Royal United Services Institute
for Defence and Security Studies

Document d'orientation 2022

Lutte contre le financement de la prolifération pour les prestataires de services d'actifs virtuels

Kayla Izenman

Lutte contre le financement de la prolifération pour les prestataires de services d'actifs virtuels

Kayla Izenman

Document d'orientation RUSI, Mars 2022

Royal United Services Institute
for Defence and Security Studies

191 années de pensée indépendante sur la défense et la sécurité

Le Royal United Services Institute (RUSI) est le plus ancien groupe de réflexion en matière de défense et sécurité au monde, ainsi que le chef de file dans le domaine au Royaume-Uni. Il a pour mission d'informer, d'influencer et d'améliorer le débat public sur un monde plus sûr et plus stable. RUSI est un institut de recherche qui produit des analyses indépendantes, pratiques et innovantes afin d'aborder les complexes défis du monde actuel.

Depuis sa fondation en 1831, RUSI s'est appuyé sur ses membres pour soutenir ses activités. À côté de cela, avec les revenus tirés de la recherche, des publications et des conférences, RUSI a maintenu son indépendance pendant 191 ans.

Clause de non-responsabilité

Les présentes constituent un document d'orientation à l'attention des prestataires de services d'actifs virtuels (PSAV) désireux d'instaurer ou de développer une fonction de lutte contre le financement de la prolifération (LFP) au sein de leur organisation. Ces orientations visent à fournir un cadre permettant aux PSAV de mettre en œuvre et d'adapter leurs propres pratiques de conformité en matière de criminalité financière, tout en respectant les exigences règlementaires nationales. Le document d'orientation ne constitue pas un avis juridique ou règlementaire et devra toujours être lu conjointement avec la législation nationale et les normes et lignes directrices internationales pertinentes. Un avis juridique indépendant devra systématiquement être demandé concernant les sanctions, la lutte contre la criminalité financière et la mise en œuvre de la LFP.

Lors de la rédaction de ces orientations, Kayla Izenman était chargée de recherche auprès du Centre for Financial Crime and Security Studies de l'institut RUSI. Le présent document fait état de son point de vue personnel à l'époque et ne reflète pas celui de son employeur actuel ni ne concerne la fonction qu'elle occupe aujourd'hui.

Les points de vue exprimés dans cette publication sont ceux de son auteur et ils ne reflètent pas les points de vue de RUSI ou de toute autre institution.

Cette version a été traduite de la version originale en anglaise, qui a été publiée en septembre 2021.

Publié en 2022 par Royal United Services Institute for Defence and Security Studie.

Document d'orientation RUSI, Mars 2022. ISSN 2397-0286 (en ligne).

Royal United Services Institute
for Defence and Security Studies
Whitehall
Londres SW1A 2ET
Royaume-Uni
+44 (0)20 7747 2600
www.rusi.org
RUSI est un organisme de bienfaisance
enregistré (n° 210639)

Tables des matières

Remerciements

La présente étude a été menée avec le généreux soutien de la fondation John D and Catherine T MacArthur Foundation. Nous remercions David Carlisle et Malcolm Wright de leurs commentaires utiles sur la première version du présent document. Nous remercions également tou(te)s ceux/celles qui ont généreusement donné de leur temps pour être interrogé(e)s dans le cadre de la recherche sur les actifs virtuels du RUSI depuis 2017, ainsi que l'équipe de publications du RUSI, pour son travail de révision des orientations.

Acronymes

AV – actif virtuel

BC – blanchiment de capitaux

FP – financement de la prolifération

FT – financement du terrorisme

GAFI – Groupe d'action financière

KYC – know your customer (connaissance du client)

LBC – lutte contre le blanchiment de capitaux

LFP – lutte contre le financement de la prolifération

LFT – lutte contre le financement du terrorisme

OVC – obligation de vigilance vis-à-vis de la clientèle

OVR – obligation de vigilance renforcée

PSAV – prestataire de services d'actifs virtuels

I. Objet et Objectifs

LE FINANCEMENT DE la prolifération (FP) des ADM est défini par le Groupe d'action financière (GAFI) comme étant « l'acte consistant à fournir des fonds ou des services financiers utilisés, en tout ou en partie, pour fabriquer, acquérir, posséder, développer, exporter, transborder, négocier, transporter, transférer, stocker ou utiliser des armes nucléaires, chimiques ou biologiques ».[1] Il s'agit là de la définition de travail du GAFI, mais il convient de noter qu'il n'existe pas de définition internationalement acceptée du FP, certains ayant plaidé pour une vision plus vaste, qui pourrait inclure, par exemple, les activités génératrices de revenus.[2]

Les proliférateurs d'ADM, comme la Corée du Nord et l'Iran, continuent de contourner les sanctions financières ciblées. Les actifs virtuels[3] (AV) sont devenus, d'une manière croissante, un instrument par le biais duquel les fonds liés à la prolifération sont levés et transférés. Néanmoins, le haut niveau de connaissance sur le blanchiment des AV et la levée de fonds de la part des proliférateurs d'ADM sanctionnés n'a pas encore fait l'objet de mesures de conformité, de règlementation et d'application de la loi. L'espace des AV s'est développé et amélioré en termes de pratiques de conformité au cours de ces dernières années, mais certains criminels ont toujours une longueur d'avance.

Les sanctions qui ciblent le programme d'armes nucléaires de la Corée du Nord ont été mises en place, au niveau des Nations unies, en 2006, et elles n'ont pas cessé de s'étendre, jusqu'à englober des sanctions financières ciblées à l'égard de personnes physiques et morales nommées, des sanctions fondées sur l'activité restreignant la capacité de la Corée du Nord à accéder au système financier international et des sanctions sectorielles ciblant des secteurs ou des exportations spécifiques de ce pays. De même, les Nations unies maintiennent des sanctions à l'égard de certaines personnes physiques et morales iraniennes et restreignent des activités afférentes au développement de missiles balistiques.[4]

Depuis au moins 2014, la Corée du Nord a fait preuve d'une expertise et d'un intérêt croissants en matière de délinquance informatique, lesquels se sont étendus, plus récemment, aux AV.[5] Au cours des

1. Groupe d'action financière (GAFI), « Combating Proliferation Financing: A Status Report on Policy Development and Consultation », Rapport FAFT-GAFI, février 2010, p. 5.
2. Pour en savoir plus sur la définition du financement de la prolifération (FP), veuillez consulter « Guide to Conducting a National Proliferation Financing Risk Assessment », Anagha Joshi, Emil Dall et Darya Dolzikova, RUSI, mai 2019, p. 5.
3. Dans ce document d'orientation, l'expression « actifs virtuels » désigne les jetons de paiement numériques, comme les Bitcoins. Pour une définition complète, veuillez consulter la section « Terminologie ».
4. Pour obtenir des informations à jour sur les exigences des Nations unies en matière de sanctions concernant la prolifération, veuillez consulter Nations unies, « Organes subsidiaires du Conseil de sécurité des Nations unies », 2021. Les sanctions unilatérales, comme celles infligées par les États-Unis d'Amérique, l'Union européenne ou le Royaume-Uni, pourraient imposer des exigences additionnelles par rapport aux sanctions des Nations unies.
5. L'un des premiers exemples d'activité de délinquance informatique de la Corée du Nord a été le tristement célèbre piratage de Sony Pictures, attribué à ce pays par le Federal Bureau of Investigation (FBI) des États-

années 2020 et 2021, le Département de la Justice des États-Unis d'Amérique a mis en examen plusieurs personnes physiques pour des faits de blanchiment d'AV pour le compte de la Corée du Nord.[6] Pourtant, bien que la plupart des activités en matière d'AV de la Corée du Nord impliquent des piratages à grande échelle, comme le piratage de 49 millions de dollars US de Upbit en 2019[7] ou les 275 millions de dollars US volés à KuCoin en 2020,[8] le régime a également montré de l'intérêt pour les attaques aux rançongiciels et le minage d'actifs virtuels.[9] Dans l'ensemble, la Corée du Nord est extrêmement avancée dans le domaine de la délinquance informatique et semble de plus en plus désireuse de mettre ces compétences au service des activités de cryptomonnaie. D'une manière similaire, bien qu'il ne s'agisse pas de l'objectif principal du présent document d'orientation, l'Iran a indiqué avoir commencé à utiliser le minage d'actifs virtuels pour contourner les sanctions et exporter du pétrole, une part importante de ce type d'activités ayant lieu dans ce pays.[10] Face au manque d'exigences et de règlementations globales dans de nombreux pays, les prestataires de services d'actifs virtuels (PSAV) peuvent constituer une cible facile pour ces acteurs.

Le présent document d'orientation vise à conseiller les PSAV concernant le respect des meilleures pratiques en ce qui a trait aux risques de FP, tout en orientant les personnes chargées de la conformité vers les publications pertinentes susceptibles de s'avérer utiles dans le cadre de leur travail (annexe II). Ce document sera particulièrement utile pour les PSAV n'ayant pas réfléchi avant au FP ou à la mise

---

Unis d'Amérique en décembre 2014. Voir FBI National Press Office, « Update on Sony Investigation », 19 décembre 2014, <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>, consulté le 24 août 2021.

6. Département de la Justice des États-Unis d'Amérique, « Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe », 17 février 2021 ; Département de la Justice des États-Unis d'Amérique « United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors », 27 août 2020 ; Département de la Justice des États-Unis d'Amérique, « Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack », 2 mars 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, consulté le 24 août 2021.
7. Pour en savoir plus sur le piratage d'Upbit, veuillez consulter Marie Huillet, « Upbit Hack: Stolen ETH Worth Millions on the Move to Unknown Wallets », Coin Telegraph, 3 décembre 2019, <https://cointelegraph.com/news/upbit-hack-stolen-eth-worth-millions-on-the-move-to-unknown-wallets>, consulté le 25 août 2021. La plainte déposée en 2020 par le Département de la Justice des États-Unis d'Amérique à l'encontre de Tian Yinyin qualifie le piratage d'Upbit « d'intrusion et vol 'de Marché 3' de novembre 2019 ». Département de la Justice des États-Unis d'Amérique, « Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack ».
8. Pour en savoir plus sur le piratage de KuCoin, veuillez consulter Chainalysis, « The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds », 2 octobre 2020, <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap>, consulté le 25 août 2021. Le Rapport final de 2021 du Groupe d'experts des Nations unies évoque une enquête en cours concernant un « piratage d'une plateforme d'échange de cryptomonnaies ayant eu lieu en septembre 2020 » qui a « permis de voler des cryptomonnaies d'une valeur de 281 millions de dollars US sur cette plateforme ». Comité des sanctions du Conseil de sécurité des Nations unies sur la Corée du Nord créé en vertu de la résolution 1718, « Rapport final présenté par le Groupe d'experts en application de la résolution 2515 (2020) », 4 mars 2021.
9. Yosuke Onchi, « North Korea Ramps up Ransomware Attacks in Hunt for Cash », Nikkei Asia, 18 février 2021.
10. Tom Robinson, « How Iran Uses Bitcoin Mining to Evade Sanctions and Export » Millions of Barrels of Oil', Elliptic, 21 mai 2021.

en œuvre des sanctions financières ciblées afférentes à la prolifération en tant que risque distinct de délinquance financière ou de sanctions.

Bien que les présentes orientations utilisent des études de cas de prolifération, concentrant l'attention, surtout, sur la Corée du Nord, une bonne partie de leur contenu est tiré des typologies, signaux d'alarme et meilleures pratiques que l'on peut trouver dans d'autres types de criminalité concernant les AV, notamment lorsque les activités illicites sont menées par de grandes organisations criminelles qui pourraient posséder une expertise et un financement comparables à ceux d'un pays faisant l'objet de sanctions.

Ces orientations suivent la structure générale du cycle de conformité, en commençant par les exigences préalables, avant l'interaction avec le client, puis en passant au processus d'intégration, suivi par un contrôle permanent pendant toute la durée de la relation avec le client. Une fois ce cycle complété, les orientations abordent les indicateurs de risque élevé et les signaux d'alarme susceptibles de susciter une obligation de vigilance renforcée ou le congédiement du client. Elles concluent avec les exigences en matière de signalement suite à toute activité repérée comme suspecte.

Les Recommandations du GAFI pour les AV et les PSAV

Il s'avère essentiel de comprendre et de mettre en œuvre les Recommandations à l'attention des PSAV pour se conformer aux meilleures pratiques, et les présentes orientations visent à compléter et soutenir lesdites recommandations.

Bien que le GAFI ait reconnu les risques associés aux AV depuis 2014,[11] la première adoption de modifications afférentes aux AV dans ses recommandations date d'octobre 2018, afin de clarifier que les Recommandations s'appliquent aux activités financières impliquant des AV. En juin 2019, le GAFI a adopté une Note interprétative de sa recommandation 15,[12] visant à clarifier davantage la façon dont les recommandations du GAFI s'appliquent aux AV et aux PSAV. Ceci incluait des orientations sur la supervision, le suivi, la licence et l'immatriculation, l'obligation de vigilance vis-à-vis de la clientèle, le signalement des transactions suspectes, les mesures de vérification des sanctions et autres.

Le GAFI a également adopté les Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels en juin 2019,[13] qui visent à aider les autorités nationales à développer les régimes règlementaires appropriés pour les AV et PSAV, ainsi qu'à conseiller les secteurs privés concernant la marche à suivre pour se conformer à ces exigences.

---

11. FATF-GAFI, « Virtual Currencies: Key Definitions and Potential AML/CFT Risks » (Monnaies virtuelles: Définitions clés et risques potentiels en matière de LBC/FT), juin 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> consulté le 25 août 2021.
12. FATF-GAFI, « Public Statement on Virtual Assets and Related Providers », 21 juin 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html>, consulté le 24 août 2021.
13. FATF-GAFI, « Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers » (Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels), juin 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>, consulté le 24 août 2021.

Les Lignes directrices du GAFI ont été révisées par deux reprises depuis leur publication, en juillet 2020 et en juillet 2021.[14] Elles sont également actualisées régulièrement, afin d'améliorer les recommandations et de demeurer à jour par rapport aux innovations dans le secteur des 'AV. Pour cela, le GAFI lance des consultations publiques sur les Lignes directrices.[15]

Les Exigences Internationales

Le présent document d'orientation vise à présenter un ensemble de normes conformes aux recommandations et règlementations internationales les plus exigeantes concernant la conformité en matière d'AV. Il convient de noter, néanmoins, qu'il ne suit pas de règlementation nationale particulière sur les cryptomonnaies. Veuillez vous assurer de bien comprendre les règlementations des pays pertinents à l'attention des PSAV avant de tenter de mettre en œuvre l'une des directives contenues dans le présent document. Par ailleurs, s'il n'existe pas de règlementation dans le(s) pays en question, veuillez vous assurer de bien comprendre les recommandations du GAFI. Voir annexe I pour en savoir plus sur ce point.

14. FATF-GAFI, « 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers », juillet 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>, consulté le 24 août 2021 ; FATF-GAFI, « Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers », juillet 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>, consulté le 24 août 2021.
15. FATF-GAFI, « Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers », mars 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>, consulté le 24 août 2021.

II. Terminologie

LE PRÉSENT DOCUMENT d'orientation emploie le vocabulaire utilisé par le GAFI. Aussi, les expressions « actif virtuel » (AV) et « prestataire de services d'actifs virtuels » (PSAV) sont utilisés dans l'ensemble du document.

Veuillez noter que bien que le terme « PSAV » soit employé, sa portée est plus étroite que celle de la définition du GAFI. Alors que la définition du GAFI inclut toute entreprise impliquée dans une transaction AV-monnaie fiduciaire, transaction AV-AV, tout transfert, protection, administration d'AV et toute entreprise qui fournit des services financiers afférents aux AV,[16] le présent document d'orientation définit les PSAV comme étant un **marché d'actifs virtuels centralisé** proposant des services AV-monnaie fiduciaire ou AV-AV.

D'une manière similaire, le terme AV ne s'applique qu'aux jetons de paiement, comme les Bitcoins, et n'a pas trait aux cryptomonnaies stables ou aux devises numériques des banques centrales. Dans ce document, l'expression AV est équivalente aux termes « cryptomonnaie », « monnaie virtuelle » ou « cryptoactif ».

Les « portefeuilles » d'AV prennent des formes diverses, et le présent document ne différencie pas entre les portefeuilles immatériels (en ligne) et les portefeuilles matériels (hors ligne). Les portefeuilles préservent la sécurité et l'accessibilité des clés privées des utilisateurs, et ils sont proposés par de nombreux prestataires, y compris les marchés centralisés.

Méthodologie

Les présentes orientations ont été élaborées dans le cadre du projet CPF du RUSI en cours. L'équipe RUSI analyse les activités de FP depuis 2015,[17] y compris en menant des recherches continues sur le rôle que les AV et d'autres systèmes de paiement jouent dans le non-respect des sanctions, concentrant largement ses efforts sur la Corée du Nord.[18] Les présentes orientations se fondent sur l'expertise de l'équipe RUSI dans ce domaine, des recherches approfondies et des conversations informelles au cours de ces trois dernières années avec des parties prenantes de secteurs pertinents, y compris des PSAV, des régulateurs, des agents chargés de l'application de la loi, des banques traditionnelles, des néo-banques et des universitaires.

16. GAFI, « International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations » (Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération :les recommandations du GAFI), mis à jour en juin 2021, p. 130.
17. Pour en savoir plus sur les publications du RUSI en matière de FP, veuillez consulter RUSI, « Proliferation Financing », <https://rusi.org/explore-our-research/topics/proliferation-financing>, consulté le 24 août 2021.
18. Pour obtenir des informations plus détaillées sur l'activité de la Corée du Nord en matière d'AV, veuillez consulter David Carlisle et Kayla Izenman, « Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia », RUSI Occasional Papers (avril 2019).

III. Conditions Préalables

LA PRÉSENTE SECTION se concentre sur tous les aspects du système de conformité qui doivent être en place avant d'intégrer quelque client que ce soit. Ces aspects incluent la présence d'une équipe efficace et compétente chargée de la conformité, des évaluations initiales des risques, une compréhension approfondie de l'ensemble des exigences nationales et internationales pertinentes, une formation et des protocoles adéquats en matière de cybersécurité, et une politique sur mesure concernant les décisions concernant le référencement des cryptomonnaies.

L'Équipe Chargée de la Conformité

Afin d'assurer la mise en œuvre adéquate de toutes les lignes directrices ci-dessous, les PSAV doivent, tout d'abord, veiller à disposer de la structure de gouvernance et de l'équipe chargée de la conformité adaptées. La structure organisationnelle d'un PSAV doit garantir que les personnes en charge de la conformité disposent des ressources, de l'autorité, de l'information et de l'indépendance nécessaires pour évaluer et gérer les risques en matière de lutte contre la criminalité financière.

Une structure de gouvernance exhaustive tient compte de l'ensemble des échelons de l'entreprise. La haute direction doit avoir la responsabilité finale concernant la supervision et l'efficacité du programme de lutte contre la criminalité financière.

Un programme efficace exige également l'existence d'un responsable de la conformité, connu, en général, sous le nom de Directeur de la conformité, qui est responsable en dernier ressort de la conception et de la mise en œuvre du programme de conformité, ainsi que d'assurer le respect de l'ensemble des obligations règlementaires et légales. Dans les sociétés de plus grande taille, un Directeur de la conformité et de l'application des sanctions peut également être présent afin de superviser les exigences spécifiques en matière de sanctions et de veilleur à leur conformité.

Les employés débutants ou de niveau intermédiaire, à tous les niveaux de la société, doivent également avoir connaissance des signaux d'alarme concernant les transactions, ainsi que des exigences en matière de vérification et de signalement, des méthodes d'enquête et des autres procédures de conformité pertinentes susceptibles de s'appliquer dans d'autres domaines des opérations commerciales du PSAV.

Certains secteurs règlementés exigent des rôles spécifiques pour l'équipe chargée de la conformité. La direction doit s'assurer que ces exigences sont prises en considération lors de la mise en place de l'équipe chargée de la conformité. Tous les membres de l'équipe chargée de la conformité doivent suivre des formations régulières afin de connaître les nouvelles tendances en matière d'AV, les outils de conformité spécifiques aux AV et l'ensemble de la règlementation locale, nationale et internationale pertinente.

Évaluation des Risques

Les PSAV doivent entreprendre régulièrement une évaluation des risques en interne, afin d'identifier les clients, secteurs ou types de transactions susceptibles d'être davantage exposés aux activités liées

au blanchiment de capitaux (BC)/financement du terrorisme (FT)/financement de la prolifération (FP), ainsi que pour élaborer et mettre en œuvre des contrôles visant à atténuer ces risques spécifiques. Les évaluations des risques sont régulièrement menées concernant des sujets similaires par les institutions financières, et les PSAV devraient adopter, eux aussi, une telle approche.

Les évaluations des risques doivent être consignées par écrit et mises à la disposition des organismes de contrôle, pour inspection. Elles se composent de trois éléments : les menaces, les vulnérabilités et les conséquences.

Pour ce qui est du FP, le GAFI considère que le terme « menace » désigne toute personne ou entité ayant contourné, violé ou exploité par le passé des sanctions liées au FP, ou qui a le potentiel de le faire à l'avenir. Les « vulnérabilités » désignent tout ce qui peut être exploité par la menace, par exemple, les lacunes dans la règlementation ou les faiblesses en matière de cybersécurité . Elles comprennent les vulnérabilités géographiques et spécifiques à un secteur. Les « conséquences » désignent le résultat selon lequel des fonds ou des actifs deviennent accessibles aux acteurs des menaces, non seulement en termes de financement des ADM, mais aussi concernant l'impact ultime sur les opérations commerciales et la réputation du PSAV.[19]

La frontière entre les menaces et les vulnérabilités peut être floue, mais il importe de comprendre l'interaction entre les deux, ainsi que tous facteurs d'atténuation. Lorsque l'on analyse les menaces et les vulnérabilités, il convient de tenir compte au moins des considérations suivantes :

- Les acteurs de menaces connus.
- Les typologies de financement de la délinquance connues.
- La taille et la complexité du PSAV.
- Les produits et les services proposés.
- La méthode de fourniture des produits et des services.
- Les types de clients.
- La position physique des clients.
- L'emplacement physique du PSAV et la règlementation pertinente.
- Les institutions associées.

Le résultat de l'évaluation des risques doit indiquer au PSAV les domaines dans lesquels ses risques inhérents s'avèrent particulièrement élevés. Les risques inhérents sont généralement définis comme le niveau de risque existant en l'absence de contrôles. Cette information deviendra plus claire après réalisation d'une évaluation des risques exhaustive. Dans le cadre de l'évaluation du risque, ces contrôles doivent être considérés comme étant des facteurs d'atténuation.

Les conséquences potentielles du FP sont plus graves que celles du BC ou du FT. Les PSAV doivent évaluer les impacts et dommages physiques, sociaux, environnementaux, économiques et structurels.

Pour en savoir plus sur la réalisation d'évaluations des risques pour les PSAV, veuillez consulter l'annexe I.

19. Pour en savoir plus sur les définitions de ces trois éléments, veuillez consulter FATF-GAFI, « Guidance on Proliferation Financing Risk Assessment and Mitigation », juin 2021, p. 9.

Cybersécurité

Outre les procédures de conformité, au vu de l'ampleur avec laquelle les attaques informatiques sont déployées pour financer la prolifération, il s'avère essentiel de mettre l'accent sur la cybersécurité . Ceci inclut aussi bien la formation du personnel de tous les niveaux du PSAV que des investissements dans des professionnels de la cybersécurité , afin que ceux-ci installent des protections pour les PSAV.

La formation du personnel aux protocoles de cybersécurité est essentielle pour se protéger des pirates informatiques qui travaillent pour le compte des prolifératrices. On sait que la Corée du Nord a été impliquée dans des machinations compliquées d'hameçonnage, afin d'infiltrer les PSAV, comme son attaque contre DragonEx en 2019.

Étude de cas 1 : DragonEx (2019)

En mars 2019, la Corée du Nord a mis en œuvre une machination élaborée d'hameçonnage par laquelle un salarié du PSAV DragonEx a installé, à son insu, des maliciels dans un ordinateur contenant des clés privées du portefeuille du PSAV, ce qui a permis à la Corée du Nord de voler des millions de dollars en actifs virtuels. Les chercheurs ont découvert que Lazarus, un groupe de cybercriminels nord-coréen, était responsable de l'attaque, laquelle a débouché sur une perte de plus de 7 millions de dollars US.

Lazarus avait enregistré deux domaines Internet, créé un faux logiciel de commercialisation d'AV avant d'y intégrer des codes malveillants, occultant la tromperie au sein d'une plateforme de négociation automatisée d'AV qui avait fonctionné normalement pendant six mois. Les assaillants avaient alors envoyé le logiciel au personnel de divers PSAV, sous couvert d'une promotion. En ouvrant le module d'installation du maliciel, le personnel du service client de DragonEx avait ainsi permis aux pirates d'obtenir la clé privée du portefeuille du PSAV et de perpétrer le vol.

Sources : Lylian Teng, « Alert! Lazarus Hacker Group Continues Targeting Crypto Using Faked Trading Software », 8BTC, 1er avril 2019, <https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software> consulté le 24 août 2021 ; Chainalysis, « As Exchanges Beef Up Security Measures, Hackers Get More Sophisticated », 21 janvier 2020, <https://blog.chainalysis.com/reports/cryptocurrency-exchange-hacks-2019> consulté le 25 août 2021.

La formation est essentielle, ainsi que la protection physique du PSAV contre ces types d'attaques. Les membres du personnel doivent être tenus de participer régulièrement à des sessions de formation à la cybersécurité et doivent savoir ce que l'on attend d'eux et comment identifier des courriers électroniques, pièces jointes, liens et programmes potentiellement suspects. Tout le personnel doit être tenu de participer à ces sessions et pas uniquement les membres des équipes impliqués dans le programme de conformité. Les PSAV doivent également investir spécifiquement dans une infrastructure informatique et de cybersécurité appropriée, afin de s'assurer que les assaillants ne peuvent pas infiltrer le système de l'extérieur.[20]

20. Pour en savoir plus sur les protections recommandées en matière de de cybersécurité , veuillez consulter Cloud Security Alliance, « Crypto-Asset Exchange Security Guidelines », 13 avril 2021, <https://

Exigences en Matière de référencement des Actifs

Au vu de l'intérêt croissant que les délinquants portent aux jetons privés, lesquels peuvent leur permettre de faire circuler les AV sans être détectés, il s'avère essentiel de considérer les capacités de traçage des blockchains pour tout actif répertorié sur la plateforme d'un PSAV. Il existe un grand éventail d'options susceptibles de contribuer à atténuer les risques posés par les jetons privés. Une option consiste simplement à proposer des actifs avec des blockchains transparentes exclusivement (autrement dit, ne pas accepter du tout les jetons privés). Si une telle option ne s'avère pas appropriée, et du fait que le listage des jetons privés constitue un risque accepté et fait partie intégrante de la stratégie commerciale du PSAV, les mesures suivantes d'atténuation des risques devraient être envisagées :

- répertorier uniquement un nombre limité de jetons privés disposant au moins d'une quelconque mesure de transparence (par exemple, Zcash) et pour lesquels l'analyse du traçage des blockchains est disponible ;
- permettre l'utilisation des jetons privés uniquement pour les transactions AV-AV (autrement dit, permettre l'échange de jetons privés contre d'autres AV, mais pas contre des monnaies fiduciaires), afin d'entraver l'encaissement des monnaies fiduciaires ;
- permettre aux clients d'échanger des jetons privés uniquement s'ils se soumettent à une procédure de vigilance renforcée et si lesdits échanges sont soumis à des limites et des plafonds stricts.

cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/>, consulté le 22 août 2021.

IV. Sanctions et Vérification des PPE

LES SANCTIONS S'APPLIQUENT à tous les clients et à toutes les transactions, peu importe le montant. Les PSAV doivent se conformer pleinement aux listes de sanctions internationales et nationales pertinentes, afin d'éviter de détenir des comptes pour des acteurs désignés, ou pour n'importe qui serait détenu ou contrôlé par de tels acteurs ou qui agirait pour leur compte ou sous leurs instructions. La vérification des sanctions doit être effectuée lors du premier contrôle de l'identité, ainsi que régulièrement, pendant toute la durée de la relation avec le client,[21] pour toute transaction entrante ou sortante, ou lorsque des ajouts sont opérés dans les listes de sanctions.

Le Bureau de contrôle des avoirs étrangers (OFAC) des États-Unis d'Amérique a également inclus, par le passé, des adresses d'AV dans ses listes de sanctions, qui devraient être repérées en plus des noms répertoriés.[22] L'OFAC a aussi sanctionné de nombreux groupes et personnes physiques pour des actes de contournement des sanctions par le biais d'AV. Il est conseillé de tenir compte des listes de sanctions des États-Unis d'Amérique, en plus de toutes les listes internationales. L'OFAC a spécifiquement inclus des adresses d'AV appartenant à des acteurs qui blanchissent des capitaux pour le compte de la Corée du Nord, montrant ainsi l'importance de ces listes pour s'attaquer au risque de financement de la prolifération.

Étude de cas 2 : Tian Yinyin et Li Jiadong (2020)

En mars 2020, l'OFAC a sanctionné Tian Yinyin et Li Jiadong, deux ressortissants chinois qui blanchissaient des AV pour le compte de la Corée du Nord. Ces acteurs ont été sanctionnés dans le cadre des programmes CYBER2 et DPRK3 États-Unis d'Amérique, et signalés comme associés au groupe de pirates informatiques nord-coréen Lazarus.

L'ajout à la liste par l'OFAC de chacune de ces personnes inclut ses coordonnées personnelles, mais aussi toutes les adresses de Bitcoins associées connues. Tian, par exemple, a huit adresses de Bitcoins répertoriées. Les listes incluent les alias connus, dans ce cas les ID en ligne des malfaiteurs.

Source : Pour en savoir plus sur les listes de l'OFAC, veuillez consulter le communiqué du Département du Trésor des États-Unis d'Amérique, « Treasury Sanctions Invididuals Laundering Cryptocurrency for Lazarus Group », 2 mars 2020, <https://home.treasury.gov/news/press-releases/sm924>, consulté le 24 août 2021 ; OFAC, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=28263>, consulté le 24 août 2021.

21. C'est le cas, par exemple, lorsque les informations du client changent (dirigeants, propriété, coordonnées d'identification).

22. Cette pratique a commencé en 2018, lorsque l'OFAC a listé les adresses d'AV d'acteurs informatiques affiliés à l'Iran. Veuillez consulter le communiqué de presse du Département du Trésor des États-Unis d'Amérique, « Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses », , 28 novembre 2018, <https://home.treasury.gov/news/press-releases/sm556>, consulté le 24 août 2021.

Outre les listes de sanctions, tous les acteurs ou groupes mentionnés dans les rapports du Groupe d'experts des Nations unies doivent être inclus dans la vérification des sanctions. Pour en savoir plus sur ces rapports, veuillez consulter l'annexe I.

Les PSAV doivent également procéder à une vérification des médias et consulter les rapports de typologie des ONG et du secteur privé, y compris ceux des entreprises d'analyse de blockchain et de cybersécurité. Ces acteurs publient régulièrement des conclusions concernant aussi bien les signaux d'alarme afférents à l'utilisation des AV par la Corée du Nord que les individus et les organisations affiliés à ce dernier pays. D'une manière similaire, les PSAV doivent vérifier les clients et de manière continue, afin de vérifier s'il s'agit de personnes politiquement exposées (PPE) (ou sont en relation avec de telles personnes).[23] Si tel est le cas, une procédure de vigilance renforcée devra être mise en œuvre. Pour en savoir plus sur la vigilance renforcée, veuillez consulter le paragraphe ci-dessous.

23. Le GAFI définit une personne politiquement exposée (PPE) comme étant « une personne exerçant ou ayant exercé une fonction publique éminente » et qui peut occuper une « fonction susceptible d'être utilisée abusivement à des fins de (…) blanchiment d'argent [fonds illicites] ». Veuillez consulter FATF-GAFI, « FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) », juin 2013, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf>, consulté le 22 août 2021.

V. Intégration du Client

L'INTÉGRATION DU CLIENT constitue l'étape suivante dans le cycle de conformité. Souvent, les PSAV ont des inquiétudes concernant le niveau d'information à demander aux clients lors du premier contact. Bien que les entreprises puissent opérer de manières différentes et les pays avoir des exigences variables, il existe des principes et meilleures pratiques communs qui offrent les meilleures chances de détecter une activité suspecte.

Les processus Connaissance du client (Know Your Customer (KYC))

Les processus KYC constituent la norme dans les banques et devraient également le devenir pour les PSAV. Hélas, un rapport de 2020 indiquait que 56 % des PSAV dans le monde disposent de processus KYC faibles ou perméables.[24] Il est possible d'adopter des mesures préalables simples pour s'assurer qu'un PSAV ne relève pas d'un tel groupe.

De nombreux PSAV permettent de créer un compte sans opérer une vérification de l'identité, mais exigent des informations additionnelles pour l'envoi ou la réception de fonds. Certains PSAV imposent même une vérification préalablement à la création du compte, alors que d'autres mettent en place un processus KYC uniquement lorsque les transactions concernent des monnaies fiduciaires.

Au sens des meilleures pratiques, le processus KYC doit avoir lieu avant que les fonds soient déposés ou acceptés par le client, que ce soit au moment de la création du compte ou immédiatement avant la réalisation de la première transaction.

La première étape consiste à identifier le client et à vérifier son identité. Bien que les autorités de contrôle puissent exiger des informations additionnelles particulières, les renseignements suivants, au minimum, devront être collectés auprès des personnes physiques :

- Nom, date de naissance et nationalité (vérifiés en utilisant le processus d'identification gouvernemental officiel).
- Adresse vérifiée en utilisant un document justificatif de celle-ci, comme un relevé bancaire, une facture d'eau ou d'électricité, une feuille d'impôts émise par le gouvernement, un document d'assurance habitation ou un certificat de résidence, ou encore par le biais de moyens numériques fournissant une assurance raisonnable sur l'emplacement physique du client.

Par ailleurs, au minimum, les renseignements suivants doivent être collectés auprès des entités juridiques :

- Dénomination, immatriculation, adresse et statut (vérifiés par le biais du numéro de l'entreprise ou de documents d'immatriculation ou registres gouvernementaux pertinents).

24. CipherTrace, « CipherTrace 2020 Geographic Risk Report: VASP KYC by Jurisdiction », octobre 2020, p. 4, <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>, consulté le 24 août 2021.

- Informations d'identification concernant le personnel de direction clé, y compris les opérateurs autorisés sur le compte du client.
- Structure de propriété.

Des processus KYC (et de vigilance renforcée permanente) devraient être menés non seulement pour les clients eux-mêmes, mais également pour tous les bénéficiaires ainsi que les personnes agissant pour le compte du client.

Les PSAV doivent également s'assurer que leurs processus de vérification de l'information sont exhaustifs. Ces processus incluent la demande des documents officiels susvisés et l'assurance de leur légitimité, ainsi que la prise en compte des mécanismes KYC additionnels, que ce soit lors de l'intégration ou à l'occasion d'une transaction suspecte. Ces exigences supplémentaires peuvent inclure :

- Des « selfies » pris avec l'application même, y compris un test « de vie », afin de prouver que le visage téléchargé correspond à une personne vivante présente au moment de la prise de l'image.
- Appels vidéo.

Les vérifications d'identité et les tests « de vie » s'avèrent essentiels pour une conformité efficace, notamment au regard des tactiques utilisées par les personnes impliquées dans le financement de la prolifération. En 2020, des blanchisseurs de capitaux qui faisaient circuler des fonds pour le compte de la Corée du Nord n'ont pas été en mesure de remplir les exigences de conformité afférentes à l'appel vidéo d'un PSAV, ce qui, idéalement, aurait empêché le blanchiment des fonds par le biais de la plateforme.

Étude de cas 3 : 'VCE3' (2020)

Dans le même cas que celui décrit dans l'Étude de cas 2, outre les sanctions de l'OFAC, le Département de laJustice des États-Unis d'Amérique avait poursuivi en justice Tian Yinyin et Li Jiadong pour le blanchiment de plus de 100 millions de dollars US en plusieurs cryptomonnaies pour le compte de la Corée du Nord. Les jetons avaient été obtenus dans le cadre de piratages informatiques de PSAV nord-coréens, et Tian et Li avaient tenté de faire circuler les fonds par le biais de PSAV multiples, avec des résultats largement satisfaisants.

Afin de fournir suffisamment de documents aux PSAV dans le cadre du processus d'intégration, Tian et Li avaient édité des photos de personnes physiques en utilisant des informations personnelles volées. Un PSAV (VCE3) n'avait pas été satisfait avec l'image fournie et avait demandé un appel vidéo avec le titulaire du compte, ce qui a été refusé. En dépit de cela, VCE3 avait accepté les transactions de Tian et Li, recevant presque 2 millions de dollars US de fonds volés dans le compte des délinquants. Si ledit appel vidéo, ainsi que des mesures de vigilance renforcée subséquentes, des rapports élaborés et/ou un refus de services avaient constitué une exigence de la part de tous les PSAV impliqués dans le blanchiment, les fonds n'auraient pas pu être blanchis par le biais de la plateforme.

Source : Département de la Justice des États-Unis d'Amérique, « Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack », 2 mars 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, consulté le 24 août 2021.

Nature et Finalité de la Relation

La nature et la finalité de la relation avec le client sont aussi importantes que l'identification du client. Le seul moyen de comprendre parfaitement ce qu'est une activité suspecte pour un client donné est de comprendre quelle est l'activité régulière de ce client ou à quoi elle devrait ressembler. Pour comprendre pleinement la nature et l'objet de la relation lors de l'intégration du client, les estimations suivantes devraient, à minima, être demandées au client :

- Fréquence escomptée des transactions.[25]
- Taille escomptée des transactions.
- Volume escompté des transactions.

Source et Destination des Fonds

Il s'avère essentiel que le PSAV comprenne aussi bien la source que la destination de tous les fonds qui transitent par le biais de la plateforme. En particulier, lorsqu'une vigilance renforcée est nécessaire, les PSAV doivent collecter des informations concernant la source des fonds du client, ainsi qu'en vérifier la légitimité avant de réaliser quelque transaction que ce soit pour le compte du client. Pour en savoir plus sur la vigilance renforcée, veuillez consulter la section dédiée à ce sujet dans les développements qui suivent.

D'une manière similaire, lorsqu'un client reçoit des fonds ou effectue des transactions, le PSAV doit tenter de collecter les informations pertinentes concernant l'autre partie.[26] Les outils d'analyse des blockchains peuvent fournir des renseignements accrus sur la source et la destination ultimes des fonds, et leur utilisation est recommandée à cette fin.

25. Ici, « transaction » désigne un dépôt, un retrait ou un échange.
26. Les moyens d'exploiter cette possibilité sont en cours de discussion, conformément à la Recommandation 16 du GAFI. Pour l'heure, les marchés doivent demander l'information qu'ils sont en mesure de collecter auprès des clients. Veuillez consulter FATF-GAFI, « International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations » (Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération :Les Recommandations du GAFI), p. 17.

VI. Surveillance Continue et Obligation de Vigilance vis-à-vis de la Clientèle

APRÈS L'INTÉGRATION DU client, l'étape suivante est celle consistant à assurer une vigilance vis-à-vis de la clientèle qui soit permanente et effective. Ceci implique un contrôle des transactions, dans un effort visant à identifier toute activité inhabituelle, comme un écart par rapport aux transactions attendues ou anticipées, ainsi qu'à comprendre le raisonnement et la finalité derrière toute variation constatée sur la plateforme. L'activité inhabituelle ou suspecte non susceptible d'être expliquée par le client peut mettre en évidence vers des connexions de BC/FT/FP potentiel. L'activité des clients devrait être analysée en permanence, pendant toute la durée de la relation, afin de s'assurer qu'elle est conforme au processus KYC mené lors de leur intégration, et que la nature et la finalité des transactions demeurent cohérentes avec celles indiquées par les clients dans le cadre des processus d'intégration et KYC. Toute modification importante devra être documentée et questionnée. Les informations KYC devraient, elles aussi, être révisées périodiquement, en fonction du risque ou d'évènements déclencheurs, comme un changement d'adresse.

Tout client réputé présenter un risque plus élevé lors de l'intégration ou à n'importe quel moment du processus de vigilance vis-à-vis de la clientèle devrait faire l'objet d'un contrôle plus fréquent et approfondi.

Les PSAV devraient également s'assurer que tous les documents et informations soumis lors de l'intégration sont tenus à jour pendant toute la durée de la relation.

Si un client requière une vigilance renforcée, la source et la destination des fonds identifiées lors de son intégration devraient continuer de faire l'objet de recherches pendant toute la durée de la relation.

Suivi Manuel ou Suivi Automatique

Tout système de contrôle des transactions vise à donner l'alerte en cas de transaction et/ou activité suspecte ou inhabituelle, afin de l'examiner de plus près. Toutes les activités ainsi signalées doivent être contrôlées rapidement par des personnes spécifiquement formées, lesquelles adopteront les mesures nécessaires en fonction de leurs conclusions, comme le signalement aux autorités règlementaires pertinentes et/ou le dépôt d'un rapport de transaction/activité suspecte (RTS/RAS). Cela peut se faire lors du processus KYC, lorsqu'une transaction est effectuée et signalée, ou une fois que celle-ci a eu lieu.

Bien que le contrôle et le traçage des blockchains puissent se faire manuellement, le recours à des solutions tierces d'analyse automatisée des blockchains est fortement recommandé. L'analyse des blockchains aide à comprendre plus précisément tous les modèles de comportement et permet de signaler toute adresse ou tout portefeuille criminel(le). Les évaluations des risques pour les clients s'avèrent, elles aussi, bien plus nuancées lorsqu'elles sont examinées à travers le prisme de l'analyse des blockchains. L'analyse des blockchains doit inclure une vérification des portefeuilles avant et après la transaction, afin d'identifier

la source et la destination des fonds. L'analyse des blockchains et la compréhension renforcée des modèles de transactions, ainsi que la coordination avec les organismes chargés de l'application de la loi permettent aux PSAV de réagir rapidement en cas de piratage ou de vol de fonds, et de geler ces derniers si besoin est, une technique utilisée par le passé pour lutter contre le financement de la prolifération par le biais des AV.

Étude de cas 4 : « Marché 9 » (2019)

Le Département de la Justice des États-Unis d'Amérique a divulgué une plainte de confiscation civile en août 2020 mettant en évidence les piratages informatiques de PSAV par des acteurs nord-coréens, qui avaient blanchi des fonds par le biais des marchés de gré à gré chinois.

La plainte indique qu'en décembre 2019, l'un des auteurs avait tenté de convertir de l'Ethereum volé en Bitcoins par le biais d'un PSAV (Marché 9). L'Ethereum volé avait été piraté auprès d'un autre PSAV (Marché 2), ce qui avait été publié. Il s'en est suivi que Marché 9 a gelé les fonds impliqués dans la transaction, les jetons volés du Marché 2 ayant été signalés dans son système. Les fonds demeurent gelés auprès de Marché 9.

Source : Département de la Justice des États-Unis d'Amérique, « United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors », 27 août 2020, <https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two>, consulté le 24 août 2021.

Les PSAV devraient non seulement investir dans des solutions d'analyse des blockchains, mais aussi dans des outils de contrôle et de lutte contre le blanchiment de capitaux (LBC) qui recherchent des comportements transactionnels classiques de BC/FT/FP.

Vigilance Renforcée

Une vigilance renforcée devrait être menée lorsqu'une transaction ou un compte est signalé(e) comme présentant un risque particulièrement élevé ou comme potentiellement suspect(e). Des indicateurs de risque particulièrement élevé peuvent être consultés dans la section qui suit. La vigilance renforcée repose sur un contrôle efficace. Elle doit être mise en œuvre sur un système fondé sur le risque, lorsqu'un crime financier est suspecté. Il existe un large éventail de raisons pour lesquelles une vigilance renforcée pourrait s'avérer nécessaire, y compris (à titre non limitatif) les cas où un client :

- est identifié, dans le cadre d'une évaluation des risques, comme présentant un risque particulièrement élevé de criminalité financière ;
- a une structure commerciale inutilement complexe ou opaque ;
- réalise des transactions avec des personnes physiques ou morale se trouvant sur des territoires à haut risque ;
- fournit une identification volée ou fausse lors de son intégration ;
- participe à des transactions qui ne correspondent pas à la nature et à la finalité de la relation ;
- envoie, reçoit ou fait circuler des montants exceptionnellement élevés d'actifs virtuels ou de monnaie fiduciaire ;

- est une PPE ;
- n'est pas en mesure d'expliquer de manière satisfaisante la finalité d'une transaction.

Il convient de noter que la définition de « montants élevés » d'actifs virtuels est relative et dépend de la taille du PSAV et de la nature de la relation avec le client.

Si l'une ou plusieurs de ces préoccupations sont identifiées, une procédure de vigilance renforcée devra être lancée. La première étape consiste à obtenir des informations d'identification additionnelles. Certaines d'entre elles pourront être demandées au client, et d'autres pourraient être obtenues séparément, par le biais de sources ouvertes. Pour une PPE, par exemple, son titre et des détails sur ses fonctions pourraient s'avérer nécessaires.

Une vérification des médias défavorables/préjudiciables devrait également être entreprise, afin de créer un profil complet. Des résultats massivement négatifs dans le cadre d'une telle vérification pourraient désigner un client avec lequel la poursuite de la relation s'avère trop risquée.

Des entretiens téléphoniques ou vidéo peuvent aussi être des outils nécessaires pour comprendre la nature et la finalité des transactions.

De nombreux PSAV enregistrent les adresses IP des clients, ainsi que l'emplacement des distributeurs automatiques/banques/autres PSAV impliqués dans tout échange, afin de s'assurer que ces emplacements correspondent à la relation attendue.

Les réseaux privés virtuels (RPV) peuvent, eux aussi, constituer un indicateur de risque susceptible de déboucher sur une procédure de vigilance renforcée dans certaines circonstances . Bien qu'il existe des utilisations légitimes des réseaux privés virtuels (RPV) pour créer des environnements d'échange sûrs, il devrait au moins exister un point de contact lorsqu'un RPV n'est pas actif, comme un enregistrement auprès d'un PSAV, afin que ce dernier consigne une adresse IP authentique.

VII. Indicateurs de Risque Élevé et Signaux d'Alarme

IL EXISTE TOUTE une série d'indicateurs de risque élevé et de signaux d'alarme susceptibles de déboucher sur une procédure de vigilance renforcée, RTS/RAS, voire même le gel des fonds. Le GAFI, le secteur privé et les autorités de règlementation nationales disposent tous de listes exhaustives de signaux d'alarme identifiés avec les études de cas correspondantes. Veuillez consulter l'annexe I pour en savoir plus à ce propos.

Utilisation de services de mixage ou d'anonymisation

Les mixeurs, portefeuilles confidentiels et services CoinJoin[27] fournissent tous des types variés d'obscurcissement des transactions et renforcent la confidentialité pour l'utilisateur. Chacun de ces services obscurcit le cheminement de la transaction et rend le traçage des blockchains de plus en plus difficile, voire parfois impossible.[28]

Il est essentiel que les PSAV puissent identifier les transactions effectuées avec des mixeurs et des portefeuilles confidentiels, pour traiter les transactions liées à des mixeurs comme présentant un risque élevé, dans la plupart des cas.

Une telle gestion du risque devrait inclure :

- la création d'une liste approuvée de mixeurs connus et/ou de confiance ou de services CoinJoin, avec lesquels les clients sont autorisés à effectuer leurs transactions ;
- l'autorisation de relations uniquement avec des mixeurs de confiance selon des conditions particulières (d'un montant inférieur à un certain seuil).

On sait que les blanchisseurs et pirates informatiques travaillant pour le compte des prolifératrices utilisent des mixeurs de plus en plus fréquemment. Le Groupe Lazarus, en particulier, est connu pour son intérêt pour cette technologie et pour son utilisation des services de mixage pour obscurcir les cheminements des transactions.

---

27. CoinJoin est une stratégie d'anonymisation qui préserve la confidentialité des transactions affectuées avec des cryptomonnaies. Elle utilise des contrats intelligents pour mixer les cryptomonnaies dans de nouvelles transactions, où les sortants sont constitués du nombre de cryptomonnaies, mais issus de toute une série de transactions différentes, obscurcissant ainsi la source et la destination prévue.
28. Pour en savoir plus sur les spécificités de ces technologies, veuillez consulter Anton Moiseienko et Kayla Izenman, « From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency », RUSI Occasional Papers (septembre 2019), pages 19–24 ; Andrea O'Sullivan, « What are Mixers and "Privacy Coins"? », Coin Center, 7 juillet 2020, <https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/>, consulté le 24 août 2021.

Case Study 5: Groupe Lazarus (2018)

Dans son rapport sur la cryptocriminalité de 2020 (2020 Crypto Crime Report), la société de traçage des blockchains basée aux États-Unis d'Amérique, Chainalysis, décrivait la façon dont le Groupe Lazarus avait modifié ses méthodes entre 2019 et 2020. L'un des éléments mis en évidence était que Lazarus avait augmenté son usage des mixeurs et des portefeuilles CoinJoin.

Selon Chainalysis, 48 % des fonds volés par Lazarus transitaient par des portefeuilles CoinJoin en 2019. Lors du piratage DragonEx (Étude de cas 1), par exemple, Lazarus avait fait circuler des altcoins volés à des PSAV, comme Ethereum et Litecoin, les échangeant contre des Bitcoins. Ensuite, ils avaient transféré les Bitcoins dans divers portefeuilles locaux, avant d'envoyer les fonds dans un portefeuille Wasabi, qui mixe les bitcoins par le biais du protocole CoinJoin.

Bien que le rapport sur la crypto-criminalité de 2021 donne des précisions sur d'autres techniques utilisées par Lazarus, les statistiques de Chainalysis montrent également que le recours par Lazarus aux mixeurs pour blanchir des fonds volés a augmenté encore davantage en 2020.

Source : Chainalysis, « The 2020 State of Crypto Crime », janvier 2020, <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>, consulté le 24 août 2021 ; Chainalysis, « The 2021 State of Crypto Crime », 16 février 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>, consulté le 2 septembre 2021.

VIII. Exigences en Matière de Signalement

LES EXIGENCES EN matière de signalement et de dépôts des RTS/RAS peuvent varier de manière significative selon les pays, tandis que d'autres pays n'exigent pas encore de signalement de la part des PSAV. Néanmoins, les PSAV doivent être préparés à respecter les exigences les plus élevées (comme d'autres fournisseurs de services financiers règlementés) et se tenir pleinement au courant des exigences en vigueur sur les territoires sur lesquels ils interviennent. Il doit être demandé au personnel de signaler toute activité suspecte, et un processus clair doit être mis en place. Il doit notamment effectuer les signalements auprès de la personne désignée, et celle-ci lancera l'enquête appropriée et effectuera les déclarations auprès des autorités pertinentes.

Ce processus doit être clairement présenté au personnel. Les dispositions pertinentes doivent être standardisées et définies afin d'être facilement comprises aussi bien par l'unité de renseignements financiers pertinente que par le PSAV. Des RTS/RAS peuvent être déposés pour des rapports afférents à :

- des inquiétudes concernant la source des fonds reçus dans le portefeuille d'un utilisateur ;
- des transactions structurées en des petits montants, juste sous les seuils de déclaration ;
- des transferts d'AV immédiats vers des PSAV opérant dans d'autres pays , notamment des pays où la règlementation concernant les PSAV est faible ;
- la réception dans le portefeuille d'un utilisateur de fonds en provenance d'adresses d'AV ayant par le passé fait l'objet d'une alerte en rapport avec des fonds volés ou des maliciels ;
- des documents ou photographies falsifié(e)s ou modifié(e)s utilisé(e)s à des fins d'identification ;
- l'impossibilité pour le PSAV d'obtenir les informations demandées au client, ou un client qui refuse de fournir les documents afférents à la vigilance vis-à-vis de la clientèle ou des renseignements sur la source des fonds.

Veuillez noter que cette liste n'est pas exhaustive. Le signalement devra se faire chaque fois que les processus internes donnent l'alerte sur une activité suspecte.[29]

29. L'Autorité monétaire des Îles Caïman a publié une liste des signaux d'alarme additionnels potentiels susceptibles de déclencher des obligations de déclaration pour les PSAV sur ce territoire. Veuillez consulter « Guidance Notes (Amendments) on the Prevention and Detection of Money Laundering, Terrorist Financing, and Proliferation Financing in the Cayman Islands » de l'Autorité monétaire des Îles Caïman, février 2021, p. 13.

IX. Observations Finales

BIEN QUE LES orientations règlementaires et de conformité des PSAV aient augmenté considérablement au cours de ces dernières années, des progrès considérables restent à accomplir. Il s'avère absolument essentiel que les PSAV réalisent des évaluations des risques et adoptent une approche coordonnée fondée sur le risque pour les activités de BC/FT/FP.

Le GAFI s'attend à ce que les pays mettent en œuvre des mesures de prévention pour les PSAV similaires à celles imposées aux institutions financières traditionnelles, y compris une supervision appropriée du secteur ainsi que des exigences en matière de licence ou d'immatriculation. Bien que les Recommandations du GAFI visent les pays membres et non pas les PSAV en tant que tels, la mise en œuvre nationale des Recommandations et des Orientations exige de plus en plus que les PSAV s'y conforment, et ce phénomène devrait s'accroître. Les PSAV ont l'occasion à présent de comprendre ce qui est demandé au secteur et de s'y conformer de manière proactive si leur pays n'a pas encore mis en œuvre les Recommandations.

La Recommandation 16 du GAFI sur les virements électroniques est très souvent évoquée, qui conseille aux PSAV de traiter toutes les transactions afférentes à des AV comme des transferts transfrontaliers, compte tenu de la nature sans frontières de la technologie.[30] Cela nécessiterait de partager les informations entre les PSAV à un degré inattendu, y compris détenir et envoyer aux autres PSAV impliqués dans une transaction aussi bien des informations sur le donneur d'ordre que sur le bénéficiaire. Diverses organisations publiques et privées recherchent actuellement des solutions technologiques en ce qui a trait à la Recommandation 16.[31]

Les PSAV doivent viser une conformité proactive et concentrer leurs efforts sur une approche fondée sur le risque, afin d'atténuer de manière efficace les menaces en provenance des pays proliférateurs qui tentent d'exploiter le système pour leur propre gain.

Alors que les orientations du GAFI sont en passe d'être modifiées pour inclure le FP, les PSAV devraient se montrer particulièrement vigilants à l'égard de ces types d'acteurs. Les études de cas continuent d'indiquer une utilisation à grande échelle des AV pour contourner les sanctions, et d'autres encore seront sans doute médiatisées à l'avenir. Afin d'atténuer aussi bien le risque commercial que les risques internationaux et géopolitiques de ces actions, les PSAV devraient mettre en œuvre le niveau de conformité le plus élevé possible, comme cela est décrit dans les présentes orientations et les lectures recommandées afférentes (voir annexe II).

---

30. GAFI, « Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération : Les Recommandations du GAFI », p. 77.
31. Voir, par exemple, Ian Allison, « US Crypto Giants Build First Version of FATF-Compliant "Travel Rule" Tool », CoinDesk, 25 juin 2021, <https://www.coindesk.com/us-crypto-giants-build-first-version-of-fatf-compliant-travel-rule-tool>, consulté le 24 août 2021.

Annexe I : Liste de Contrôle

La liste de contrôle ci-dessous résume le contenu du présent document d'orientation. Pour en savoir plus sur l'une quelconque des mesures qui y sont évoquées, veuillez consulter la section correspondante.

Prérequis

- □ Le prestataire de services d'actifs virtuels (PSAV) dispose de sa propre structure de gouvernance et d'une équipe chargée de la conformité.
    - o La haute direction supervise et est chargée de la mise en œuvre du programme de lutte contre la criminalité financière.
    - o L'équipe inclut un Responsable de la conformité.
    - o Si applicable, l'équipe inclut un Responsable du respect des sanctions.
    - o Les employés débutants ou de niveau intermédiaire sont informés des procédures de conformité pertinentes susceptibles de s'appliquer dans d'autres domaines de l'activité du PSAV.
    - o Le personnel suit régulièrement des formations sur les tendances et les typologies en matière de LBC/FT/FP.
- □ Le PSAV a mené au moins une évaluation des risques exhaustive et documentée au cours des deux dernières années.
    - o Le PSAV a mis en œuvre des exigences de contrôle clés pour certains domaines présentant un risque élevé au vu des résultats de l'évaluation des risques.
- □ Le PSAV dispose de protocoles efficaces en matière de cybersécurité.
    - o Le personnel participe régulièrement à des sessions de formation sur la cybersécurité.
    - o Une infrastructure informatique et de cybersécurité appropriée et complète est en place.
- □ Le PSAV a élaboré des exigences appropriées en matière de référencement des actifs.

Vérification des Sanctions et des Personnes Politiquement Exposées (PPE)

- □ Le PSAV effectue une vérification des sanctions concernant tous les clients.
- □ Le PSAV utilise tout le matériel disponible pour procéder à des vérifications exhaustives.

- Le PSAV respecte pleinement les listes de sanctions internationales et des États-Unis d'Amérique.
- Le PSAV vérifie la liste des acteurs inclus dans les rapports du Groupe d'experts des Nations unies.
- Le PSAV consulte les rapports de typologie des ONG et utilise la vérification des médias défavorables.

□ La vérification des sanctions et des PPE est permanente. Le PSAV vérifie les portefeuilles d'actifs virtuels (AV) avant les transactions et opère un contrôle permanent sur les transactions.

- La vérification est réalisée lors de la première vérification de l'identité.
- La vérification est effectuée pendant toute la durée de la relation avec le client.

Intégration du Client

□ Le PSAV a mis en place des processus de connaissance du client (KYC) exhaustifs.

- Les processus d'identification des clients requièrent, à minima, le nom du client, sa date de naissance, sa nationalité et son adresse.
- Les informations personnelles des clients sont vérifiées en utilisant des documents d'identification gouvernementaux officiels. Les adresses sont vérifiées en utilisant un document justificatif de l'adresse ou des moyens numériques appropriés.
- L'identification de l'entité juridique exige, à minima, la dénomination de l'entité, son immatriculation, son adresse, son statut, les informations d'identification de son personnel de direction clé et sa structure de propriété.
- es informations de l'entité juridique sont vérifiées en utilisant le numéro de l'entreprise, des documents d'immatriculation gouvernementaux pertinents et des registres.
- Des processus permanents de connaissance du client et de vigilance renforcée sont menés pour tous les propriétaires ou les personnes qui agissent pour le compte du client.
- Des mécanismes de connaissance du client additionnels sont envisagés ou mis en œuvre, y compris des « selfies » pris avec l'application et des appels vidéo, vérifiés par des « tests de vie ».

□ Le PSAV comprend parfaitement la nature et la finalité de la relation avec le client.

- Le client indique la fréquence escomptée des transactions.
- Le client indique la taille escomptée des transactions.

- Le client indique le volume escompté des transactions.

□ Le PSAV comprend, dans la mesure du possible, aussi bien la source que la destination de tous fonds transférés.

Contrôle et Vigilance Permanents vis-à-vis de la Clientèle

□ Tous les documents et informations soumis au PSAV lors de l'intégration du client sont tenus à jour pendant toute la durée de la relation.

□ Le PSAV a mis en place un système de contrôle des transactions manuel ou automatisé.

- Le PSAV utilise un système permettant une vérification exhaustive des sanctions.
- Le PSAV comprend les limitations du système en place.

□ Le PSAV a envisagé les avantages de la mise en œuvre d'une analyse de à grande échelle.

□ Le PSAV mène des processus de vigilance renforcée lorsqu'une transaction ou un compte apparaît comme présentant un risque élevé.

- Le PSAV comprend quand et comment mener un processus de vigilance renforcée.

Indicateurs de Risque Élevé et Signaux d'Alarme

□ Le PSAV gère les relations avec les mixeurs.

- Le PSAV dresse une liste améliorée de mixeurs connus et/ou de confiance et de services CoinJoin.
- Le PSAV n'autorise des rapports qu'avec les mixeurs de confiance sous certaines conditions .

Obligations de Signalement

- □ Le PSAV connaît et comprend les Recommandations du GAFI.
- □ Le PSAV connaît, comprend et respecte l'ensemble des règlementations nationales appropriées.
- □ Le PSAV connaît, comprend et respecte les exigences nationales en matière de déclaration.
- □ Le personnel a connaissance des modalités de signalement des transactions suspectes et des informations précises à transmettre au responsable interne concerné.
- □ La personne chargée du signalement sait précisément comment effectuer la déclaration auprès des autorités compétentes et comment améliorer la situation.
- □ Les dispositions pertinentes sont standardisées et définies en interne pour en faciliter la compréhension.

Annexe II : Lectures recommandées

Lignes Directrices sur les Actifs Virtuels et les Prestataires de Services d'Actifs Virtuels du GAFI

FATF-GAFI, « Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers » (Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels), juin 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

FATF-GAFI, « 12-Month Review: Virtual Assets and VASPs », juillet 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>.

FATF-GAFI, « Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs », juillet 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>.

FATF, « International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations »(Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération : les recommandations du GAFI), mise à jour de juin 2021.

Orientations sur l'Évaluation par les Prestataires de Services d'Actifs Virtuels des Risques liés au Financement de la Prolifération

Anagha Joshi, Emil Dall and Darya Dolzikova, « Guide to Conducting a National Proliferation Financing Risk Assessment », RUSI, mai 2019.

BitAML, « Cryptocompliance 101: Do You Need a Risk Assessment? In Crypto, the Answer Is Yes », 28 janvier 2019, <https://bitaml.com/2019/01/28/risk-assessment-crypto/>.

FATF-GAFI, « Guidance on Proliferation Financing Risk Assessment and Mitigation », juin 2021, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>.

Ministère de la Justice du Gouvernent du Grand-Duché de Luxembourg, « ML/TF Vertical Risk Assessment: Virtual Asset Service Providers », décembre 2020, <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf>.

Ministère de l'Intérieur du gouvernement de la Nouvelle-Zélande, « Financial Institutions Sector Risk Assessment », Part 19: Sector Risks – Virtual Asset Service Providers, décembre 2019, <https://static1.squarespace.com/static/5a77b9d390bade7aa2cf8692/t/600e144cc42d5b31a3ccc997/1611535442275/Financial-Institutions-SRA-2019.pdf>.

Indicateurs de Risque Élevé et Signaux d'Alarme

Chainalysis, « The Chainalysis 2021 Crypto Crime Report », mars 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

Elliptic, « Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield », mai 2021, <https://www.elliptic.co/hubfs/downloads/Elliptic_Sanctions-Compliance-In_Crypto.pdf>.

FATF-GAFI, « Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing », septembre 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>.

Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), « Money Laundering and Terrorist Financing Indicators – Virtual Currency Transactions » (Indicateurs de blanchiment d'argent et de financement du terrorisme – Opérations en monnaie virtuelle), décembre 2020, <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng>.

Département du Trésor des États-Unis d'Amérique, Financial Crimes Enforcement Network (FinCEN), « Advisory on Illicit Activity Involving Convertible Virtual Currency », 9 mai 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

Sources Additionnelles Concernant la Vérification des Sanctions

Ministère des Affaires étrangères et des sanctions commerciales du gouvernement australien, « Australia and Sanctions », <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.

Service européen pour l'action extérieure, « Consolidated List of Sanctions List », <https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions>.

Gouvernent du Canada, « Consolidated Canadian Autonomous Sanctions List » (Liste consolidée des sanctions autonomes canadiennes), <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>.

Ministère de l'Économie, du Commerce et de l'Industrie du Japon, « Sanctions List », <https://www.meti.go.jp/english/>.

Bureau chargé de la mise en œuvre des sanctions du Trésor de sa Majesté du Royaume-Uni (UK HM Treasury Office of Financial Sanctions Implementation », « Consolidated Sanctions List », <https://sanctionssearch.ofsi.hmtreasury.gov.uk/>.

Conseil de sécurité des Nations unies, « Liste récapitulative », <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

Conseil de sécurité des Nations unies, « Rapports du Groupe d'experts du Comité des sanctions 1718 (République populaire démocratique de Corée) », <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>.

Bureau de contrôle des avoirs étrangers des États-Unis d'Amérique (US Office of Foreign Assets Control), « Sanctions List Search », <https://sanctionssearch.ofac.treas.gov/>.