GAFI

RAPPORT DU GAFI

Actifs virtuels

Indicateurs d'alerte

de blanchiment de capitaux et de financement du terrorisme

Septembre 2020

Le Groupe d'action financière (GAFI) est un organisme intergouvernemental indépendant dont la mission consiste à élaborer et promouvoir des stratégies de protection du système financier mondial face au blanchiment de capitaux, au financement du terrorisme et au financement de la prolifération d'armes de destruction massive. Les Recommandations du GAFI se sont imposées comme les normes internationales en matière de lutte contre le blanchiment de capitaux (LBC) et de financement du terrorisme (LFT).

Pour obtenir des informations complémentaires sur le GAFI, veuillez consulter le site **www.fatf-gafi.org.**

Ce document et/ou toute carte qu'il pourrait contenir est/sont publié(e)s sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales et du nom d'un(e) quelconque territoire, ville ou région quelconque territoire, ville ou région.

Référence de citation :

GAFI (2020), *Actifs virtuels : Indicateurs d'alerte de blanchiment de capitaux et de financement du terrorisme* https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html l

Table des matières

Abréviations

CAR	Cryptomonnaies à anonymat renforcé
DVC	Devoir de vigilance relatif à la clientèle
EPNFD	Entreprises et professions non financières désignées
RND	Registraires de noms de domaine
GAFI	Groupe d'action financière
IF	Institutions financières
CRF	Cellules de renseignement financier
OPC	Offre au public de cyberjetons
KYC	Know-your-customer (Connaissance du client)
AEPP	Autorités d'enquête et de poursuite pénale
BC	Blanchiment de capitaux
DOS	Déclarations d'opérations suspectes
FT	Financement du terrorisme
AV	Actifs virtuels
PSAV	Prestataires de services d'actifs virtuels

Introduction

1. Les actifs virtuels (AV) et les services connexes ont le potentiel de stimuler l'innovation et l'efficacité financières. Cependant, leurs caractéristiques distinctes créent également de nouvelles opportunités pour les blanchisseurs de capitaux, les financiers des terroristes et d'autres criminels de blanchir leurs produits ou de financer leurs activités illicites. La possibilité de réaliser rapidement des opérations transfrontalières permet non seulement aux criminels d'acquérir, de déplacer et de stocker des actifs sous forme numérique, souvent en dehors du système financier réglementé, mais aussi de dissimuler l'origine ou la destination des fonds et d'empêcher les entités déclarantes d'identifier à temps une activité suspecte. Ces facteurs constituent autant d'obstacles à la détection et à l'investigation des activités criminelles par les autorités nationales.

2. En octobre 2018, le Groupe d'action financière (GAFI) a mis à jour ses normes afin de clarifier l'application des normes du GAFI en ce qui concerne les activités liées aux AV et les prestataires de services d'actifs virtuels (PSAV) dans le but, notamment, d'aider les pays à atténuer les risques de blanchiment de capitaux (BC) et de financement du terrorisme (FT) associés aux activités liées aux AV et à protéger l'intégrité du système financier mondial. En juin 2019, le GAFI a adopté la Note interprétative de la Recommandation 15 afin de mieux comprendre l'application des exigences du GAFI en ce qui concerne les activités ou opérations liées aux AV et les PSAV, notamment en ce qui concerne la déclaration des opérations suspectes.

3. Le GAFI a élaboré ce bref rapport sur les indicateurs d'alerte concernant le blanchiment de capitaux et le financement du terrorisme liés aux AV afin d'aider les entités déclarantes, (notamment les institutions financières (IF), les entreprises et professions non financières désignées (EPNFD) et les PSAV), quelle que soit leur catégorie, à identifier et à déclarer les activités potentielles de BC et de FT impliquant des AV. Ce rapport devrait également faciliter l'application par les entités déclarantes d'une approche fondée sur le risque pour leur devoir de vigilance relatif à la clientèle (DVC), qui exige de connaître l'identité des clients et des bénéficiaires effectifs, de comprendre la nature et l'objet de la relation d'affaires, et de comprendre la source des fonds.

4. Les agences opérationnelles, notamment les cellules de renseignement financier (CRF), les autorités d'enquête et de poursuite pénale (AEPP) et les procureurs pourront utiliser ce rapport à titre de référence pour analyser les déclarations d'opérations suspectes (DOS) ou améliorer la détection et la confiscation des AV impliqués dans un usage abusif et les enquêtes les concernant.

5. Les autorités de régulation financières, les EPNFD et les PSAV pourront trouver ces indicateurs utiles lors de la préparation des DOS et du suivi de la conformité des entités avec les contrôles de LBC/FT. Lorsqu'une entité déclarante dispose d'informations indiquant l'existence d'un ou de plusieurs indicateurs sans explication commerciale logique, mais qu'elle ne dépose pas de DOS malgré l'explication incohérente du client ou qu'elle ne demande pas d'éclaircissements sur l'opération, les autorités compétentes peuvent envisager de prendre contact avec l'entité déclarante en tenant compte du profil commercial de cette dernière.

Méthodologie et sources utilisées pour établir la liste des indicateurs d'alerte

6. Les indicateurs d'alerte inclus dans ce rapport sont basés sur plus d'une centaine d'études de cas fournies par les pays entre 2017 et 2020, sur les conclusions du *Rapport confidentiel du GAFI sur les enquêtes financières impliquant des actifs virtuels* (juin 2019) et du Rapport *Monnaies virtuelles : Définitions clés et risques potentiels en matière de LBC/FT* publié par le GAFI (juin 2014), ainsi que sur les informations relatives à l'utilisation abusive des AV disponibles dans le domaine public.

Tendances de l'utilisation des AV à des fins de BC/FT

La majorité des infractions liées aux AV concernent des infractions sous-jacentes ou des infractions de blanchiment de capitaux. Néanmoins, les criminels utilisent les AV pour se soustraire aux sanctions financières et pour collecter des fonds destinés à soutenir le terrorisme.

Les types d'infractions signalées par les pays comprennent le blanchiment de capitaux, la vente de substances contrôlées et d'autres articles illégaux (y compris les armes à feu), la fraude, l'évasion fiscale, les délits informatiques (par exemple les cyberattaques entraînant des vols), l'exploitation des enfants, la traite des êtres humains, l'évasion des sanctions et le financement du terrorisme. Parmi ces infractions, le type d'abus le plus courant est le trafic illicite de substances contrôlées, soit avec des ventes réalisées directement en AV, soit avec l'utilisation des AV dans le cadre d'une technique de virements successifs. La deuxième catégorie d'abus la plus courante est liée aux fraudes, aux escroqueries, aux logiciels rançonneurs et à l'extorsion. Plus récemment, les réseaux professionnels de BC ont commencé à exploiter les AV comme l'un de leurs moyens de transférer, de collecter ou de superposer des produits.

Source : Études de cas fournies par les pays entre 2017 et 2020

Questions à prendre en compte lors de la lecture de ce rapport

7. Ces indicateurs sont spécifiques à la nature des AV et aux activités financières qui y sont associées, et ne sont en aucun cas exhaustifs. Les activités suspectes impliquant l'utilisation d'AV peuvent également présenter des caractéristiques similaires à celles des activités de BC/FT impliquant l'utilisation de monnaie fiduciaire ou d'autres types d'actifs. Les entités déclarantes doivent donc tenir compte des risques posés par leurs clients, leurs produits et leurs opérations, ainsi que de la présence d'indicateurs de risque conventionnels. Les indicateurs de risque doivent toujours être considérés dans leur contexte.

8. Les signaux d'alerte indépendants tels que ceux énumérés ci-dessous peuvent être développés ou combinés avec des informations provenant d'agences opérationnelles, qui peuvent à leur tour être développées dans le cadre d'un

partenariat public-privé, dans un processus cyclique et évolutif qui prend en compte le risque et le contexte uniques d'un pays, d'un type de client, ou de l'entité déclarante elle-même. La simple présence d'un indicateur d'alerte ne constitue pas nécessairement un motif de suspicion de BC ou de FT, mais peut inciter à une surveillance et à un examen plus approfondis. Il est possible que le client soit finalement en mesure de fournir une explication pour justifier l'indicateur d'alerte et la finalité commerciale ou économique d'une opération financière.

9. Lors de l'évaluation d'une activité suspecte potentielle, les autorités compétentes, les IF, les EPNFD et les PSAV doivent avoir conscience du fait que certains indicateurs d'alerte sont plus facilement observables lors du suivi général des opérations, tandis que d'autres sont plus facilement observables lors de l'examen spécifique d'une opération financière. L'observation d'un ou de plusieurs indicateurs dépend des secteurs d'activité, des produits ou des services qu'un établissement ou un PSAV propose et de la manière dont il interagit avec ses clients. Lorsqu'un ou plusieurs indicateurs sont présents et que rien, ou presque, n'indique une finalité économique ou commerciale légitime, l'entité déclarante peut être plus susceptible de développer un soupçon de BC ou de FT.[1] Ces indicateurs ne doivent pas être les seuls facteurs pour déterminer si une DOS doit être déposée ou non. Les entités déclarantes doivent envisager de déposer une DOS si elles savent, soupçonnent ou ont des motifs raisonnables de penser qu'une opération de BC ou de FT a été commise.

Indicateurs d'alerte

10. Les sections qui suivent contiennent un ensemble d'indicateurs d'alerte pour signaler des activités suspectes liées à des AV ou d'éventuelles tentatives d'échapper à la détection des forces de l'ordre, tels qu'identifiées grâce à plus de cent études de cas recueillies depuis 2017 dans l'ensemble du réseau mondial du GAFI, à des analyses documentaires et à des recherches dans des sources du domaine public. Comme nous l'avons déjà vu, l'existence d'un seul indicateur n'est pas nécessairement témoin d'une activité criminelle. Souvent, c'est la présence de plusieurs indicateurs pour une opération financière sans explication commerciale logique qui éveille les soupçons d'une activité criminelle potentielle. La présence d'indicateurs doit inciter à approfondir le contrôle et l'examen et à procéder à un signalement le cas échéant.

Indicateurs d'alerte liés aux opérations financières

11. Si les AV ne sont pas encore très utilisées par le public, leur usage s'est répandu parmi les criminels. L'utilisation des AV à des fins de blanchiment de capitaux est apparue il y a plus de dix ans, mais ils deviennent de plus en plus courants dans le cadre des activités criminelles en général. Cette série d'indicateurs montre que les signaux d'alerte traditionnellement associés aux opérations financières mettant en jeu des moyens de paiement plus conventionnels restent pertinents pour détecter les activités illicites potentielles liées aux AV.

1 Bien qu'un certain nombre d'indicateurs d'alerte puisse s'appliquer à la fois au BC et au FT, comme les activités de collecte de fonds, le financement de combattants terroristes étrangers et l'achat d'armes (par exemple sur le darknet) à l'aide d'AV, nous encourageons le lectorat à consulter les sources qui ont trait au Rapport confidentiel du GAFI sur la détection du financement du terrorisme : les indicateurs de risque pertinents (juin 2016) (accès restreint aux membres du GAFI).

Taille et fréquence des opérations financières

- Fractionner les opérations d'AV (comme les échanges ou les virements) en petits montants, ou en montants inférieurs aux seuils d'enregistrement ou de déclaration, de manière similaire au fractionnement des opérations en espèces.
- Effectuer plusieurs opérations de grande valeur :
  - dans un court laps de temps, par exemple au cours d'une période de 24 heures ;
  - de manière échelonnée et régulière, sans qu'aucune autre opération ne soit enregistrée pendant une longue période, ce qui est particulièrement fréquent dans les cas de logiciels rançonneurs ;
  - vers un compte nouvellement créé ou vers un compte auparavant inactif.
- Transférer immédiatement des AV vers plusieurs PSAV, en particulier vers des PSAV enregistrés ou exploités dans un autre pays :
  - qui n'a aucun lien avec le lieu de résidence ou d'activité du client ;
  - dont la réglementation en matière de LBC/FT est inexistante ou insuffisante.
- Déposer des AV auprès d'une plateforme d'échange et, souvent, immédiatement :
  - retirer les AV sans autre activité d'échange vers d'autres AV, ce qui constitue une étape inutile et entraîne des commissions d'intervention ;
  - convertir les AV en plusieurs types d'AV, ce qui entraîne également des commissions d'intervention supplémentaires, mais sans explication commerciale logique (comme une diversification du portefeuille) ;
  - retirer les AV d'un PSAV immédiatement et les transférer vers un portefeuille privé. Cela transforme la plateforme d'échange/le PSAV en un service de mixage de BC.
- Accepter des fonds suspectés d'être volés ou frauduleux :
  - déposer des fonds à partir d'adresses d'AV qui ont été identifiées comme détenant des fonds volés, ou d'adresses d'AV qui sont liées à des détenteurs de fonds volés.

Étude de cas 1. Transferts multiples et immédiats d'un grand nombre d'AV vers des PSAV à l'étranger

Un PSAV local a transmis des DOS à la suite de soupçons concernant l'achat de grandes quantités d'AV par plusieurs individus et leur transfert immédiat vers des PSAV situés dans un pays étranger. Dans plusieurs cas, les individus partageaient la même adresse résidentielle et la plupart des adresses d'AV ont été consultées à partir de la même adresse IP, ce qui indique l'utilisation potentielle de passeurs de fonds

par des blanchisseurs de capitaux professionnels pour blanchir les produits illicites.

En outre, avant l'achat des AV par les passeurs de fonds, les fonds en monnaie fiduciaire avaient fait l'objet de virements successifs. Pour dissimuler l'origine des fonds, des espèces ont d'abord été déposées sur divers comptes auprès de différentes institutions financières dans le pays. Ces fonds ont ensuite été transférés sur divers comptes détenus au nom d'entités enregistrées dans le pays. Des paiements électroniques ont été effectués sur ces comptes pour des montants moindres. Ensuite, les fonds ont été transférés sur un autre groupe de comptes avant d'atteindre les comptes des passeurs de fonds détenus auprès des PSAV locaux. Des AV ont été immédiatement achetés et transférés vers des PSAV à l'étranger. Plus de 150 individus ont été impliqués dans cette affaire, responsables du transfert d'un total d'environ 108 352 900 USD (ou 11 960 BTC) vers plusieurs comptes d'AV détenus par deux PSAV à l'étranger.

Source : Afrique du Sud

Étude de cas 2. Plusieurs AV et plusieurs transferts vers des PSAV étrangers

Une plateforme d'échange d'AV locale a signalé qu'environ 400 millions de KRW (301 170 EUR) ont été volés à des victimes de phishing et ont finalement été échangés contre des AV dans le cadre d'une technique de virements successifs. La déclaration a été déclenchée en raison des multiples opérations de grande valeur transférées vers un PSAV étranger dans un seul portefeuille. Les fonds volés en monnaie fiduciaire ont d'abord été échangés contre trois types d'AV différents, puis déposés dans le portefeuille d'AV du suspect, détenu auprès d'un PSAV local. Le suspect a ensuite tenté de dissimuler la source des fonds en les transférant 55 fois sur 48 comptes distincts détenus chez différents PSAV locaux, puis sur un autre portefeuille d'AV situé à l'étranger.

Source : Corée du Sud

Indicateurs de signaux d'alerte liés aux schémas de transaction

12. Comme dans la section précédente, les signaux d'alerte ci-dessous illustrent comment l'utilisation abusive des AV à des fins de BC/FT peut être repérée par des schémas de transactions irréguliers, inhabituels ou peu courants.

Opérations concernant de nouveaux utilisateurs

- Effectuer un dépôt initial important pour ouvrir une nouvelle relation avec un PSAV, alors que le montant financé ne correspond pas au profil du client.

- Effectuer un dépôt initial important pour ouvrir une nouvelle relation avec un PSAV, financer la totalité du dépôt le premier jour de l'ouverture, et commencer à transférer le montant total ou une grande partie du montant le même jour ou le jour suivant, ou retirer la totalité du montant le jour suivant. Comme la plupart des AV ont une limite transactionnelle pour les dépôts, le blanchiment de montants importants peut également se faire par le biais d'opérations de gré à gré.[2]
- Un nouvel utilisateur tente de transférer la totalité du solde des AV, ou retire les AV et tente d'envoyer la totalité du solde à l'extérieur de la plateforme.

Étude de cas 3. Dépôt initial incompatible avec le profil du client

La présence des indicateurs suspects suivants a incité une IF (banque) à déposer une DOS auprès des autorités, ce qui a donné lieu à une enquête sur le blanchiment de capitaux :

- des opérations incompatibles avec le profil du titulaire du compte – au cours des deux premiers jours suivant la création d'un compte personnel pour un jeune individu, le compte a reçu des dépôts de nature commerciale de différentes personnes morales pour des montants importants ;
- les schémas de transaction – les fonds déposés ont été immédiatement transférés sur les comptes de plusieurs PSAV (en une journée) pour l'achat d'AV (Bitcoin) ;
- le profil du client – l'un des donneurs d'ordre était connu de la banque pour avoir été impliqué dans une affaire de fraude. La banque a également fourni aux autorités les adresses IP utilisées pour les services bancaires en ligne.

L'enquête a révélé que le titulaire du compte personnel semblait être un passeur de fonds recruté par les criminels sur une plateforme de médias sociaux pour les aider à recevoir les paiements réclamés pour des marchandises vendues en ligne. Cependant, ces fonds semblaient avoir été déposés par d'autres entreprises victimes et ne constituaient pas des paiements pour des marchandises. Les fonds déposés ont été immédiatement transférés du compte bancaire personnel par le biais de plusieurs paiements fractionnés vers un autre compte détenu par une société par actions en République tchèque, et ont été échangés contre des AV (Bitcoin) détenus chez plusieurs PSAV locaux. Ces PSAV ont ensuite été immédiatement retirés du compte. Outre le dépôt d'une DOS, la banque a également suspendu les transferts suspects, ce qui a permis la saisie ultérieure des fonds.

Le PSAV local a également remarqué des irrégularités dans les fonds reçus et a fourni des informations utiles à l'enquête. Ces informations comprenaient : les circonstances dans lesquelles les AV ont été achetées ; des informations sur l'opération et sur le DVC telles que l'adresse du portefeuille, la copie du document d'identification utilisé

2 Les opérations de gré à gré concernent les titres négociés pour des sociétés qui ne sont pas cotées sur une bourse officielle, par l'intermédiaire d'un réseau de courtiers.

frauduleusement pour l'achat, et le nom de l'acheteur présumé. Ces informations ont permis aux autorités de demander des renseignements supplémentaires aux banques (par exemple, des relevés bancaires).

Source : République tchèque

Opérations concernant tous les utilisateurs

- Effectuer des opérations impliquant l'utilisation de plusieurs AV ou de plusieurs comptes, sans explication commerciale logique.
- Effectuer des transferts fréquents au cours d'une certaine période (par exemple, un jour, une semaine, un mois, etc.) sur le même compte d'AV :
  - par plus d'une personne ;
  - à partir de la même adresse IP par une ou plusieurs personnes ;
  - concernant des montants importants.
- Recevoir des opérations provenant de nombreux portefeuilles sans lien entre eux pour des montants relativement faibles (accumulation de fonds), avec transfert ultérieur vers un autre portefeuille ou échange intégral contre des monnaies fiduciaires. Ces opérations effectuées par un certain nombre de comptes accumulateurs liés peuvent initialement utiliser des AV au lieu de la monnaie fiduciaire.
- Échanger des AV en monnaie fiduciaire, potentiellement à perte (par exemple, lorsque la valeur de l'AV fluctue, ou en raison de frais de commission anormalement élevés par rapport aux normes du secteur, et en particulier lorsque les opérations n'ont pas d'explication commerciale logique).
- Convertir une grande quantité de monnaie fiduciaire en AV, ou une grande quantité d'un type d'AV en d'autres types d'AV, sans explication commerciale logique.

Étude de cas 4. Transferts effectués de manière récurrente

Une IF locale (maison de titres) a déposé une DOS concernant des paiements non autorisés entre les comptes d'AV de son courtier et un ressortissant étranger. La maison de titres a signalé l'activité après avoir déterminé que le ressortissant étranger avait l'intention d'effectuer des transferts d'un montant total de 4,8 millions d'USD (deux opérations distinctes effectuées à six minutes d'intervalle le même jour), et a déposé une demande de compte d'exploitation auprès du courtier le jour ouvrable suivant. Le portefeuille n'était pas hébergé dans les îles Caïmans. La DOS a permis un échange d'informations fructueux avec les CRF étrangères et la restitution de la plupart des fonds à la victime, car la plateforme en ligne hébergée dans un pays étranger avait pu geler le compte du suspect avant que l'infraction n'ait été finalisée.

Source : Îles Caïmans

Indicateurs d'alerte liés à l'anonymat

13. Cette série d'indicateurs s'appuie sur les caractéristiques et les vulnérabilités inhérentes à la technologie sous-jacente des AV. Les diverses caractéristiques technologiques ci-dessous renforcent l'anonymat et ajoutent des obstacles à la détection des activités criminelles par les AEPP. Ces facteurs rendent les AV attrayants pour les criminels qui cherchent à déguiser ou à stocker leurs fonds. Néanmoins, la simple présence de ces caractéristiques dans une activité ne signifie pas automatiquement qu'il s'agit d'une opération illicite. Par exemple, l'utilisation d'un portefeuille matériel ou papier peut être légitime en tant que moyen de sécuriser les AV contre les vols. Encore une fois, la présence de ces indicateurs doit être considérée dans un contexte englobant d'autres caractéristiques du client et de la relation, ou d'une explication commerciale logique.

- Opérations effectuées par un client impliquant plus d'un type d'AV, malgré des commissions d'intervention supplémentaires, et en particulier les AV qui permettent de bénéficier d'un anonymat plus élevé, telles que les cryptomonnaies à anonymat renforcé (CAR) ou les *privacy coins*.
- Déplacer une AV qui fonctionne sur une *blockchain* publique et transparente, comme le Bitcoin, vers une plateforme d'échange centralisée et l'échanger immédiatement contre une CAR ou un *privacy coin*.
- Clients qui opèrent en tant que PSAV non enregistré/non licencié sur des sites d'échange entre pairs (P2P), en particulier lorsque l'on craint que les clients traitent d'énormes quantités de transferts d'AV pour le compte de leurs clients, et facturent à ces derniers des frais plus élevés que les services de transmission proposés par d'autres plateformes d'échange. Utilisation de comptes bancaires pour faciliter ces transactions P2P.
- Activité transactionnelle anormale (niveau et volume) d'AV encaissés sur des plateformes d'échange à partir de portefeuilles associés à une plateforme P2P, sans explication commerciale logique.
- AV transférés vers ou depuis des portefeuilles qui présentent des schémas d'activité antérieurs associés à l'utilisation de PSAV qui exploitent des services de mixage ou des plateformes P2P.
- Opérations faisant appel à des services de mixage, ce qui suggère une intention de dissimuler les flux de fonds illicites entre les adresses connues des portefeuilles et les places de marché du darknet.
- Fonds déposés ou retirés d'une adresse ou d'un portefeuille d'AV présentant des liens d'exposition directs et indirects avec des sources suspectes connues, notamment des places de marché du darknet, des services de mixage, des sites de jeu douteux, des activités illégales (par exemple, logiciels rançonneurs) et/ou des déclarations de vol.
- L'utilisation de portefeuilles décentralisés/non hébergés, matériels ou papier, pour faire passer les frontières aux AV.

- Utilisateurs qui accèdent à la plateforme du PSAV après avoir enregistré leurs noms de domaine Internet par l'intermédiaire de proxys ou en utilisant des registraires de noms de domaine (RND) qui suppriment ou caviardent les propriétaires des noms de domaine.
- Utilisateurs qui accèdent à la plateforme du PSAV en utilisant une adresse IP associée à un darknet ou à un autre logiciel similaire permettant une communication anonyme, y compris les messageries électroniques cryptées et les VPN. Opérations entre partenaires utilisant divers moyens de communication anonymes et cryptés (par exemple, forums, chats, applications mobiles, jeux en ligne, etc.) au lieu d'un PSAV.
- Un grand nombre de portefeuilles d'AV apparemment sans rapport contrôlés à partir de la même adresse IP (ou adresse MAC), ce qui peut impliquer l'utilisation de portefeuilles fictifs enregistrés au nom de différents utilisateurs afin de dissimuler leurs relations mutuelles.
- Utilisation d'AV dont la conception n'est pas suffisamment documentée, ou qui sont liés à une fraude possible ou à d'autres outils visant à mettre en œuvre des systèmes frauduleux, tels que les systèmes de Ponzi.
- Réception de fonds de la part de PSAV ou envoi de fonds à des PSAV dont les processus de DVC ou de connaissance du client (KYC) sont manifestement faibles ou inexistants.
- Utilisation des distributeurs automatiques d'AV :
    - malgré des commissions d'intervention plus élevés, et notamment des distributeurs couramment utilisés par les passeurs de fonds ou les victimes d'escroquerie ;
    - dans des lieux à risque élevé où les activités criminelles sont nombreuses.

  Une seule utilisation d'un distributeur automatique n'est pas suffisante en soi pour constituer un signal d'alerte, mais elle le devient si le distributeur se trouve dans une zone à risque élevé, ou s'il est utilisé pour de petites opérations répétées (ou si d'autres facteurs s'ajoutent).

Étude de cas 5. Utilisation d'une adresse IP associée à une place de marché du Darknet – Alpha Bay

AlphaBay, le plus grand marché criminel du darknet démantelé par les autorités en 2017, a été utilisé par des centaines de milliers de personnes pour acheter et vendre des substances illégales, des documents d'identification et des dispositifs d'accès volés et frauduleux, des produits contrefaits, des logiciels malveillants et d'autres outils de piratage informatique, des armes à feu et des produits chimiques toxiques sur une période de deux ans. Le site fonctionnait comme un service caché sur le réseau TOR afin de dissimuler l'emplacement de ses serveurs sous-jacents ainsi que l'identité de ses administrateurs, modérateurs et utilisateurs. Les vendeurs d'AlphaBay utilisaient un certain nombre de types d'AV différents et comptaient environ 200 000 utilisateurs, 40 000 vendeurs, 250 000 annonces et ont facilité plus d'un milliard d'USD d'opérations d'AV entre 2015 et 2017.

En juillet 2017, le gouvernement américain, avec l'aide d'homologues étrangers, a mis hors service les serveurs hébergeant la place de marché AlphaBay, a arrêté l'administrateur et, en vertu d'un mandat de saisie délivré dans le Eastern District de Californie, a saisi les actifs physiques et virtuels de la place de marché elle-même, ainsi que ceux qui représentaient les produits illicites de l'entreprise criminelle AlphaBay. Les agents fédéraux ont obtenu les mandats après avoir retracé les opérations d'AV provenant d'AlphaBay vers d'autres comptes d'AV et identifié les comptes bancaires et autres actifs tangibles contrôlés par l'administrateur présumé.

Source : États-Unis

Étude de cas 6. Utilisation du mixage – Helix

Helix, un PSAV situé sur le darknet, a fourni un service de mixage qui aidait les clients à dissimuler la source ou les propriétaires des AV, moyennant une rémunération sur une période de trois ans. Helix aurait transféré plus de 350 000 bitcoins, d'une valeur de plus de 300 millions d'USD au moment de la transmission. L'opérateur présentait spécifiquement le service comme un moyen de dissimuler des opérations sur le darknet aux forces de l'ordre. En février 2020, des accusations criminelles ont été portées contre une personne qui exploitait Helix, notamment pour complot de blanchiment de capitaux et exploitation d'une entreprise de transfert de fonds sans licence.

Helix collaborait avec la place de marché du darknet AlphaBay jusqu'à la saisie de cette dernière par les forces de l'ordre en 2017.

Source : États-Unis

Étude de cas 7. Utilisation d'un portefeuille décentralisé

Cette affaire montre comment les criminels utilisent les portefeuilles décentralisés pour dissimuler la source des fonds illicites générés par les activités de trafic de stupéfiants. Dans cette affaire, les criminels ont effectué un grand nombre de ventes de drogue sur Internet et ont cherché à se faire payer non seulement en monnaie fiduciaire, mais aussi sous forme d'AV (Bitcoin, EX-codes, EXMO-chèques).

Les fonds illicites reçus en monnaie fiduciaire étaient convertis en AV à l'aide d'un compte anonyme sur une plateforme d'échange de Blockchain en ligne. Ces fonds, sous forme d'AV, étaient ensuite reconvertis en monnaie fiduciaire via un échangeur, avant d'être retransférés sur les comptes de cartes bancaires personnels des criminels. Quant aux fonds illicites reçus sous forme d'AV, ils ont d'abord été transférés vers des portefeuilles bitcoins décentralisés détenus par les criminels concernés, avant d'être transférés vers d'autres portefeuilles bitcoins sur différentes plateformes d'échange. Cela accroît la difficulté de tracer et de suivre les fonds. De même, les fonds blanchis (en AV) ont ensuite été reconvertis en monnaie fiduciaire avant d'être crédités sur les comptes de cartes bancaires des criminels. Le criminel a été reconnu coupable et condamné à sept ans d'emprisonnement et à une amende pénale à l'issue du procès.

Source : Fédération de Russie

Indicateurs d'alerte concernant les expéditeurs ou les destinataires

14. Cette série d'indicateurs concerne le profil et le comportement inhabituel de l'expéditeur ou du destinataire des opérations illicites.

Irrégularités observées lors de la création d'un compte

- Création de comptes séparés sous des noms différents afin de contourner les restrictions sur les opérations ou les limites de retrait imposées par les PSAV.
- Opérations initiées à partir d'adresses IP non fiables, d'adresses IP provenant de pays sanctionnés ou d'adresses IP précédemment signalées comme suspectes.
- Fréquentes tentatives d'ouverture de compte dans le même PSAV à partir de la même adresse IP.
- En ce qui concerne les commerçants/utilisateurs professionnels, leurs enregistrements de domaines Internet se font dans un pays différent de leur pays d'établissement ou dans un pays où la procédure d'enregistrement de domaines est insuffisante.

Irrégularités observées au cours du processus de DVC

- Informations KYC incomplètes ou insuffisantes, ou refus par le client de répondre aux demandes de documents KYC ou aux demandes de renseignements sur l'origine des fonds.

- L'expéditeur ou le destinataire n'a pas connaissance de l'opération, de la source des fonds ou de la relation avec la contrepartie, ou a fourni des informations inexactes à ce sujet.
- Le client a fourni des documents falsifiés ou a modifié des photographies et/ou des documents d'identification dans le cadre du processus d'intégration.

Étude de cas 8. Refus du client de fournir des informations sur l'origine des fonds

Une IF (banque) a déposé une DOS concernant le compte d'une entreprise locale qui détenait des fonds générés par la vente de bons d'achat pouvant être échangés contre un produit (en l'occurrence, des bioplastiques). Les fonds étaient déposés à la fois par des personnes physiques et morales, certains étant à l'origine des AV. Malgré les demandes de renseignements complémentaires de la banque, les représentants du titulaire du compte n'ont pas fourni d'informations sur l'origine des fonds. L'analyse qui s'en est suivie par les autorités a indiqué que les fonds envoyés par la société présentaient des liens avec des personnes liées au crime organisé et avec des fonds reçus dans le cadre d'un projet frauduleux.

Source : Italie

Profil

- Le client fournit des informations d'identification ou des références de compte (par exemple une adresse IP non standard ou des cookies flash) partagées par un autre compte.
- Des divergences existent entre les adresses IP associées au profil du client et les adresses IP à partir desquelles les opérations sont initiées.
- L'adresse d'AV du client apparaît sur des forums publics associés à des activités illégales.
- Le client est connu des forces de l'ordre par le biais d'informations accessibles au public en raison d'une association criminelle antérieure.

Étude de cas 9. Le profil du client ne correspond pas aux opérations régulières d'AV de grande valeur

Un PSAV (échangeur) et un IF (établissement de paiement) ont déposé des DOS auprès de la CRF concernant des opérations d'AV à valeur élevée qui ont commencé dès l'ouverture du compte auprès de l'échangeur. Plus précisément, le titulaire du compte avait effectué diverses opérations d'achat et de vente d'AV pour un montant supérieur à 180 000 EUR, ce qui ne correspondait pas au profil du titulaire du compte (dont sa profession et son salaire).

L'analyse a révélé que les AV ont ensuite été utilisées pour (i) des opérations sur un marché du darknet ; (ii) des jeux en ligne ; (iii) des opérations avec des PSAV qui n'étaient pas soumises à des contrôles adéquats en matière de LBC/FT ou qui faisaient l'objet d'enquêtes antérieures sur le blanchiment de capitaux portant sur des millions de dollars ; (iv) des opérations sur des plateformes qui proposaient des transactions d'AV P2P ; et (v) des services de mixage. Le titulaire du compte avait également utilisé divers de moyens (par exemple, transfert d'argent, banque en ligne et cartes prépayées) pour faire sortir un montant important de fonds de son compte dans le même laps de temps. Les fonds reçus par le titulaire du compte semblaient provenir d'un réseau de personnes qui achetaient des AV (bitcoins) en espèces et étaient situées dans différents pays en Asie et en Europe (dont l'Italie), à la fois par transfert d'argent et par le biais du système bancaire. Il recevait également des fonds sur ses cartes prépayées de la part de sujets en Afrique et au Moyen-Orient, qui à leur tour collectaient des fonds auprès de concitoyens résidant en Italie et à l'étranger. Ces fonds étaient ensuite utilisés pour des virements transfrontaliers et des jeux d'argent en ligne, et étaient retirés en espèces à partir de distributeurs automatiques de billets en Italie.

Source : Italie

Profil des passeurs de fonds potentiels ou des victimes d'escroquerie

- Un expéditeur qui ne semble pas bien au fait de la technologie des AV ou des solutions de portefeuilles de dépôt en ligne. Ces personnes peuvent être des passeurs de fonds recrutés par des blanchisseurs de capitaux professionnels, ou des victimes d'escroquerie forcées de devenir passeuses de fonds, qui transfèrent des produits illicites sans en connaître l'origine.
- Un client nettement plus âgé que l'âge moyen des utilisateurs de la plateforme qui ouvre un compte et effectue un grand nombre d'opérations, ce qui laisse supposer qu'il pourrait être un passeur de fonds ou une victime de l'exploitation financière des personnes âgées.
- Un client identifié comme personne financièrement vulnérable, souvent utilisée par les trafiquants de drogue pour les aider dans leurs affaires illicites.
- Un client qui achète de grandes quantités d'AV qui ne sont pas justifiées par le patrimoine disponible ou qui ne correspondent pas à son profil financier historique, ce qui peut indiquer qu'il s'agit de blanchiment de capitaux, ou que la personne est passeuse de fonds ou victime d'escroquerie.

Étude de cas 10. Des victimes d'escroquerie qui deviennent des passeurs de fonds

Dans ces escroqueries à l'investissement, des ressortissants étrangers ont contacté des retraités et généralement des personnes âgées par téléphone, par e-mail ou par le biais des médias sociaux, et leur ont proposé des opportunités d'investissement dans le bitcoin ou d'autres

AV avec la promesse de générer d'énormes profits en raison de la popularité croissante des AV et de l'augmentation de leur prix. L'investissement initial, d'un faible montant (dans de nombreux cas, pas plus de 250 euros), était prélevé sur le compte bancaire des victimes, sur leur carte de crédit ou par d'autres moyens auprès de divers services de paiement, avant de se retrouver entre les mains des criminels. Dans d'autres cas, les victimes étaient invitées à échanger de la monnaie fiduciaire contre des bitcoins en utilisant un distributeur automatique de billets et à envoyer les fonds à une adresse communiquée par les criminels.

Les victimes n'étaient pas très expertes en technologie et ne comprenaient généralement pas la technologie de l'AV ni ce dans quoi elles investissaient réellement. Les criminels demandaient également aux victimes d'installer une application de bureau à distance sur leur appareil afin que les criminels puissent les aider à transférer correctement les fonds sur des comptes spécifiques. Cela compromettait les appareils des victimes et permettait aux criminels d'effectuer des transferts de fonds non autorisés sans que la victime s'en aperçoive, jusqu'à ce qu'elle remarque que de l'argent manquait sur son compte. Dans certains cas, les criminels ont également fabriqué des articles prétendant que des célébrités, des hommes d'affaires fortunés ou des présentateurs de journaux télévisés faisaient la promotion des investissements dans les AV, donnant ainsi aux victimes un sentiment de confiance et de légitimité à l'égard de ces « investissements ».

Source : Finlande

Autres comportements inhabituels

- Un client modifie fréquemment ses informations d'identification, y compris ses adresses électroniques, ses adresses IP ou ses informations financières, ce qui peut également indiquer que quelqu'un d'autre a pris le contrôle du compte du client.
- Un client tente plusieurs fois d'entrer dans un ou plusieurs PSAV à partir de différentes adresses IP, au cours d'une même journée.
- Utilisation, dans les champs de texte des AV, d'un langage indiquant que les opérations sont effectuées pour soutenir une activité illicite ou pour acheter des biens illicites, tels que des stupéfiants ou des informations de cartes de crédit volées.
- Un client effectue de manière répétée des opérations avec un sous-ensemble d'individus en réalisant des profits ou des pertes importants. Cela peut indiquer une prise de contrôle potentielle du compte et une tentative d'extraction des soldes de la victime par le biais d'échanges, ou un stratagème de blanchiment de capitaux visant à brouiller les flux de fonds au moyen d'une infrastructure de PSAV.

Indicateurs d'alerte en lien avec la source des fonds

15. Comme le montrent les cas soumis par les pays, l'utilisation abusive des AV est souvent liée à des activités criminelles, telles que le trafic de stupéfiants et de substances psychotropes, la fraude, le vol et l'extorsion (y compris la cybercriminalité). Vous trouverez ci-dessous les signaux d'alerte les plus courants concernant la source des fonds ou des richesses liés à ces activités criminelles :

- Opérations avec des adresses d'AV ou des cartes bancaires liées à des systèmes connus de fraude, d'extorsion ou de logiciels rançonneurs, à des adresses sanctionnées, à des places de marché du darknet ou à d'autres sites web illicites.
- Opérations d'AV en provenance ou à destination de services de jeux d'argent en ligne.
- Utilisation d'une ou de plusieurs cartes de crédit et/ou de débit liées à un portefeuille d'AV pour retirer de grandes quantités de monnaie fiduciaire (cryptomonnaie vers monnaie plastique), ou le fait que les fonds pour l'achat d'AV proviennent de dépôts en espèces sur des cartes de crédit.
- Dépôts nettement plus élevés que les dépôts ordinaires sur un compte ou à une adresse d'AV, avec une source de fonds inconnue, suivis d'une conversion en monnaie fiduciaire, ce qui peut indiquer un vol de fonds.
- Manque de transparence ou informations insuffisantes sur l'origine et les propriétaires des fonds, par exemple : utilisation de sociétés écrans ; le placement de fonds dans une offre au public de cyberjetons (ICO) où les données personnelles des investisseurs ne sont pas disponibles ; la réception de fonds provenant d'un système de paiement en ligne par le biais de cartes de crédit ou de cartes prépayées suivies d'un retrait instantané.
- Fonds d'un client qui proviennent directement de services de mixage tiers.
- Majeure partie de la richesse d'un client qui provient d'investissements dans des AV, des ICO, des ICO frauduleuses, etc.
- Richesse d'un client qui provient de manière disproportionnée d'AV provenant d'autres PSAV qui n'ont pas de contrôles en matière de LBC/FT.

Étude de cas 11. Utilisation de sociétés écrans – Deep Dot Web

En mai 2019, les AEPP américaines ont saisi un site web, DeepDotWeb (DDW), en vertu d'une décision de justice. Les propriétaires et opérateurs présumés de DDW ont été inculpés dans le cadre d'un complot de blanchiment de capitaux lié à des millions de dollars de commissions occultes qu'ils ont reçues pour avoir orienté des personnes vers des places de marché du darknet à partir du site web de DDW. Grâce à des liens de renvoi, les propriétaires et exploitants présumés de DDW recevaient des commissions sur le produit de l'achat de marchandises illégales, telles que le fentanyl et l'héroïne, effectué par des personnes renvoyées vers une place de marché du darknet à partir du site de DDW.

Les paiements de ces rétrocommissions ont été effectués en AV et versés dans un portefeuille Bitcoin contrôlé par DDW. Pour dissimuler et

déguiser la nature et la source des produits illicites, qui s'élevaient au total à plus de 15 millions d'USD, les propriétaires et les opérateurs ont transféré leurs paiements illégaux de rétrocommissions du portefeuille Bitcoin de DDW vers d'autres portefeuilles Bitcoin, ainsi que vers des comptes bancaires qu'ils contrôlaient au nom de sociétés écrans. Les prévenus ont utilisé ces sociétés écrans pour transférer leurs gains illicites et mener d'autres activités liées à DDW. Au cours d'une période de cinq ans, le site web a reçu environ 8 155 bitcoins en paiements de commissions occultes de la part de places de marché du darknet, pour une valeur d'environ 8 millions d'USD, ajustée en fonction de la valeur de négociation du bitcoin au moment de chaque opération. Les bitcoins ont été transférés sur le portefeuille Bitcoin de DDW, contrôlé par les prévenus, en une série de plus de 40 000 dépôts, et ont ensuite été transférés vers diverses destinations au moyen de plus de 2 700 opérations. La valeur des bitcoins au moment des retraits du portefeuille Bitcoin de DDW s'élevait à environ 15 millions d'USD.

Source : États-Unis

Étude de cas 12. Utilisation de multiples plateformes d'échange d'AV, de faux documents d'identification pour le DVC et de cartes prépayées

Les prévenus dans cette affaire auraient mis en œuvre un système de blanchiment de capitaux en relation avec des cybercriminels qui ont piraté une plateforme d'échange d'AV et volé des AV d'une valeur de 250 millions d'USD. Les deux prévenus auraient blanchi environ 91 millions d'USD des AV volés, ainsi que 9,5 millions d'USD provenant d'un autre cybervol.

Les AV volés ont ensuite été acheminés par des centaines d'opérations automatisées d'AV et par de multiples plateformes d'échange d'AV. Les blanchisseurs ont utilisé des photographies trafiquées et des documents d'identification falsifiés dans certains cas pour contourner les procédures KYC dans les plateformes d'échange d'AV. Quelque 35 millions d'USD de fonds illicites ont finalement été transférés sur des comptes bancaires étrangers et ont également été utilisés pour acheter des cartes prépayées, qui pouvaient être échangées contre des AV. Les prévenus opéraient par l'intermédiaire de comptes indépendants ou liés et fournissaient à leurs clients des services de transmission d'AV, comme la conversion d'AV en monnaie fiduciaire, moyennant une rémunération. Les prévenus ont également exercé des activités aux États-Unis, mais ne se sont jamais enregistrés auprès du Financial Crimes Enforcement Network (FinCEN).

Source : États-Unis

Indicateurs d'alerte liés aux risques géographiques

16. Cette série d'indicateurs souligne la manière dont les criminels, lorsqu'ils déplacent leurs fonds illicites, tirent parti des différents stades de mise en œuvre, selon les pays, des normes révisées du GAFI en matière d'AV et de PSAV.[3] Selon les affaires signalées par les pays, les criminels ont exploité les lacunes des régimes de LBC/FT concernant les AV et les PSAV en déplaçant leurs fonds illicites vers des PSAV domiciliés ou opérant dans des pays où les réglementations de LBC/FT en matière d'AV et de PSAV sont inexistantes ou très réduites. Ces pays peuvent ne pas disposer d'un régime d'enregistrement ou d'autorisation, ou ne pas avoir étendu les exigences en matière de DOS aux AV et aux PSAV, ou encore ne pas avoir mis en place l'ensemble des mesures préventives exigées par les normes du GAFI. Bien que le présent rapport ne cherche pas à dresser une liste des pays « à haut risque », les entités déclarantes sont invitées à prendre en compte les indicateurs suivants lorsqu'elles examinent les risques géographiques. Ces risques sont associés aux pays d'origine, de destination et de transit d'une opération. Ils concernent également les risques associés au donneur d'ordre d'une opération et au bénéficiaire des fonds, qui peuvent être liés à un pays à haut risque. En outre, ils peuvent s'appliquer à la nationalité, à la résidence ou au lieu d'activité du client.

- Les fonds du client proviennent d'une plateforme d'échange ou sont envoyés vers une plateforme d'échange qui n'est pas enregistrée dans le pays où le client ou la plateforme sont situés.
- Le client utilise une plateforme d'échange d'AV ou un STFV situé à l'étranger dans un pays à haut risque qui ne dispose pas d'une réglementation adéquate suffisante en matière de LBC/FT pour les entités d'AV, et notamment dont les mesures en matière de DVC ou de KYC sont inadéquates.
- Le client envoie des fonds à des PSAV opérant dans des pays qui n'ont pas de réglementation en matière d'AV ou qui n'ont pas mis en place de contrôles en matière de LBC/FT.
- Le client établit des bureaux dans des pays qui n'ont pas de réglementation ou qui n'ont pas mis en œuvre de réglementation régissant les AV, ou transfère des bureaux dans des pays où aucune raison commerciale claire ne le justifie.

3 En juillet 2020, le GAFI a publié un examen à 12 mois des normes révisées du GAFI sur les actifs virtuels et les prestataires de services d'actifs virtuels. La section 2 du rapport couvre les progrès de la mise en œuvre des normes révisées depuis juin 2019.

Étude de cas 13. Trafiquant de bitcoins exploitant des entreprises de transmission de fonds non agréées (éléments transfrontaliers)

En avril 2019, le prévenu a été condamné à une peine de deux ans de prison pour avoir exploité une entreprise de transmission de fonds sans licence après avoir vendu des centaines de milliers de dollars d'AV (Bitcoin) à plus d'un millier de clients aux États-Unis. Le prévenu a également été condamné à la confiscation de 823 357 USD de ses bénéfices.

Le prévenu faisait de la publicité pour ses services sur des sites web destinés aux utilisateurs d'AV, et a rencontré certains clients en personne pour accepter de l'argent liquide en échange d'AV. D'autres clients le payaient par l'intermédiaire de guichets automatiques ou de services de transmission de fonds. Le prévenu recevait une prime de 5 % sur le taux de change en vigueur pour ses services. Il a d'abord acquis des bitcoins par l'intermédiaire d'une plateforme d'échange américaine, mais lorsque ses activités ont éveillé les soupçons et que son compte a été fermé, il s'est tourné vers une plateforme d'échange asiatique. Par le biais de cette plateforme, le prévenu a acheté pour 3,29 millions d'USD de bitcoins, au moyen de centaines d'opérations distinctes, entre mars 2015 et avril 2017. Le prévenu a également admis avoir échangé ses liquidités américaines, qu'il conservait dans un autre pays limitrophe des États-Unis, avec un négociant en métaux précieux, et qu'entre fin 2016 et début 2018, lui et d'autres personnes ont importé aux États-Unis un total de plus d'un million d'USD, pour des montants légèrement inférieurs à l'obligation de déclaration de 10 000 USD.

Source : États-Unis

Un PSAV transfère ses activités dans un pays dont la réglementation en matière de LBC/FT est inadéquate

Avant la mise en œuvre d'une politique visant à interdire les opérations des PSAV dans le pays A en Asie en 2017, un PSAV (plateforme d'échange) établi dans le pays A a transféré ses opérations au pays B dans la même région. En 2018, le pays B a renforcé son régime juridique de LBC/FT en matière d'AV à la suite de piratages importants de certains grands PSAV (plateformes d'échange). En mars 2018, le PSAV a annoncé son intention de transférer son siège dans le pays C en Europe (pays qui n'avait pas encore introduit de régime complet de LBC/FT en matière d'AV et de PSAV à l'époque). Plus tard, en novembre 2018, le pays C a introduit certaines réglementations sur les PSAV et, en février 2020, elle a confirmé qu'aucune autorisation n'avait été donnée au PSAV en question pour mener ses activités. Des rapports plus récents datant de 2020 indiquaient que le PSAV avait déjà transféré son statut et son domicile dans le pays D en Afrique.

Source : Domaine public

Conclusion

17. Le présent rapport s'appuie sur les nombreuses contributions des membres du GAFI dans l'ensemble du réseau mondial et vise à fournir un outil pratique aux secteurs public et privé pour identifier, détecter et prévenir les activités criminelles, de blanchiment de capitaux et de financement du terrorisme impliquant des AV.

18. Les indicateurs inclus dans ce rapport sont spécifiques aux caractéristiques et vulnérabilités inhérentes aux AV. Ils ne sont ni exhaustifs ni applicables à toutes les situations. Les indicateurs ne sont souvent qu'un des nombreux éléments contribuant à une image globale plus large du risque potentiel de BC ou de FT et il est important que ces indicateurs (ou tout indicateur unique) ne soient pas considérés de manière isolée. Ils doivent être mis en contexte avec les informations obtenues auprès des autorités compétentes.

19. Une approche fondée sur les risques, mise en œuvre dans le cadre d'un dialogue régulier et dynamique entre les secteurs public et privé, renforcerait très certainement l'efficacité du présent rapport. Les autorités compétentes sont donc encouragées à diffuser ce rapport auprès des entités déclarantes et à organiser des sessions d'engagement et de sensibilisation avec celles-ci afin de favoriser leur bonne compréhension de ce rapport.

20. Bien que les indicateurs identifiés soient en constante évolution, il est préférable de les utiliser en conjonction avec d'autres informations contextuelles provenant des forces de l'ordre nationales et de sources publiques. Les autorités compétentes peuvent également fournir au secteur privé les informations et les indicateurs les plus pertinents pour leur pays. Par exemple, elles peuvent utiliser les informations contenues dans le présent rapport pour préparer leurs propres avis à l'intention des entités déclarantes concernées. Toutefois, ce rapport ne doit pas être utilisé comme un outil réglementaire à des fins de conformité et d'examen, ou comme une liste de contrôle lors de la supervision d'institutions du secteur privé, car tous les indicateurs ne sont pas applicables à tous les pays ou à toutes les institutions.

Références

GAFI (juin 2014), Rapport du GAFI, Monnaies virtuelles : Définitions clés et risques potentiels en matière de LBC/FT

GAFI (juin 2019), Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels

GAFI (juin 2020), 12-month Review of Revised FATF Standards – Virtual Assets and VASPs (en anglais uniquement)

Rapports réservés aux membres du GAFI

GAFI (juin 2016), Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators (en anglais uniquement)

GAFI (juin 2019), Confidential FATF Report on Financial Investigations Involving Virtual Assets (en anglais uniquement)

www.fatf-gafi.org

Septembre 2020

Actifs virtuels - Indicateurs d'alerte de blanchiment de capitaux et de financement du terrorisme

Les actifs virtuels (AV) et les services connexes ont le potentiel de stimuler l'innovation et l'efficacité financières. Cependant, leurs caractéristiques distinctes créent également de nouvelles opportunités pour les blanchisseurs de capitaux, les financiers des terroristes et d'autres criminels de blanchir leurs produits ou de financer leurs activités illicites.