avoirs constitue une obligation de résultat à la charge des PSAN[41].

63. Les PSAN mettent en place une organisation et des procédures internes, comprenant un dispositif de détection, ainsi que des mesures de contrôle interne, conformément aux articles L. 562-4-1 et R. 562-1 du CMF et aux articles 11 et suivants de l'arrêté du 6 janvier 2021. Les PSAN sont invités à se référer aux paragraphes 58 et suivants des lignes directrices précitées de l'ACPR et de la DG Trésor.

64. Pour la mise en œuvre concrète des obligations de gel des avoirs :

- dans le cadre de la fourniture du service de conservation, les PSAN se réfèrent aux dispositions des lignes directrices applicables au traitement des comptes (*cf.* notamment § 131 à 133), quelles que soient les modalités techniques de la conservation des actifs numériques.

- dans le cadre de la fourniture des services d'achat/vente d'actifs numériques en monnaie ayant cours légal ou d'échange d'actifs numériques contre d'autres actifs numériques, les PSAN s'abstiennent d'effectuer l'opération avec une personne ou une entité faisant l'objet d'une mesure de gel. En principe, ils retiennent les fonds reçus (en monnaie ayant cours légal et en actifs numériques) en contrepartie de l'opération d'achat-vente d'actifs numériques en monnaie ayant cours légal ou d'échange entre actifs numériques, sauf en cas de risque pour la sécurité physique de leur personnel[42], et en informent, en tout état de cause, la DG Trésor. Si les fonds sont retenus, les PSAN les conservent avec les détails de l'identification du client. Ils sont conservés dans un endroit sécurisé (par exemple, un coffre-fort, une adresse publique spécifiquement dédiée à cet effet), jusqu'à la levée de la mesure de gel.

65. Les PSAN sont en mesure de justifier de la mise en œuvre sans délai de leurs obligations de gel des avoirs, d'interdiction de mise à disposition ou d'utilisation et d'information de la DG Trésor. À cette fin, ils conservent toute information utile quel qu'en soit le support (captures d'écran, justificatif horodaté du blocage de l'accès au compte de la personne faisant l'objet d'une mesure de gel, etc.).

66. Pour rappel, des autorisations de dégel peuvent être accordées par la DG Trésor pour répondre aux besoins fondamentaux des personnes ou entités désignées.

67. En cas de transfert d'actifs numériques vers une adresse publique dont les PSAN n'assurent pas la conservation au sens du 1° de l'article L. 54-10-2 du CMF, ces derniers recueillent 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 les PSAN n'assurent pas la conservation afin de permettre, le cas échéant, la mise en œuvre de la mesure d'interdiction de mise à disposition ou d'utilisation des avoirs. Il peut s'agir de demander directement au client d'indiquer l'identité du propriétaire de l'adresse publique de destination ou d'analyser l'historique de transaction de cette adresse via un OAT.

[41] V. CDS, 27 novembre 2012, n°2011-03 ; 21 décembre 2018, n°2018-01 ; 24 septembre 2019, n°2018-08 ; 4 février 2020, n°2019-04 ; 7 mai 2021, n°2020-05 ; 30 novembre 2021, n°2020-09.
[42] C'est le cas pour les PSAN qui exploitent des bureaux de change « physiques ».

68. Les PSAN sont également tenus d'appliquer les autres mesures restrictives adoptées par l'Union européenne conformément aux articles 75 et 215 du traité sur le fonctionnement de l'Union européenne (TFUE). À cet égard, l'attention est notamment appelée sur les mesures restrictives portant sur la fourniture de services sur actifs numériques prévues à l'article 5 *ter* du règlement (UE) n° 833/2014 du Conseil du 31 juillet 2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine.

69. Conformément à l'article L. 562-6 du CMF et aux règlements européens portant mesures restrictives, il est interdit aux PSAN de participer, sciemment et volontairement, à des activités ayant pour objet ou pour effet de contourner les mesures restrictives. L'article L. 562-4-1 du CMF impose aux PSAN de se doter d'une organisation et de procédures internes pour mettre en œuvre cette interdiction.

70. Conformément à l'article R. 562-3 du CMF, les PSAN informent immédiatement la DG Trésor des opérations dont ils estiment qu'elles ont pour but ou pour effet de contourner les mesures de gel ou d'interdiction de mise à disposition ou d'utilisation des avoirs. Ils réalisent par ailleurs une déclaration de soupçon à Tracfin[43].

Tentatives de violation ou de contournement des mesures restrictives adoptées dans le cadre des régimes de sanctions en vigueur, y compris du régime de sanctions en lien avec la situation en Ukraine

71. Les PSAN prêtent une attention particulière aux éventuelles tentatives (i) d'infraction à l'interdiction de mise à disposition indirecte de fonds au bénéfice de personnes soumises à des mesures de gel des avoirs ou (ii) de contournement, au moyen d'actifs numériques, des mesures restrictives adoptées dans le cadre des régimes de sanctions en vigueur, notamment du régime de sanction en lien avec la situation en Ukraine. À cet égard, ils prennent notamment en compte les critères d'alerte suivants :

- Le client réside ou initie des transactions depuis ou vers un pays soumis à des mesures restrictives ou un pays figurant sur les listes du GAFI ou de la Commission européenne ou considéré comme risqué par le PSAN[44] ;

- Le client a des liens, notoires ou connus du PSAN, de nature familiale, personnelle, professionnelle ou de proximité avec une personne faisant l'objet de mesures restrictives ;

- Le client utilise des outils destinés à dissimuler sa localisation réelle (VPN, utilisation du navigateur Tor, proxys) ou l'origine de ses actifs numériques (*mixers, tumblers,* etc.) ;

- Le client refuse de fournir des informations sur son identité ou fournit des informations inexactes ;

- Le client effectue des transactions depuis ou vers une adresse publique identifiée par un outil d'analyse transactionnelle de *blockchain* comme risquée ou liée à des personnes faisant l'objet de mesures restrictives ;

- Les actifs numériques du client proviennent ou sont transférés vers une plateforme d'actifs numériques (i) qui n'a pas fait l'objet d'une autorisation, (ii) qui n'est pas soumise à une

[43] Le fait, pour les personnes faisant l'objet d'une mesure de gel ou d'interdiction, de se soustraire aux obligations en résultant ou de faire obstacle à sa mise en œuvre ou le fait de s'en rendre complice est puni des peines prévues au 1 de l'article 459 du code des douanes.

[44] Il convient notamment de prendre en compte l'adresse IP du client ainsi que l'utilisation, le cas échéant, d'un VPN, du navigateur Tor ou de proxys.

réglementation[45] ou une supervision équivalente, (iii) qui est située dans des pays soumis à des mesures restrictives ou dans un pays figurant sur les listes du GAFI ou de la Commission européenne ou considéré comme risqué par le PSAN ;

- Le bénéficiaire effectif du client (i) réside dans un pays soumis à des mesures restrictives ou un pays figurant sur les listes du GAFI ou de la Commission européenne ou considéré comme risqué par le PSAN ou (ii) est notoirement connu pour entretenir des liens personnels ou professionnels avec de tels pays ou (iii) entretient des liens, notoires ou connus du PSAN, de nature familiale, personnelle, professionnelle ou de proximité avec une personne faisant l'objet de mesures restrictives.

- Le client est une personne morale ayant récemment fait l'objet d'un changement de bénéficiaires effectifs.

[45] V. rapport d'activité et d'analyse de Tracfin 2021, p. 73. Certains outils d'analyse transactionnelle permettent de déterminer une telle provenance des actifs numériques.