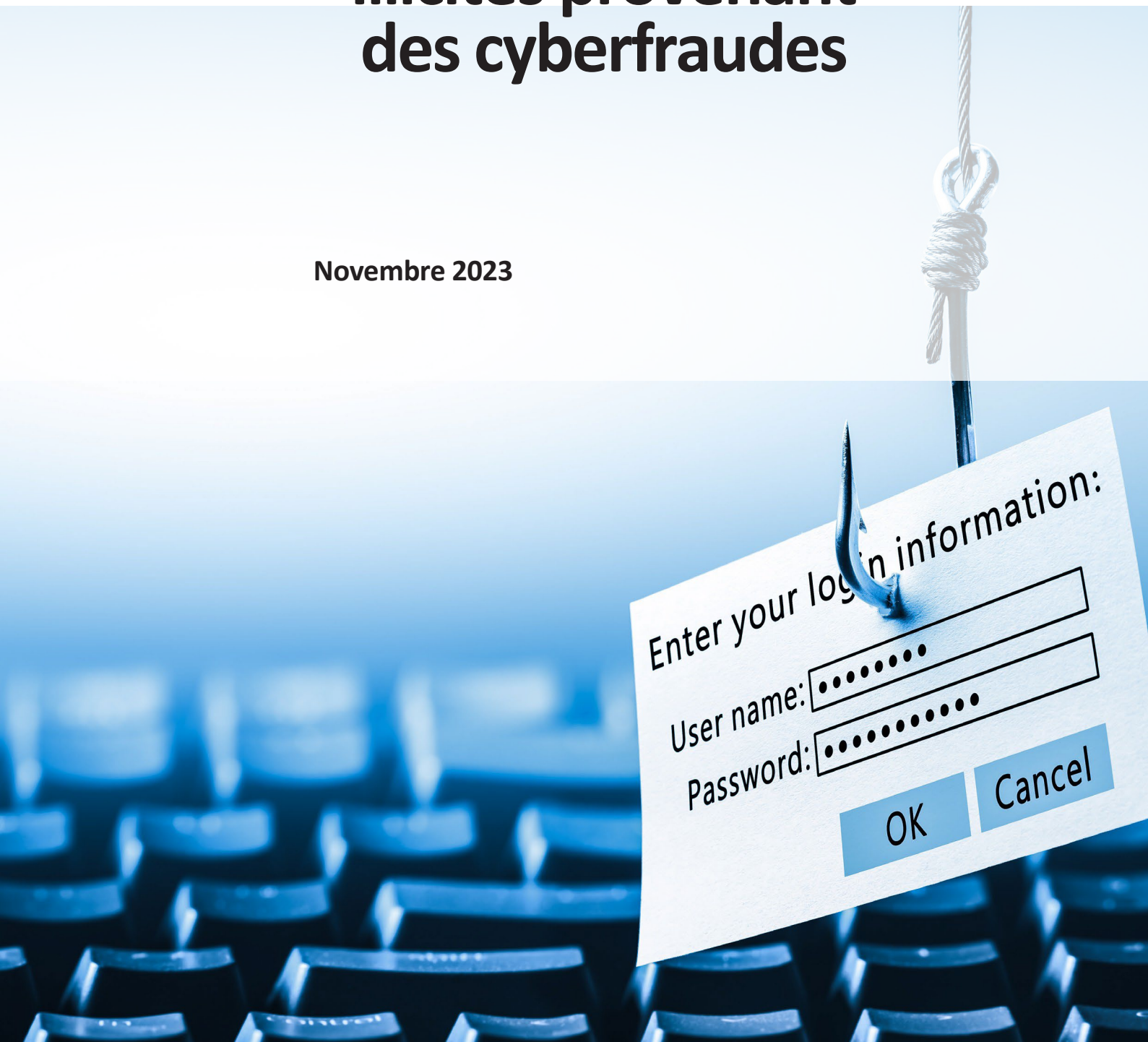
Flux financiers illicites provenant des cyberfraudes

Novembre 2023



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 des 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 le 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.

L'objectif du Groupe Egmont des cellules de renseignement financier (Groupe Egmont) est de fournir un forum aux cellules de renseignement financier (CRF) du monde entier afin d'améliorer la coopération dans la lutte contre le blanchiment d'argent et le financement du terrorisme et de favoriser la mise en œuvre de programmes nationaux dans ce domaine. Pour de plus amples renseignements concernant le Groupe Egmont, veuillez consulter le site Web : www.egmontgroup.org.

Le rôle d'INTERPOL est de permettre aux polices de ses 195 pays membres de travailler ensemble pour lutter contre la criminalité transnationale et rendre le monde plus sûr. L'organisation gère des bases de données mondiales contenant des informations de police relatives aux malfaiteurs et aux infractions; elle apporte également un appui opérationnel et un soutien en matière de police scientifique, fournit des services d'analyse et organise des formations. Ces capacités policières sont mises à disposition dans le monde entier et viennent à l'appui de quatre programmes mondiaux sur la criminalité financière et la corruption, l'antiterrorisme, la cybercriminalité et la criminalité organisée et les nouvelles formes de criminalité.

Référence :

GAFI – Interpol – Groupe Egmont (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, GAFI, Paris, France, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

Source de la photo sur la page couverture ©Getty Images

Table des matières

Liste des Acronymes

AV	Actif virtuel
BC	Blanchiment de capitaux
BCVC	Blanchiment de capitaux par voie commerciale
BEC	Compromission de messagerie d'entreprise
CDD	Diligence raisonnable à l'égard de la clientèle
CF	Cyberfraude
CRF	Cellule de renseignement financier
DOD	Déclaration d'opérations douteuses
EJ	Entraide juridique
EPNFD	Entreprises et professions non financières désignées
FSAV	Fournisseurs de services d'actifs virtuels
FT	Financement du terrorisme
GAB	Guichet automatique bancaire
IBAN	Numéro de compte bancaire international
IF	Institution financière
IP	Protocole Internet
LBC/LFT	Lutte contre le blanchiment de capitaux/lutte contre le financement du terrorisme
OAL	Organisme d'application de la loi
PPP	Partenariat public-privé
PSP	Prestataire de services de paiement
RPV	Réseau privé virtuel
vIBAN	Numéro de compte bancaire international virtuel
VoIP	Voix par protocole Internet

Sommaire

Les cyberfraudes (CF) sont une forme de criminalité transnationale organisée en plein essor. Les organisations criminelles responsables des CF sont souvent bien structurées et divisées en sous-groupes distincts associés à des domaines d'expertise criminelle spécialisés, y compris le blanchiment de capitaux. Ces sous-groupes peuvent aussi être peu structurés et décentralisés dans différentes administrations, ce qui complique davantage les efforts déployés pour enquêter sur les CF. Il apparaît également que les organisations responsables des CF sont souvent liées à d'autres types de criminalité, notamment la traite de personnes et le travail forcé dans des centres d'appel spécialisés dans les CF ainsi que le financement de la prolifération lié à des cyberactivités illicites de la République populaire démocratique de Corée (RPDC).

Des groupes qui s'adonnent au blanchiment d'argent et des promoteurs professionnels participent au processus de CF et de BC. Le réseau de comptes utilisés pour le BC comporte souvent des mules financières, mais peut aussi comprendre des sociétés fictives ou des entreprises honnêtes. Les réseaux de BC comprennent aussi différents types d'institutions financières (IF), notamment des banques, des fournisseurs de services de paiements et d'envoi ainsi que des fournisseurs de services d'actifs virtuels (FSAV). Pour dissimuler encore mieux la piste financière de leurs gains mal acquis, les criminels utilisent différentes techniques de BC, comme l'utilisation d'argent comptant, le blanchiment de capitaux par voie commerciale (BCVC) et des services non autorisés.

Avec l'aide de la numérisation, les technologies ont permis aux criminels responsables des CF de se perfectionner et d'accroître l'ampleur, la portée et la rapidité de leurs activités illicites. Ils utilisent divers outils et techniques pour tromper leurs victimes ou exploiter leur état psychologique et jouer sur les émotions pour leur extorquer le plus d'argent possible. Les organisations qui s'adonnent aux CF exploitent les innovations technologiques pour faciliter et accélérer le blanchiment des produits de leurs crimes. Les services virtuels, comme l'ouverture de comptes en ligne à distance, permet aussi aux criminels de créer facilement des comptes et de blanchir des produits à l'étranger, les transactions financières étant réalisées presque instantanément. Les criminels profitent des plateformes de médias sociaux et de messagerie pour recruter des mules financières au-delà des frontières à grande échelle. Les criminels sont aussi prompts à exploiter les vulnérabilités des nouvelles institutions financières et des produits financiers numériques ainsi que des secteurs non traditionnels comme le commerce électronique et les plateformes de médias sociaux et de diffusion en continu.

Les administrations doivent réagir plus efficacement. Elles doivent notamment :

- mettre en œuvre des initiatives visant à accroître les signalements par les victimes et à améliorer les déclarations d'opérations douteuses;
- analyser efficacement un grand volume de renseignements afin de lutter contre les CF;
- étant donné la nature transectorielle des CF, de solides mécanismes de coordination nationaux sont nécessaires pour combattre et prévenir, de façon globale, les CF et le BC connexe.

En général, les principales infractions liées aux CF ne sont pas réalisées au même endroit que le processus de BC. Les produits peuvent être blanchis rapidement grâce à un réseau de comptes, qui s'étend souvent à de nombreuses administrations et institutions financières. Une collaboration multilatérale entre les administrations est requise pour intercepter efficacement et rapidement les produits des CF qui sont

blanchis à l'étranger. Pour ce faire, les administrations doivent tirer profit des mécanismes multilatéraux existants (et futurs) (comme le projet I-GRIP d'INTERPOL et le projet BEC du Groupe Egmont) pour favoriser une collaboration et un échange de renseignements internationaux rapides pour lutter plus efficacement contre les CF. Finalement, le présent rapport comprend une liste d'indicateurs de risque, ainsi que les exigences et contrôles antifraude, qui peuvent être utiles pour que les entités des secteurs public et privé puissent détecter et prévenir les CF et le BC connexe.

1. Introduction

1. Les fraudes et les escroqueries en ligne dominent le milieu de la cybercriminalité. Si rien n'est fait, elles deviendront de plus en plus sophistiquées et représenteront une plus grande menace et un risque plus important à mesure qu'augmentera le nombre de groupes criminels organisés s'adonnant à ces activités illicites et profitant des occasions associées aux nouvelles technologies, comme l'intelligence artificielle générative[1].

2. Sous la présidence singapourienne, le GAFI a lancé une nouvelle initiative axée sur la lutte contre les flux financiers illicites provenant des cyberfraudes. Le présent rapport résulte d'un projet conjoint du Groupe Egmont, du GAFI et d'INTERPOL, le premier projet que ces trois organismes ont réalisé ensemble, et reflète un solide engagement collectif pour s'attaquer aux groupes criminels organisés et à leurs réseaux.

1.1. Objectifs et portée

3. Le présent rapport est axé sur le financement illicite lié à des activités frauduleuses qui sont réalisées ou facilitées dans le cyberenvironnement et qui (i) relèvent de la criminalité transnationale, comme des acteurs et des flux de fonds transnationaux et (ii) impliquent des techniques de fraude psychologique (comme la manipulation des victimes pour avoir accès à des renseignements personnels ou confidentiels). Reconnaissant les nombreuses variantes possibles de ces fraudes, le présent rapport se concentre sur les types d'activités criminelles ci-dessous (appelés collectivement les *cyberfraudes* [CF]).

   - **Fraude de compromission de messagerie d'entreprise (BEC) :** Les victimes reçoivent des instructions par courriel censées provenir de clients ou de fournisseurs et demandant aux victimes de transférer des fonds vers de nouveaux comptes de paiement.
   - **Fraude par hameçonnage :** Les victimes sont amenées à révéler des renseignements sensibles, comme des données personnelles, des renseignements bancaires ou des identifiants de connexion à des comptes. Le criminel utilise ensuite l'information pour détourner l'argent des victimes de leurs comptes de paiements, ouvrir de nouveaux comptes ou effectuer des opérations frauduleuses.
   - **Fraude par usurpation d'identité sur les médias sociaux et dans les télécommunications :** Elle comprend les cas où des victimes sont contactées par l'entremise d'applications mobiles ou de médias sociaux par des criminels qui prétendent être des représentants du gouvernement, des proches ou des amis et qui profitent des émotions des victimes pour leur soutirer de l'argent, pour prendre le contrôle de comptes de paiement ou pour effectuer des activités financières comme demander un prêt ou ouvrir un compte pour recevoir des produits de la criminalité.
   - **Fraude liée au commerce ou à des plateformes de négociation en ligne :** Les victimes sont induites en erreur par des publicités trompeuses ou des annonceurs fictifs en ligne qui les orientent vers des plateformes inexistantes

[1] Voir aussi le document du Fonds monétaire international (août 2023) *Fintech Note : Generative Artificial Intelligence in Finance: Risk Considerations* [en anglais seulement].

ou fausses (frauduleuses) pour effectuer des échanges ou des investissements impliquant des actifs fiduciaires et virtuels.

- **Fraude amoureuse en ligne :** Les victimes sont amenées à envoyer de l'argent à des criminels après avoir été convaincues de s'engager dans une relation amoureuse.
- **Fraude d'embauche :** Les fausses offres d'emploi sur des plateformes de médias sociaux incitent les victimes à payer des escrocs sous divers prétextes, y compris des paiements anticipés pour l'achat de marchandises afin de stimuler les ventes sur une plateforme de négociation ou une commission de garantie pour obtenir un emploi.

4. Le financement illicite lié aux rançongiciels et les autres crimes utilisant des maliciels ne seront pas abordés dans le présent rapport. Les lecteurs devraient consulter le rapport du GAF *Lutte contre le financement des rançongiciels* (mars 2023) pour de plus amples renseignements sur les rançongiciels et sur le blanchiment par l'entremise d'actifs virtuels (AV) et de fournisseurs de services d'actifs virtuels (FSAV) ainsi que sur les défis à relever et les bonnes pratiques à adopter pour atténuer les risques. Cette information est pertinente, puisque les AV et les FSAV sont souvent utilisés pour blanchir les produits des CF.

1.2. Objectifs et structure

5. Le présent rapport vise à améliorer la compréhension des risques associés à la menace que représentent les CF par les autorités compétentes. Le rapport met à profit des travaux existants déjà réalisés par le GAFI et d'autres organismes internationaux (y compris le Groupe Egmont, Europol et INTERPOL) et cherche à déterminer les nouveaux éléments et les progrès importants permettant de mieux comprendre les risques.

- **Les chapitres 2 et 3** du rapport traitent de l'environnement de risque opérationnel en lien avec les CF et fournissent de l'information sur les risques, les techniques et les tendances en ce qui a trait aux CF et au blanchiment de capitaux (BC) connexe, y compris les conséquences et les vulnérabilités associées à la numérisation et aux nouvelles technologies.
- **Les chapitres 4 et 5** du rapport indiquent les bonnes pratiques et les solutions opérationnelles qu'utilisent les administrations pour relever les défis afin de combattre et de perturber les CF et le BC connexe, y compris des mécanismes de collaboration internationale et de recouvrement des avoirs.

1.3. Méthodologie

6. Des spécialistes de Singapour (pour le compte du GAFI), de la CRF de Hong Kong (Chine) (pour le compte du Groupe Egmont) et d'INTERPOL ont codirigé ce projet. En outre, les administrations et les entités suivantes ont participé aux travaux à titre de membres de l'équipe de projet : l'Azerbaïdjan, le Brésil, la Belgique, le Canada, la Chine, le Conseil de l'Europe, la Commission européenne, Europol, l'Allemagne, le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (GIABA), l'Inde, l'Italie, Israël, le Japon, la Malaisie, le Mexique, le Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (MONEYVAL), le Pakistan, le Portugal, l'Arabie saoudite, le Togo, le Royaume-Uni et les États-Unis.

7. Les constatations du rapport sont fondées sur les éléments ci-dessous.

- Une revue de la documentation existante et des renseignements de source ouverte à ce sujet, ce qui comprend les données du Groupe Egmont et d'INTERPOL et leurs recherches.
- Une demande de renseignements au réseau mondial du GAFI et au Groupe Egmont provenant de plus de 200 pays et 170 CRF, respectivement, concernant les risques, les cadres et les stratégies d'application de la loi ainsi que les mécanismes de collaboration et de coordination nationaux et internationaux. Au total, l'équipe de projet a reçu des contributions de plus de 80 délégations.
- Les discussions et les points de vue échangés dans le cadre de la Réunion commune d'experts du GAFI (avril 2023) et du Forum consultatif du secteur privé (mai 2023), y compris un engagement ciblé avec le secteur privé.

2. Environnement de risque : Cyberfraude

2.1. Menace croissante du blanchiment de capitaux (BC)

8. Le nombre de CF a augmenté de façon considérable à l'échelle internationale. Bien qu'il n'existe pas d'estimation détaillée de l'ampleur et de la portée des CF dans le monde, de nombreuses administrations ont signalé une croissance constante dans les dernières années. Les produits illicites de la CF sont souvent transférés vers des administrations étrangères. Ces produits peuvent ensuite être blanchis davantage en utilisant les systèmes financiers d'une administration tierce.

9. Selon le Rapport de synthèse d'INTERPOL sur les tendances mondiales de la criminalité en 2022[2], les escroqueries en ligne sont un des cybercrimes les plus fréquemment perçus comme représentant une menace « élevée » ou « très élevée » à l'échelle internationale. La plupart des administrations qui ont fourni de l'information pour ce projet prennent en compte les risques du BC découlant de la CF dans leurs évaluations nationales des risques. Sans surprise, les régions qui utilisent très peu les espèces et qui sont très axées sur le numérique (p. ex. lorsque l'on effectue l'essentiel de l'intermédiation financière par l'entremise de services en ligne) sont plus vulnérables aux risques de BC associés à ce crime, même si la nature transnationale de la CF permet aux criminels de cibler facilement leurs victimes, sans égard pour les frontières internationales. L'encadré ci-dessous rassemble diverses sources d'information[3] pour dresser un portrait régional de la menace associée à la cyberfraude.

Encadré 1. Menaces accrues liées au BC : tendances régionales de la CF

Afrique : En Afrique, le secteur financier, qui a migré rapidement vers le numérique, a généré de multiples occasions pour les criminels de commettre des CF, causant ainsi une forte augmentation des fraudes bancaires en ligne, notamment de l'hameçonnage, du vol d'identité et des escroqueries virtuelles impliquant des actifs. La hausse des pertes financières dues à ces crimes constitue une menace accrue de BC. Par exemple, en Afrique occidentale, la CF serait considérée comme une source importante de revenus pour les organisations criminelles.

Amériques : La CF a été désignée comme représentant un risque à la hausse ou émergent. Une administration a indiqué comment les signalements de CF ont augmenté année après année et a souligné qu'il en est de même pour le risque de BC. Une autre a affirmé que les fraudes en matière d'investissement dans les actifs virtuels ont augmenté de plus de 180 % de 2021 à 2022 et que les criminels ont profité de l'engouement et de la publicité entourant les actifs virtuels.

[2] Voir INTERPOL (2022), *Rapport de synthèse d'INTERPOL sur les tendances mondiales de la criminalité en 2022*.
[3] Comprend les renseignements et les données fournis par les administrations ainsi que les rapports d'INTERPOL et Europol.

Asie-Pacifique : Des administrations ont associé la CF à un risque élevé ou important de BC. Par exemple, une administration a affirmé que la majorité des signalements de fraudes mentionnent une forme ou une autre de CF et qu'elle a observé une augmentation du BC lié aux CF. Une autre administration a souligné le rôle d'acteurs transnationaux pour escroquer les victimes au moyen d'une pléthore de demandes d'investissement illégales. La pandémie de COVID-19 a accéléré la numérisation des services et des comportements des simples citoyens, des gouvernements et des entreprises dans la région.

Par conséquent, la CF et le BC connexe ont augmenté et cette tendance devrait se poursuivre.

Caraïbes : La région est très vulnérable aux CF et au BC connexe, les fraudes générales liées aux CF ayant augmenté au cours des cinq dernières années. Le secteur des actifs virtuels en pleine croissance dans le bassin des Caraïbes favorise également les vulnérabilités, y compris en raison de la présence de fournisseurs de services d'actifs virtuels (FSAV), comme des mélangeurs, qui peuvent être utilisés de façon malveillante pour blanchir les fonds illégaux d'organisations criminelles, notamment en lien avec la CF.

Europe : On considère généralement que la CF est associée à un risque de BC. De nombreuses administrations ont remarqué une augmentation considérable du nombre de CF et elles sont perçues comme représentant une menace élevée. Les actifs virtuels (AV) servent fréquemment à blanchir les produits des CF (en particulier dans le cas des fraudes boursières en ligne liées aux AV, comme les premières émissions de cryptomonnaie frauduleuses).

Moyen-Orient et Afrique du Nord (MOAN) : Conformément aux tendances dans d'autres régions du monde, le MOAN a vu les taux de numérisation s'accélérer pendant la pandémie, à mesure que les gouvernements, les entreprises et les citoyens adoptaient massivement les activités en ligne. Les fraudes financières en ligne, y compris l'hameçonnage, la fraude par usurpation d'identité et les escroqueries en ligne, sont considérées comme des menaces élevées. La région du MOAN est aussi vulnérable au BC, puisque les pays membres du Conseil de coopération du Golfe (CCG), en particulier, servent de centres de transbordement pour les activités commerciales et financières mondiales.

10. La migration vers le numérique et la conception de nouvelles technologies servent de facteurs clés sous-tendant l'augmentation des CF. Les services numériques font désormais partie intégrante de notre vie quotidienne et des fonctions publiques. Par conséquent, davantage de citoyens (y compris les groupes vulnérables) prennent part aux activités en ligne. Parallèlement, la numérisation oblige les administrations à être de plus en plus connectées et favorise une circulation rapide des renseignements et des fonds au-delà des frontières. Ces deux facteurs ont essentiellement modifié le milieu criminel et créé un climat de menace accrue associé aux CF.

11. La pandémie de COVID-19 a accéléré la transition des activités financières en

personne vers l'ouverture de comptes, les paiements et les prêts en ligne. Les activités frauduleuses, comme les arnaques par téléphone ou courriel, les fraudes bancaires, aux dépens des personnes âgées et dans les soins de santé (p. ex. les fraudes liées à l'équipement de protection personnelle et à d'autres produits de santé) et les escroqueries en matière d'investissement frauduleuses ont grandement augmenté sur Internet avec l'utilisation des téléphones intelligents, des courriels et des médias sociaux. Ces nouveaux comportements financiers ont aussi eu une incidence sur le contexte du blanchiment d'argent, y compris l'utilisation accrue des plateformes bancaires et de paiement numériques ainsi que des opérations à distance (voir aussi la section « Impact de la numérisation et des nouvelles technologies » à la page 25)[4].

12. L'utilisation de plus en plus répandue des téléphones intelligents, des technologies (avec des outils et des applications en constante évolution) et des opérations financières à distance a considérablement augmenté la vulnérabilité des utilisateurs. Si l'on ajoute les technologies améliorant l'anonymat, comme les réseaux privés virtuels (RPV) et le routeur en oignon[5], il devient plus facile pour les criminels de préserver leur anonymat dans le cadre de leurs activités illicites. En mettant à profit les technologies, les criminels peuvent accroître l'ampleur, la portée et la rapidité de leurs activités criminelles. On observe aussi chez les criminels une augmentation de l'adoption d'un modèle de « crime en tant que service »[6], qui réduit aussi de façon importante les obstacles à l'entrée pour les organisations criminelles s'adonnant aux CF grâce à une spécialisation accrue de divers sous-groupes pour différents aspects de la CF (voir la section 2.2 ci-dessous)[7].

13. Dans bien des cas, les groupes criminels organisés se sont élargis ou ont adapté leurs activités pour prendre en compte la CF en utilisant des techniques existantes pour blanchir les autres sommes obtenues illégalement.

[4] Voir GAFI (mai 2020), *Blanchiment de capitaux et financement du terrorisme liés à la COVID-19 - Risques et réponses politiques* et (décembre 2020) *Update : COVID-19-Related Money Laundering and Terrorist Financing Risks* [en anglais seulement].
[5] Aussi appelé TOR (pour The Onion Router), il s'agit d'un logiciel ouvert permettant aux utilisateurs de naviguer sur Internet de façon anonyme.
[6] C'est à ce moment qu'est effectuée la division du travail, lorsque des organisations criminelles renforcent et offrent des capacités, des compétences et de l'expertise criminelles spécialisées à d'autres.
[7] Voir Europol (juillet 2023) *Internet Organised Crime Threat Assessment (IOCTA) 2023* [en anglais seulement] et INTERPOL (2022) *La criminalité financière et la cybercriminalité sont au cœur des préoccupations de la police à l'échelle mondiale, d'après un nouveau rapport d'INTERPOL*.

Encadré 2. Réseau de BC couramment utilisé pour les CF et d'autres crimes

Un réseau de BC offre des jeux de hasard en ligne et effectue des opérations de CF dans les installations de son entreprise dans la zone économique spéciale (ZES) du pays A. Le complexe héberge une dizaine d'entreprises qui offrent aussi des jeux de hasard en ligne et effectuent des opérations de CF ou louent leurs bureaux à d'autres pour qu'ils le fassent. Le réseau compte aussi des entreprises présumées légitimes dans les régions frontalières du pays voisin B. Le réseau est dirigé par des ressortissants du pays B qui utilisent des comptes bancaires dans la devise du pays B pour faciliter la circulation de l'argent entre la ZES et le pays C, où sont situés les principaux investisseurs de l'entreprise. Les dollars américains de la ZES sont blanchis au cours des échanges d'argent dans le pays B, où l'argent est converti dans la devise du pays B puis envoyé au pays C. Du côté de la frontière du pays C, l'argent est ensuite transféré aux investisseurs de l'entreprise.

Source : Transnational Organized Crime, Casinos and Money Laundering in Southeast Asia: A Threat Analysis (Office des Nations Unies contre la drogue et le crime, 2022) [en anglais seulement].

2.2. Caractéristiques des criminels qui s'adonnent à la CF

Éléments de la CF

14. D'après l'expérience des administrations, les criminels qui s'adonnent à la CF peuvent compter sur un ou plusieurs des éléments suivants pour inciter les victimes à effectuer un transfert frauduleux. Différentes variantes de la CF peuvent combiner ces éléments de différentes façons :

    - l'extraction d'information (p. ex. en utilisant l'hameçonnage);
    - la tromperie sociale ou la fraude psychologique et l'exploitation des émotions de personnes vulnérables (p. ex. en prétendant être une autre personne ou entité et en profitant de l'occasion pour susciter un sentiment d'urgence, de peur ou de confiance; ou en utilisant de fausses allégations pour soutirer de l'argent facilement);
    - un support ou une plateforme en ligne (qui peuvent être utilisés soit aux fins de communication ou pour amener des victimes à effectuer des opérations dans le cas de fraudes commerciales en ligne).

15. Une personne peut être victime de plus d'un type de CF; en fin de compte, l'objectif est d'obtenir un transfert de fonds et les criminels utilisent un éventail de techniques pour y arriver. Les criminels sont créatifs et peuvent utiliser ou adopter d'autres types de CF si la première tentative semble vouloir échouer. Par exemple, une victime d'hameçonnage ou d'usurpation d'identité sur les médias sociaux pourrait être convaincue et orientée vers un système de fraude en matière d'investissement par le même criminel en mettant à profit la relation de confiance déjà établie pour la fraude initiale.

Encadré 3. Mêmes victimes, multiples infractions

La pig butchering (abattage du cochon) est un mélange d'arnaque amoureuse et de fraude en matière d'investissement. Avec ce modus operandi, les criminels établissent une relation de confiance avec la victime et la convainquent d'investir ses économies dans des plateformes d'échange de cryptomonnaies frauduleuses. L'arnaque s'échelonne sur une certaine période, ce qui entraîne la perte d'une somme importante.

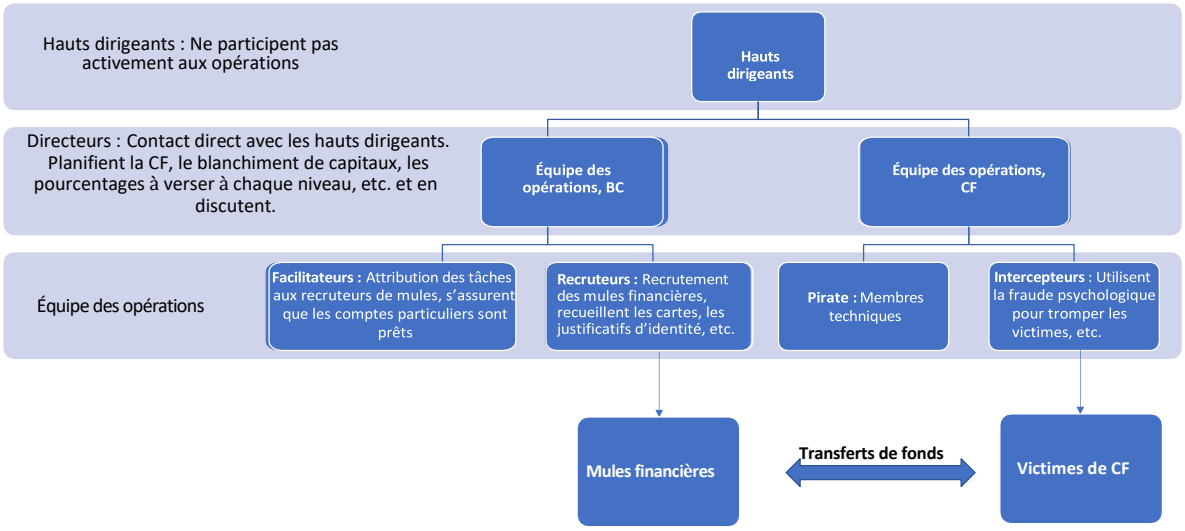
Après l'exécution de la fraude, les criminels communiquent souvent avec leurs victimes en affirmant être des avocats ou des agents des forces de l'ordre pour leur offrir de l'aide afin de retrouver leur argent en échange d'honoraires.

Structure d'une organisation criminelle

16. La CF et le BC connexe sont souvent l'œuvre d'organisations criminelles ou de syndicats du crime organisé transnationaux. Même si leur structure peut varier, les syndicats de la CF fonctionnent souvent comme des organisations hiérarchiques (voir l'exemple à la figure 1). Ils peuvent aussi être peu organisés afin de conserver leur souplesse, les membres pouvant se joindre au groupe et le quitter selon les besoins. Ces syndicats peuvent aussi être bien organisés en sous-groupes distincts ayant des domaines d'expertise criminelle spécialisés (p. ex. en lien avec les éléments de la CF susmentionnés [extraction d'information, tromperie sociale ou autre expertise technique comme la création d'une plateforme en ligne ou le BC]). Dans beaucoup de cas, ces syndicats de la CF sont décentralisés et n'ont jamais communiqué en personne (p. ex. ils utilisent des canaux chiffrés en ligne), ce qui complique la tâche des autorités qui doivent enquêter sur eux.

17. En outre, ces syndicats sont couramment composés de professionnels instruits et compétents sur le plan technique. Cette situation a donné lieu à la création d'une approche de plus en plus élaborée en matière de CF et de blanchiment des profits illicites. Des administrations ont souligné comment les syndicats de la CF peuvent recruter intentionnellement des personnes travaillant dans des secteurs professionnels (y compris des IF), qui peuvent être utilisées comme sources de données et de renseignements pour exécuter avec succès une CF et faciliter le BC. Pour de plus amples renseignements sur la structure des syndicats dans le domaine de la CF et leurs techniques pour blanchir des capitaux, consultez la section 2.3 ci-dessous.

Figure 1. Exemple de structure d'une organisation criminelle s'adonnant aux CF



Source : GAFI

Liens avec d'autres formes de criminalité

18. En plus du BC, les syndicats dans le domaine de la CF peuvent être liés à d'autres formes de criminalité. Les crimes courants englobent les activités connexes ou nécessaires pour effectuer la CF, y compris les activités de cybercriminalité comme le piratage pour obtenir des renseignements personnels, le développement et la vente de logiciels à des fins criminelles, la falsification de documents, etc. Une partie des produits de la criminalité peut être blanchie par les organisations qui s'adonnent à la CF en achetant du nouvel équipement et en concevant d'autres outils technologiques plus perfectionnés.

Encadré 4. Opération Falcon

Trois suspects ont été arrêtés à Lagos, au Nigéria, en 2020, après une enquête conjointe sur la cybercriminalité d'INTERPOL, de Group-IB et de la Force de police du Nigéria. Les ressortissants nigériens étaient réputés être membres d'un groupe criminel organisé plus vaste responsable d'envoi de maliciels, de campagnes d'hameçonnage et de vastes arnaques liées à la compromission de messagerie d'entreprise. Les suspects auraient mis au point des liens d'hameçonnage, des noms de domaines pour l'hameçonnage et des campagnes d'envoi massif de messages électroniques dans lesquels ils se faisaient passer pour des représentants d'organisations. Ils auraient ensuite utilisé ces campagnes pour diffuser 26 programmes de maliciels, de logiciels espions et d'outils de prise de contrôle à distance.

Ces programmes étaient utilisés pour infiltrer et surveiller les systèmes des organisations et des personnes victimes avant de lancer les escroqueries et de soutirer des fonds. Selon Group-IB, la bande organisée prolifique était soupçonnée d'avoir mis en péril des entreprises publiques et privées dans plus de 150 pays depuis 2017. Group-IB avait également pu établir que la bande était divisée en sous-groupes et qu'un certain nombre d'individus étaient toujours en liberté.

Des enquêtes sur le BC menées parallèlement ont révélé que les suspects ont aussi utilisé des comptes bancaires et d'AV étrangers au Royaume-Uni, aux États-Unis et en Thaïlande pour recevoir les paiements des victimes. Les trois suspects ont été inculpés pour leurs activités illégales, y compris pour fraude et blanchiment d'argent. Un véhicule de luxe a été saisi et les comptes des suspects ont été gelés et confisqués par le tribunal.

Source : Nigéria

19. Il y a aussi un lien de plus en plus évident entre la CF et la traite de personnes, dont les victimes sont attirées par de fausses offres d'emploi dans des centres d'appel en ligne et forcées de commettre des CF à l'échelle industrielle. Les syndicats de la CF peuvent ainsi accroître la diversité géographique des victimes qu'ils peuvent cibler en ligne (puisque les victimes de la traite de personnes peuvent être exploitées pour leurs connaissances des langues et leurs valeurs culturelles). Cette technique peut aussi renforcer la complexité des centres où sont réalisées les CF en exploitant des professionnels compétents, comme des travailleurs en technologies de l'information ou des « directeurs des ventes numériques »[8]. Parfois, ces centres d'appels sont exploités intentionnellement en tenant compte des fuseaux horaires des victimes ciblées et utilisent des immeubles locatifs pour effectuer des opérations criminelles temporaires, ce qui leur permet de déménager rapidement et de modifier leurs adresses IP pour éviter d'être découverts par les forces de l'ordre[9].

[8] Voir INTERPOL (juin 2023), *INTERPOL lance une alerte mondiale contre des escroqueries reposant sur la traite d'êtres humains*.

[9] Voir INTERPOL (juillet 2023), *Operational Analysis Online Scams and Human Trafficking in South East Asia / Update 2 – From Regional to Global Threat*, accessible uniquement aux forces de l'ordre nationales.

Encadré 5. Opération Storm Makers

Dans le cadre de l'opération Storm Makers, les autorités ont pris des mesures exécutoires contre des organisations criminelles organisées soupçonnées d'aider des hommes, des femmes et des enfants asiatiques à traverser les frontières aux fins d'exploitation ou pour le profit. L'opération a entraîné 121 arrestations dans 25 pays et a donné lieu à 193 nouvelles enquêtes.

Dans le cadre de l'opération Storm Makers, les corps policiers malaisiens et cambodgiens ont travaillé en étroite collaboration sur une affaire impliquant 15 hommes et une femme attirés au Cambodge par la promesse de se faire offrir un emploi bien payé dans un centre d'appels. À leur arrivée, ils ont été enfermés et forcés de travailler 14 heures par jours comme fraudeurs.

Remarque : Pour de plus amples renseignements, voir INTERPOL (mai 2022), *121 arrestations lors d'une opération contre le trafic de migrants et la traite d'êtres humains*

Source : INTERPOL

20. La plupart des administrations n'ont pas trouvé de preuves évidentes d'activités de financement du terrorisme liées aux CF. Toutefois, elles ont été témoins de certains cas où des éléments d'activités terroristes et de financement étaient associés à des criminels s'adonnant aux CF. Par exemple, des déclarations d'opérations douteuses (DOD) d'une administration laissent entendre qu'il y aurait eu des transferts de produits de CF vers des zones de conflits avérées ou des administrations reconnues pour leurs actes liés au terrorisme.

21. Des liens avec le financement de la prolifération et des cybercrimes ont aussi été signalés comme étant une source importante de revenus illicites pour la République populaire démocratique de Corée (RPDC). Parmi les cyberactivités illicites figurent la vente de renseignements personnels recueillis ou la fourniture d'outils et de services de piratage et d'hameçonnage, qui peuvent être utilisés par d'autres criminels pour commettre des CF[10].

[10] Voir aussi Conseil de sécurité des Nations Unies (mars 2023) *S/2023/171 Lettre datée du 3 mars 2023, adressée au Président du Conseil de sécurité par le Groupe d'experts créé en application de la résolution 1874 (2009)*.

Encadré 6. Utilisation d'outils d'hameçonnage en RPDC pour commettre des CF visant à financer des programmes d'armement

Selon les renseignements fournis au Groupe d'experts des Nations unies, des informaticiens de la République populaire démocratique de Corée liés au Département de l'industrie des munitions ont touché des devises étrangères en vendant des applications de piratage par hameçonnage vocal et en utilisant de multiples serveurs et adresses de protocole Internet à l'étranger.

En juillet 2020, quatre ressortissants de la RPDC ont été arrêtés par les autorités en Chine et extradés en RPDC. L'un d'entre eux a témoigné que des groupes criminels avaient acheté à un informaticien de la RPDC les données personnelles de ressortissants de ce pays ainsi que des applications de piratage par hameçonnage vocal.

Les groupes criminels ont incité leurs victimes à télécharger des outils conçus pour leur soutirer davantage de renseignements. Par la suite, ils ont affirmé être des employés d'IF pour amener les victimes à leur envoyer de l'argent.

Remarque : Pour de plus amples renseignements, voir Conseil de sécurité des Nations Unies (septembre 2022) *S/2022/668 Lettre datée du 2 septembre 2022, adressée au Président du Conseil de sécurité par le Groupe d'experts créé en application de la résolution 1874 (2009)*.
Source : Groupe d'experts des Nations unies et Corée du Sud.

2.3. Techniques et typologies du BC

Structure des réseaux de BC

22. Au moment de blanchir les produits générés par différents types de CF, les criminels doivent agir rapidement et efficacement. Les administrations ont observé la participation de groupes spécialisés dans le BC et de tiers professionnels, y compris des avocats, des comptables, des conseillers fiscaux, des secrétaires généraux et des banquiers. Les groupes de BC professionnels peuvent faire partie de syndicats du crime s'adonnant aux CF ou d'une organisation distincte décentralisée qui offre des services de BC selon un modèle de « crime en tant que service » (réseaux de BC professionnels).

Encadré 7. Réseau QQAAZZ

Le réseau QQAAZZ s'est annoncé comme « fournisseur de services de dépôts bancaires complice, à l'échelle mondiale » sur des forums en ligne de cybercriminels russophones, où les cybercriminels se réunissent pour offrir ou trouver des compétences ou des services spécialisés nécessaires pour s'adonner à diverses cyberactivités criminelles. Le réseau QQAAZZ a lancé et maintenu en service des centaines de sociétés fictives et de comptes bancaires personnels dans des institutions financières partout dans le monde, qui étaient utilisés pour recevoir les fonds de cybercriminels œuvrant dans le domaine des CF. Les fonds étaient ensuite transférés vers d'autres comptes bancaires contrôlés par le QQAAZZ et ils étaient parfois convertis en cryptomonnaie en utilisant les services d'un mélangeur conçu pour dissimuler la source d'origine des fonds. Après avoir prélevé une part pouvant aller jusqu'à 50 %, QQAAZZ retournait le reste des fonds volés à ses clients criminels.

En novembre 2020, une opération policière internationale impliquant 16 pays a entraîné l'arrestation de 20 personnes soupçonnées d'appartenir au réseau criminel QQAAZZ qui tentaient de blanchir des dizaines de millions d'euros pour le compte des principaux cybercriminels au monde. Une quarantaine de perquisitions ont été réalisées en Lettonie, en Bulgarie, au Royaume-Uni, en Espagne et en Italie et des poursuites pénales ont été engagées contre les personnes arrêtées par les États-Unis, le Portugal, le Royaume-Uni et l'Espagne.

Source : Portugal et Europol

23. Habituellement, les produits des CF sont rapidement blanchis par l'entremise d'un réseau de comptes. Des études de cas montrent que ces réseaux peuvent être complexes en s'étendant au-delà des frontières et à de nombreuses institutions financières, même si la situation peut varier selon le niveau de complexité de l'organisation criminelle[11].

24. Les réseaux de comptes utilisés pour le BC lié aux CF impliquent généralement des individus et des personnes morales.

- **Les mules financières individuelles** sont souvent recrutées par les criminels en utilisant différentes méthodes, y compris des offres d'emploi et des publicités ainsi que des interactions en ligne sur des médias sociaux. Les recruteurs des mules financières sont aussi appelés « gardiens ». Les mules financières peuvent être sciemment complices dans le blanchiment des fonds ou elles peuvent travailler involontairement (par la tromperie), ou par négligence, et peuvent aussi se voir offrir des incitatifs ou des honoraires pour gérer les fonds illicites. Il est difficile de déterminer qui contrôle la mule (c.-à-d. le gardien des mules), qui recrute les participants, conscients ou non, ou détermine l'origine des sommes frauduleuses. Certaines administrations ont mentionné des cas de recrutement de ressortissants étrangers, sans lien

[11] Pour de plus amples renseignements sur l'utilisation de mules par des blanchisseurs de capitaux professionnels et des réseaux de BC, voir GAFI (juillet 2018), *Professional Money Laundering* [en anglais seulement].

manifeste avec l'administration, qui avaient pour tâche de créer des comptes, que ce soit en se rendant physiquement sur place ou en ouvrant un compte virtuel.

Encadré 8. Recrutement de mules : offre d'emploi

Mme RS est la propriétaire d'un magasin sari-sari qui a été recrutée par un certain M. O pour ce qu'elle croyait être une offre d'emploi légitime. M. O est un ressortissant nigérien qui a été arrêté en 2019 pour s'être soi-disant livré à une arnaque amoureuse en ligne très lucrative ayant entraîné des pertes chiffrées à plus de 8 millions de pesos philippins (environ 129 000 euros).

M. O avait promis à Mme RS une part de chaque transaction bancaire qu'elle effectuait. Au total, Mme RS s'est occupée de 83 transactions équivalant à 3,6 millions de pesos philippins (environ 58 000 euros) sur une période de 6 mois. Toutes les transactions étaient en espèces (c.-à-d. des dépôts et des retraits en espèces à des GAB et au comptoir). M. O a finalement été arrêté avec la collaboration de Mme RS dans le cadre d'une opération de provocation policière.

Source : Philippines

- **Les sociétés fictives** sont contrôlées par des criminels s'adonnant aux CF, généralement par le biais de prête-noms ou d'administrateurs désignés. Les mules financières recrutées peuvent aussi avoir pour tâche de servir de prête-nom et d'ouvrir des comptes d'entreprise dans le but de mieux dissimuler le criminel propriétaire. Certaines administrations ont indiqué que des sociétés fictives ont utilisé des adresses d'entreprise en ligne[12] pour masquer davantage leurs activités criminelles. Dans le cas de fraudes commerciales en ligne, les criminels peuvent aussi utiliser des sociétés fictives pour ouvrir des points de vente virtuels pour des entreprises de services commerciaux afin de traiter les paiements et les transferts des victimes.

[12] Les adresses des entreprises virtuelles sont des adresses physiques réelles fournies par certains fournisseurs de services qui permettent aux entreprises de recevoir du courrier et des colis par la poste.

Encadré 9. Les entreprises fictives constituent une fraude liée à une plateforme de négociation en ligne

Un certain nombre de DOD ont été remplies par la CRF de la Türkiye relativement à un modèle de fraude utilisant une plateforme de négociation en ligne dont les victimes étaient approchées pour faire des investissements en devises étrangères par téléphone ou sur les médias sociaux. Un réseau de 209 entreprises, qui blanchissaient les produits les unes des autres, soutenait cette fraude. Les entreprises disposaient de comptables communs et étaient principalement créées à la même date et étaient liquidées peu après leur création.

Une analyse de la CRF de la Türkiye a révélé que les sociétés fictives étaient aussi réparties dans trois sous-groupes distincts, selon les fonds transférés et la tierce partie complice associée à la société. Au total, environ 10 milliards de livres turques (TRL) (environ 336,7 millions d'euros) ont été frauduleusement acquises et blanchies.

- Dans cette affaire, 135 entreprises ont reçu 9,6 milliards de livres turques (environ 323,2 millions d'euros) découlant de la fraude par l'entremise d'entreprises de paiement. Pour faciliter la réception des transactions réalisées par les victimes, ces entreprises ont conçu des comptes de point de vente virtuel. Un montant de 100 millions de livres turques (environ 3,4 millions d'euros) a été retiré en espèces et environ 6 milliards de livres (environ 202 millions d'euros) ont été transférés vers une société d'exploitation aurifère.
- De plus, 59 entreprises se sont partagé 700 millions de livres turques (environ 23,6 millions d'euros) provenant des produits de la fraude. Un montant de 200 millions de livres turques (environ 6,7 millions d'euros) a été retiré en espèces et le reste du montant a été transféré à des FSAV après avoir été blanchi au moyen de comptes gérés par des tierces parties complices.
- Enfin, 23 entreprises ont reçu 875 millions de livres turques (environ 29,5 millions d'euros) provenant des produits de la fraude. Un montant de 220 millions de livres turques (environ 7,4 millions d'euros) a été retiré en espèces et le reste du montant a été transféré à des FSAV après avoir été blanchi au moyen de comptes gérés par des tierces parties complices.

Source : Türkiye

- **Des entreprises légitimes**, semblables aux mules financières, peuvent aussi être amenées à recevoir des produits de CF (p. ex. comme occasion d'affaire ou d'investissement) et se voir demander de rediriger les fonds ou d'être remboursées à partir d'un compte distinct contrôlé par une organisation criminelle. Dans certains cas, on a vu des entreprises légitimes accepter volontairement de telles « occasions d'affaires », particulièrement en cas de difficultés économiques. La participation d'entreprises légitimes fournit une façade supplémentaire pour empêcher la détection des activités illicites.

25. Il y a des similitudes quant à la façon dont les mules financières des réseaux de BC sont mises en place pour les CF et les autres types de crimes. Toutefois, les administrations ont aussi observé certaines différences qui s'appliquent peut-être davantage aux mules liées aux CF.

- **Méthode de recrutement :** Les mules financières pour les CF sont plus susceptibles d'être recrutées en ligne, y compris au moyen d'offres d'emploi provenant de fausses entreprises ou de courriels indésirables. Les criminels peuvent aussi exploiter la conjoncture économique et faire semblant qu'il s'agit d'une véritable offre d'emploi permettant de gagner de l'argent facilement. Les victimes de CF (p. ex. une fraude amoureuse) peuvent souvent être amenées à servir de mules financières. Dans certains cas, des victimes de la traite de personnes (comme les migrants ou les travailleurs illégaux) sont aussi utilisées pour ouvrir de tels comptes.
- **Utilisation de comptes :** Les mules financières liées aux CF sont utilisées pour leurs comptes dans des institutions financières, puisqu'ils permettent de recevoir et d'envoyer rapidement des fonds obtenus frauduleusement grâce à des modes de paiement électroniques, contrairement à des transferts physiques ou à des dépôts en espèces. Cette situation découle probablement de la façon dont les victimes sont escroquées (c.-à-d. par transferts de fonds). Étant donné la commodité des services bancaires numériques pour les mouvements de capitaux, les personnes ciblées pour devenir des mules financières dans les cas de CF sont susceptibles de posséder un certain niveau de connaissances de base ou de maîtrise des ordinateurs et de la technologie.

Encadré 10. Une victime d'une arnaque amoureuse devenue une mule

Entre avril et mai 2022, une femme âgée qui avait, à l'origine, ouvert un compte bancaire pour recevoir sa pension a reçu deux versements d'un montant plus élevé. Un des transferts de fonds provenait d'un compte bancaire national, alors que le second provenait d'une victime signalée à l'étranger.

Une enquête ultérieure des autorités slovaques a révélé que la femme communiquait avec un individu par l'intermédiaire des médias sociaux et qu'elle avait été victime d'une arnaque amoureuse. La femme âgée avait fourni ses identifiants de connexion bancaire en ligne au fraudeur et son compte bancaire avait ensuite été utilisé pour blanchir d'autres produits de la criminalité. Une partie des sommes reçues étaient transformées en cryptomonnaie en utilisant la plateforme d'un FSAV étranger.

Source : Slovaquie

Techniques et typologies du BC

26. L'endroit où survient la CF (c.-à-d. où se trouve la victime) diffère souvent de l'endroit où sont blanchis les produits de la CF et les réseaux de mules financières peuvent s'étendre à de nombreuses administrations. Les syndicats du crime qui s'adonnent à la CF réalisent que les IF ou les autorités compétentes peuvent avoir déjà identifié les comptes utilisés pour des activités frauduleuses avant le blanchiment des capitaux, ce qui pourrait entraîner l'interception des produits de la

criminalité avant qu'ils atteignent les comptes des criminels. Pour améliorer leur taux de réussite, les criminels peuvent effectuer des « tests » en réalisant des transactions de faible valeur afin de pouvoir modifier la destination des fonds si les tests échouent.

27. Le type de compte utilisé au départ pour recevoir les produits des CF dépend généralement du type de CF réalisées pour conserver l'apparence de légitimité. Des modifications apportées au fil du temps ont aussi été observées dans des comptes de premier niveau. Par exemple, dans des cas de BEC, les syndicats du crime organisé s'adonnant aux CF ont cessé d'utiliser les comptes de particuliers pour utiliser plutôt des comptes d'entreprises afin de réduire le risque de détection.

Tableau 1. Relations entre le type de CF et le compte de premier niveau

Type de CF	Type de compte de premier niveau
Fraude par compromission de messagerie d'entreprise	Compte d'entreprise (p. ex. sociétés fictives ou nouvellement enregistrées)
Fraude par hameçonnage	Mules financières individuelles
Fraude par usurpation d'identité sur les médias sociaux et dans les télécommunications	Mules financières individuelles
Fraude liée au commerce ou à des plateformes de négociation en ligne	Compte d'entreprise (p. ex. sociétés fictives ou nouvellement enregistrées)
Fraude amoureuse en ligne	Mules financières individuelles
Fraude d'embauche	Mules financières individuelles

Remarque : Ce tableau tente de souligner certaines tendances générales fondées sur l'expérience des administrations quant aux types de comptes de premier niveau utilisés selon le type de fraude. Toutefois, ces tendances ne s'appliquent pas nécessairement à tous les cas.

28. Une fois le compte créé par le syndicat de la CF, les fonds acquis frauduleusement sont rapidement traités pour entrer dans le réseau de BC. Par la suite, les fonds sont rapidement acheminés sur plusieurs niveaux au cours d'une série de transactions « canalisées » par l'entremise de comptes au pays ou à l'étranger qui sont contrôlés par les mules ou les prête-noms eux-mêmes ou par le syndicat de la CF. Dans ce dernier cas, les mules financières transmettent les identifiants bancaires, les cartes ou les jetons ou offrent une procuration au syndicat pour lui conférer le contrôle direct des comptes. La participation de facilitateurs professionnels au processus, pendant la création d'une procuration par exemple, confère aux transactions une apparence de légitimité et favorise la dissimulation du crime.

29. Pour éviter d'être découverts et demeurer anonymes, les syndicats du crime qui s'adonnent à la CF utilisent différents mécanismes et techniques, comme le blanchiment fractionné; le passage d'un compte à l'autre entre différentes institutions financières; les fournisseurs de services de transfert de fonds ou de paiement; et la conversion en d'autres types d'actifs financiers (p. ex. argent électronique [monnaie électronique][13], cartes prépayées, AV). Ces méthodes peuvent augmenter le temps requis pour que la CRF et les corps policiers accèdent aux données financières nécessaires provenant de différents pays, secteurs et institutions afin de localiser, de protéger et finalement, de récupérer les produits

[13] La monnaie électronique est une représentation numérique d'une monnaie fiduciaire utilisée pour transférer par voie électronique la valeur libellée en monnaie fiduciaire. La monnaie électronique est un mécanisme de transfert numérique pour les monnaies fiduciaires, c.-à-d. qu'elle permet de transférer par voie électronique la valeur qui a cours légal; GAFI (juin 2014), *Virtual Currencies - Key Definitions and Potential AML/CFT Risks* [en anglais seulement].

illicites. Il est aussi possible que certaines mules financières n'autorisent l'utilisation de leurs comptes qu'à certains moments précis et limités. La période restreinte ainsi que les procédures d'intégration légitimes rendent relativement difficile la détection des activités anormales pour les institutions.

Encadré 11. Sociétés fictives, comptes bancaires et actifs virtuels

De multiples plaintes ont été déposées auprès des corps policiers indiens en raison de l'utilisation d'une application mobile pour frauder les gens sous couvert d'une plateforme d'investissement pour le minage de cryptomonnaie. L'application promettait une part des profits découlant de ces investissements. L'entreprise avait incité les victimes à investir davantage dans la plateforme et par la suite, les retraits et les paiements ont cessé. Le site Web et l'application sont devenus inaccessibles et les exploitants de l'application ont cessé de répondre aux investisseurs. De nombreux OAL enquêtant sur les plaintes déposées par des clients dans différentes régions du pays ont demandé des renseignements sur cette affaire à la CRF de l'Inde. L'analyse de la CRF de l'Inde a permis d'identifier deux entités exploitant l'application sur Google Play Store, qui ont plus tard été supprimées de Google Play Store. L'analyse a permis d'identifier 34 autres entités liées aux 2 premières entités. Sur les 36 entités, 28 avaient pour directeurs des ressortissants étrangers.

La Direction de l'exécution de l'Inde a aussi entamé des enquêtes parallèles sur le BC, qui ont révélé un complot à grande échelle et la participation de plusieurs entités fictives à l'exploitation d'applications et de sites Web frauduleux semblables afin de tromper les gens crédules et de détourner les produits de la criminalité. Après une vérification sur place, il a été impossible de trouver les entités aux adresses enregistrées. En suivant la piste financière, plusieurs de ces entités se sont aussi avérées impliquées dans l'exploitation d'applications de paris et de prêts illégaux et fraudaient aussi la population au moyen de ces applications. Les sommes illicites soutirées aux victimes étaient transférées dans les comptes de diverses entités fictives et une partie des produits du crime finissait aussi par être convertie en actifs virtuels. Des produits de la criminalité sous forme de soldes disponibles dans les comptes bancaires détenus par les différentes entités fictives d'un montant s'élevant à 865 millions de roupies indiennes (9,9 millions d'euros) ont été trouvés et gelés.

Source : Inde

30. Les administrations ont aussi constaté l'utilisation d'autres techniques de BC ayant pour but de dissimuler le lien entre les diverses organisations criminelles s'adonnant aux CF et au BC.

- **Espèces :** Bon nombre d'études de cas dans ce rapport prévoient le retrait d'espèces par les mules et les syndicats de la CF. Il peut être difficile de suivre les mouvements d'espèces en dehors des IF. Il est possible de retirer des espèces de GAB après leur blanchiment dans un réseau de BC, ce qui permet aux criminels d'éviter tout contact direct avec les IF. Ces fonds peuvent être transportés au-delà des frontières par des passeurs de fonds et déposés dans

un autre compte pour être blanchis à nouveau. Les produits de la criminalité peuvent aussi être utilisés pour acheter des objets de valeur et des effets qui peuvent être revendus plus tard contre des espèces, comme des cartes prépayées ou des métaux précieux.

Encadré 12. Retraits d'espèces et achats d'or et de cartes de carburant

En mars 2023, un comptable d'une entreprise chinoise a été victime d'une fraude bancaire par usurpation d'identité. Il avait été ajouté à un groupe sur une application de messagerie sous le prétexte qu'il fallait procéder à une inspection annuelle des comptes de l'entreprise.

Des criminels faisant partie du groupe de messagerie se sont ensuite fait passer pour les représentants juridiques et les actionnaires de l'entreprise et ont demandé à la victime de transférer 7,8 millions de yuans (environ 996 000 euros) dans deux comptes d'entreprise désignés contrôlés par le groupe criminel. Des enquêtes policières ont démontré que les fonds avaient été transférés dans 26 comptes bancaires secondaires, puis retirés en espèces à partir de comptoirs bancaires et de GAB, transférés à des plateformes de paiement de tiers et utilisés pour acheter de l'or et des cartes de carburant.

Source : Chine

- **BC fondé sur le commerce et les services :** Il existe différentes techniques de BC fondées sur le commerce et les services que les criminels peuvent utiliser pour transférer les fonds par-delà les frontières[14]. En ce qui concerne les produits des CF, certaines administrations ont observé que les criminels utilisent des techniques de blanchiment de capitaux par voie commerciale (BCVC), comme la facturation fictive ou fausse, et utilisent les produits illicites pour acheter des biens de grande valeur ou facilement négociables (p. ex. pièces d'automobile, billets, articles ménagers, etc.). Par exemple, certaines administrations ont rapporté des virements électroniques frauduleux vers des entreprises légitimes, qu'il s'agisse de marques d'articles électroniques ou luxueuses bien connues ou de petites entreprises locales, pour l'achat de biens. Ces biens peuvent être déplacés entre les frontières et reconvertis en espèces pour un empilement et une intégration accrus. Les entreprises commerciales n'appartenant pas au programme de LBC/LFT ne possèdent pas toujours les connaissances requises pour vérifier une identité ou surveiller une transaction et elles peuvent donc être exploitées involontairement par des criminels. La fourniture de factures surévaluées ou fictives pour des services de TI ou de consultation peut aussi faire partie des techniques de BC adoptées.

[14] Voir aussi GAFI – Groupe Egmont (décembre 2020), *Blanchiment de capitaux basé sur le commerce : Tendances et évolution*; et GAFI (juillet 2018), *Professional Money Laundering* [en anglais seulement].

Encadré 13. CF, mules et BCVC

Les autorités irlandaises ont arrêté un individu important, Person MS, dans le cadre d'une arnaque amoureuse aux fins de blanchiment et de transfert des produits de CF de l'Irlande au Nigéria en utilisant le BCVC. Des enquêtes sont toujours en cours. Jusqu'à maintenant, les autorités croient que le mécanisme de blanchiment d'argent utilisait au moins 60 noms et 64 comptes bancaires.

Dans ce stratagème, les produits des fraudes étaient d'abord transférés dans les comptes bancaires de mules irlandaises. Les fonds étaient ensuite retirés en espèces et transférés dans des comptes irlandais directement liés à Person MS ou lui appartenant. Beaucoup de comptes liés à Person MS avaient été ouverts sous de fausses identités.

Une entreprise nigérienne (contrôlée par un Nigérien que l'on présume habiter aux États-Unis) commandait des marchandises d'entreprises européennes ou chinoises légitimes. Ces entreprises légitimes géraient des biens pouvant être achetés et expédiés pour la revente, notamment de l'alcool, des vêtements, du matériel électronique et des produits pharmaceutiques. Les factures visées étaient payées à partir des comptes irlandais de Person MS et les biens étaient ensuite expédiés à l'entreprise du complice au Nigéria.

À une occasion, une entreprise pharmaceutique allemande a reçu un montant de plus de 1,7 million d'euros pour payer des biens achetés par l'entreprise nigérienne. Ces fonds ont été directement reliés aux produits d'une CF et d'une arnaque amoureuse réalisées en Europe et aux États-Unis et ils provenaient de différents comptes liés à Person MS ou lui appartenant ou provenaient directement des victimes. Ces marchandises ont finalement été expédiées au Nigéria.

Source : Irlande

- **Expéditeurs de fonds et FSAV sans permis ou non enregistrés :** Les produits de la criminalité peuvent être transférés en dehors d'un pays en faisant appel à des expéditeurs de fonds illégaux ou à un système hawala prévoyant peu ou pas de mesures de contrôle pour appuyer la LBC/LFT. Lorsque des AV sont concernés, les syndicats peuvent utiliser des FSAV situés dans des administrations où les mesures de contrôle pour la LBC/LFT sont faibles ou inexistantes.
- **Techniques de renforcement de l'anonymat pour les AV[15] :** L'utilisation de portefeuilles non hébergés, de transactions entre particuliers, de chaînes de pelage et d'échanges à risque élevé sont les méthodes privilégiées pour blanchir rapidement les produits de CF liés aux AV à l'extérieur d'une administration et elles sont souvent utilisées simultanément. Les criminels

[15] Ces techniques sont examinées en détail dans GAFI (mars 2023), *Lutte contre le financement des rançongiciels*

utilisent aussi de plus en plus les guichets automatiques Bitcoin pour transférer des valeurs et dissimuler l'identité des personnes qui contrôlent les fonds, y compris en fournissant des documents d'identification falsifiés ou modifiés, comme des identifiants, des dates de naissance ou des numéros de téléphone différents lorsqu'ils déposent ou retirent des fonds. Elles utilisent aussi des techniques de dissimulation, comme des services de mélangeurs et des AV confidentiels (aussi appelés jetons privés confidentiels, comme le Monero) et des services de finance décentralisée (FiDé).

Encadré 14. BC complexe dans de nombreux secteurs

L'arnaque amoureuse d'un syndicat du crime étranger a fait environ 70 victimes au Japon. Des sommes s'élevant à 3 millions de dollars américains ont été transférées sur différents comptes bancaires de mules financières japonaises. Un Japonais agissant comme recruteur de mules local a blanchi les fonds au Ghana, où se trouvait le syndicat du crime. L'homme a finalement été arrêté par INTERPOL avec la collaboration du Ghana.

Les fonds des comptes des mules étaient ensuite transférés dans le compte du recruteur de mules japonais. Une analyse des DOD a conclu que les fonds étaient blanchis de trois façons différentes par le recruteur de mules japonais.

- Des virements électroniques étaient faits vers un compte bancaire appartenant au recruteur de mules japonais au Ghana. Les fonds étaient ensuite retirés physiquement en espèces au Ghana et livrés en mains propres au chef du syndicat du crime, qui est toujours en liberté. Pour effectuer les virements électroniques, le Japonais présentait des factures fictives à sa banque au Japon et déclarait à tort qu'elles découlaient d'une activité commerciale légitime (achat de fèves de cacao).
- Certains fonds étaient aussi transformés en AV par l'entremise d'un FSAV au Japon.
- Une autre partie des fonds était transférée au Ghana en utilisant une banque clandestine liée à la communauté ghanéenne du Japon.

Source : Japon

Impact de la numérisation et des nouvelles technologies de BC

31. Les nouvelles technologies offrent de nouveaux avantages et des possibilités aux consommateurs. Un changement important en faveur de la numérisation des services financiers est en cours et il s'est accéléré pendant la pandémie de COVID-19. La réduction de l'utilisation de l'argent comptant et l'augmentation de l'activité en ligne ont généré de nouveaux outils et processus novateurs. La chaîne des paiements financiers est aussi de plus en plus dynamique et fragmentée, compte tenu de la plus grande diversité des fournisseurs offrant des services de paiement et de transactions (voir aussi la section 3.1 ci-dessous).

32. Cependant, les progrès technologiques peuvent aussi être avantageux pour les

groupes criminels, qui profitent de ces occasions pour améliorer considérablement leurs techniques de BC. Les transactions financières sont de plus en plus réalisées presque instantanément, en partie à cause des attentes des clients qui souhaitent une expérience fluide. Comme mentionné plus tôt, ces technologies, combinées aux techniques d'anonymisation numériques comme les RPV, compliquent la tâche aux autorités qui tentent d'identifier les plus hauts criminels qui procèdent à des transactions de BC coup sur coup.

33. La numérisation a augmenté la vitesse et la facilité avec lesquelles il est possible de créer un compte aux fins de BC et d'étendre la portée des syndicats de la CF à l'étranger. Certaines administrations ont remarqué une augmentation des procédures virtuelles à distance dans deux domaines : l'ouverture de comptes et la création d'entreprises. Les procédures virtuelles à distance rendent inutiles les déplacements physiques. Les criminels peuvent donc en profiter pour blanchir des capitaux.

Encadré 15. L'expansion par la numérisation

Une analyse de la CRF a mis à jour un vaste réseau constitué de 147 personnes et 276 comptes bancaires dans huit banques différentes. Ces personnes avaient cédé leur identité numérique nationale, permettant l'identification des utilisateurs sur des plateformes gouvernementales et d'autres plateformes en ligne, à des syndicats du crime. Les syndicats utilisaient ensuite les identités numériques pour ouvrir des comptes bancaires à distance et contrôler directement ces comptes de mules financières pour blanchir les produits de CF. La CRF a détecté le réseau en cernant des similitudes comme des transactions bancaires, des points de données (coordonnées et ID de l'appareil à l'étranger) ainsi que des coordonnées (adresse, courriel, téléphone) en commun.

Les renseignements ont été communiqués à Anti-Scam Command (ASCom), l'unité consacrée à la lutte contre la CF et le BC connexe relevant de la Force de police de Singapour. Les enquêtes d'ASCom ont conduit à l'arrestation de six personnes et des poursuites ont été intentées contre trois individus en raison de leur rôle dans l'arnaque.

Source : Singapour

34. Les criminels peuvent rapidement étendre la portée (souvent transnationale) d'un réseau de mules financières en utilisant des outils numériques pour renforcer le recrutement au-delà des frontières. Les médias sociaux et les applications de voix par protocole Internet (VoIP) s'avèrent aussi être des méthodes fréquemment utilisées dans le processus de recrutement de mules. Traditionnellement, le processus de blanchiment au moyen de réseaux de mules pouvait connaître certains ralentissements en raison du temps requis pour que les mules reçoivent et suivent les directives fournies par les autres syndicats du crime. Ces retards ont été considérablement réduits grâce à l'utilisation de plateformes de messagerie instantanée par les syndicats de la CF.

35. De plus en plus, les criminels peuvent voler des identités en utilisant divers outils technologiques et techniques, y compris l'hameçonnage, les achats ou l'incitation des personnes à céder volontairement leur identité. Parfois, ils peuvent utiliser de fausses identités ou des identités synthétiques, qui impliquent l'utilisation de

renseignements sur l'identité réels et fictifs pour créer des comptes frauduleusement. Les criminels peuvent ensuite configurer et contrôler directement les comptes en utilisant les identités volées ou falsifiées. Il est ainsi plus difficile de retracer les activités de BC, puisque les titulaires des comptes ne sont pas nécessairement au courant de leur participation.

36. Une délégation a signalé les risques que des hypertrucages puissent être utilisés pour pirater des comptes. Avec l'aide d'algorithmes d'apprentissage automatique, un fraudeur pourrait créer un hypertrucage de la voix ou de l'image d'une personne, qui pourrait ensuite être utilisé pour usurper l'identité de cette personne au téléphone ou dans des systèmes d'authentification biométrique. Les hypertrucages peuvent aussi être combinés à des techniques de piratage psychologique pour amener les victimes à fournir leurs identifiants de compte. La technologie d'hypertrucage est relativement nouvelle, ce qui signifie que les risques de piratage de comptes au moyen d'hypertrucages sont probablement assez faibles pour le moment. Toutefois, cette technologie pourrait représenter un risque important dans le futur si elle continue de se développer et devient plus largement accessible.

Encadré 16. Vol d'identité à distance aux fins de contrôle direct

Dans une série de fraudes par hameçonnage, les criminels ont amené les victimes à installer des outils d'accès à distance sur leurs ordinateurs. Dans bien des cas, des comptes ont été créés à l'aide de FSAV en utilisant les noms des victimes sans qu'elles soient au courant. Pour ce faire, les criminels utilisaient les données volées grâce aux outils d'accès à distance. On soupçonne aussi les criminels d'avoir guidé les victimes pendant le processus de vérification en ligne des comptes ouverts, en utilisant les outils d'accès à distance pour cacher les véritables interfaces.

Enfin, les victimes étaient incitées à transférer des fonds dans les comptes de FSAV. Les criminels pouvaient utiliser directement ces comptes pour des activités de blanchiment de capitaux par la suite. Au total, on estime que les victimes ont perdu plus de 600 000 euros dans cette série de fraudes.

Source : Autriche

3. Autres vulnérabilités émergentes liées au BC

37. Les mesures de prévention exigées des IF, des EPNFD et des FSAV en vertu des normes du GAFI (recommandations 9 à 23) visent à empêcher les produits des CF d'entrer dans les secteurs financiers ou autres. Cette section est axée sur les nouvelles vulnérabilités liées au BC que les syndicats de la CF pourraient exploiter.

3.1. Risque lié aux institutions financières numériques[16]

38. L'évolution des paiements a entraîné la création de nouvelles institutions financières numériques, comme les fournisseurs de services de paiement (FSP), l'émission de monnaie virtuelle, etc. Les IF traditionnelles ont plus de ressources à leur disposition, ce qui peut entraîner des mesures de contrôle plus solides par rapport aux IF numériques plus récentes. Cette situation peut entraîner des remplacements, les criminels cherchant à exploiter les vulnérabilités de ces autres fournisseurs de services financiers pour blanchir les fonds.

39. Le réseau de paiement peut aussi être fragmenté. Il peut y avoir différentes relations financières établies entre ces institutions, p. ex. lorsque diverses institutions de paiement effectuent des transactions les unes avec les autres ou fournissent des comptes à de plus petits fournisseurs, qui à leur tour offrent d'autres types de services financiers (voir aussi l'encadré 17 ci-dessous). Cette fragmentation peut aussi amplifier les difficultés à retracer les transactions au sein des différents types d'institutions dans la « chaîne de paiement ». Elle peut aussi représenter un obstacle au moment de garantir la disponibilité immédiate des renseignements de base sur l'émetteur et le bénéficiaire des transferts dans l'ensemble de la chaîne de paiement[17].

40. Conformément aux normes du GAFI, une solide surveillance de la réglementation devrait être appliquée pour les nouvelles institutions financières, y compris un permis ou un enregistrement approprié et des mesures pour empêcher les criminels ou leurs associés de contrôler ces entités. Les organismes de réglementation devraient s'assurer que toutes les institutions qui effectuent des transactions appliquent une surveillance suffisante à leurs activités respectives; toutes les institutions ont la responsabilité de prendre des mesures de vigilance à l'égard de la clientèle (CDD) et de surveiller les transactions à l'émission et à la réception.

[16] Le présent rapport reconnaît aussi les risques de BC liés aux AV et aux FSAV. Pour de plus amples renseignements sur les risques réglementaires et les défis liés aux FSAV, voir GAFI (mars 2023), *Lutte contre le financement des rançongiciels* et (juin 2023), *Virtual Assets : Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* [en anglais seulement].

[17] Le GAFI envisage aussi de nouvelles modifications à la recommandation 16 (sur les virements électroniques) pour prendre en compte les développements récents et à venir concernant l'architecture des systèmes de paiement.

Encadré 17. Abus dans le secteur des PSP

Une analyse des autorités de surveillance françaises réalisée dans la première moitié de 2021 a permis de cibler les principaux prestataires de services de paiement utilisés pour recevoir des virements électroniques frauduleux. Ces PSP offraient généralement des « opérations bancaires comme service » (banking as a service), et certains avaient une succursale en France uniquement pour pouvoir offrir des IBAN français, moyennant une présence physique minimale.

L'analyse a conclu que ces PSP importants étaient environ 200 fois plus risqués que les autres institutions. La plupart d'entre eux avaient en place de mauvaises procédures de vérification de l'identité et de surveillance des transactions. Les criminels avaient ouvert des comptes en utilisant une identité usurpée et pouvaient vérifier rapidement si certains des comptes ouverts étaient considérés comme frauduleux par le PSP en essayant d'abord de réaliser des transactions impliquant de petits montants et en modifiant la destination des fonds, si nécessaire. Ils transféraient ensuite rapidement les fonds acquis frauduleusement vers un ou plusieurs comptes. Le fait de diviser les montants entre plusieurs comptes permet aux criminels de contourner les restrictions imposées par le PSP relativement à ses services, comme les limites des retraits en espèces ou l'obligation de demeurer sous le seuil de contrôle des opérations déterminé à l'interne par le PSP.

Source : France

3.2. Abus liés aux IBAN virtuels[18]

41. Un autre exemple de méthode utilisée pour exploiter les innovations financières aux fins des CF est l'utilisation de numéros de compte bancaire international virtuels (vIBAN). Bon nombre d'institutions émettent des vIBAN pour leurs clients, y compris des banques et des PSP. Même si les vIBAN sont utilisés pour de nombreuses raisons légitimes, comme pour faciliter et catégoriser les paiements de multiples parties, plusieurs administrations ont souligné l'usage abusif des vIBAN comme outil pour effectuer du BC lié à des CF.

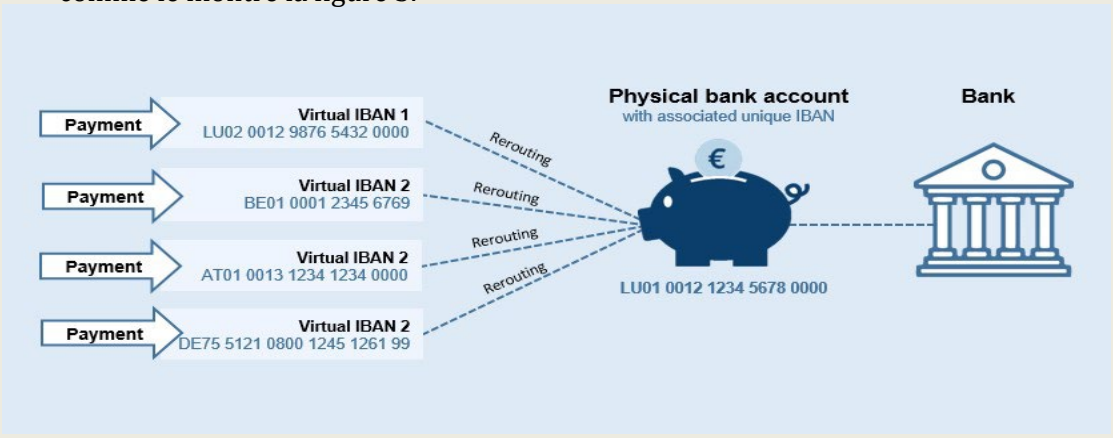
[18] Pour de plus amples renseignements concernant les risques et les défis associés aux vIBAN, voir (juin 2023), *Europol Financial Intelligence Public Private Partnership (EFIPPP) Threat Intelligence Information on Virtual IBANs* (accessible uniquement aux membres du projet de partenariat public-privé de renseignement financier d'Europol [EFIPPP]).

Encadré 18. Qu'est-ce qu'un vIBAN?

Les vIBAN fonctionnent de la même façon que les IBAN conventionnels, puisqu'ils peuvent être utilisés pour envoyer et recevoir des paiements à l'échelle mondiale. Ils ont également le même aspect que leurs équivalents traditionnels et sont aussi composés de jusqu'à 34 caractères alphanumériques. Sur les plans fonctionnels et visuels, ils sont donc impossibles à distinguer des IBAN courants.

La principale différence entre les IBAN courants et virtuels repose sur le jumelage des comptes. Un IBAN est jumelé selon un rapport de 1:1 à un compte bancaire, ce qui signifie qu'il n'y a qu'un seul compte bancaire physique lié à chaque IBAN. Par conséquent, si une personne utilise un IBAN pour faire un paiement, les fonds se retrouvent automatiquement dans le compte bancaire correspondant au IBAN.

Par contre, un IBAN virtuel est un numéro virtuel qui n'est pas jumelé à une banque physique. Il s'agit d'un numéro de référence émis par une banque permettant à un paiement entrant d'être redirigé vers un IBAN physique, qui est lui-même lié à un compte bancaire physique. Il ne peut pas contenir de fonds et son solde est constamment à zéro. Les détenteurs de vIBAN peuvent aussi posséder plusieurs IBAN virtuels uniques, qui redirigent et centralisent tous les paiements dans un seul compte bancaire physique, comme le montre la figure 3.

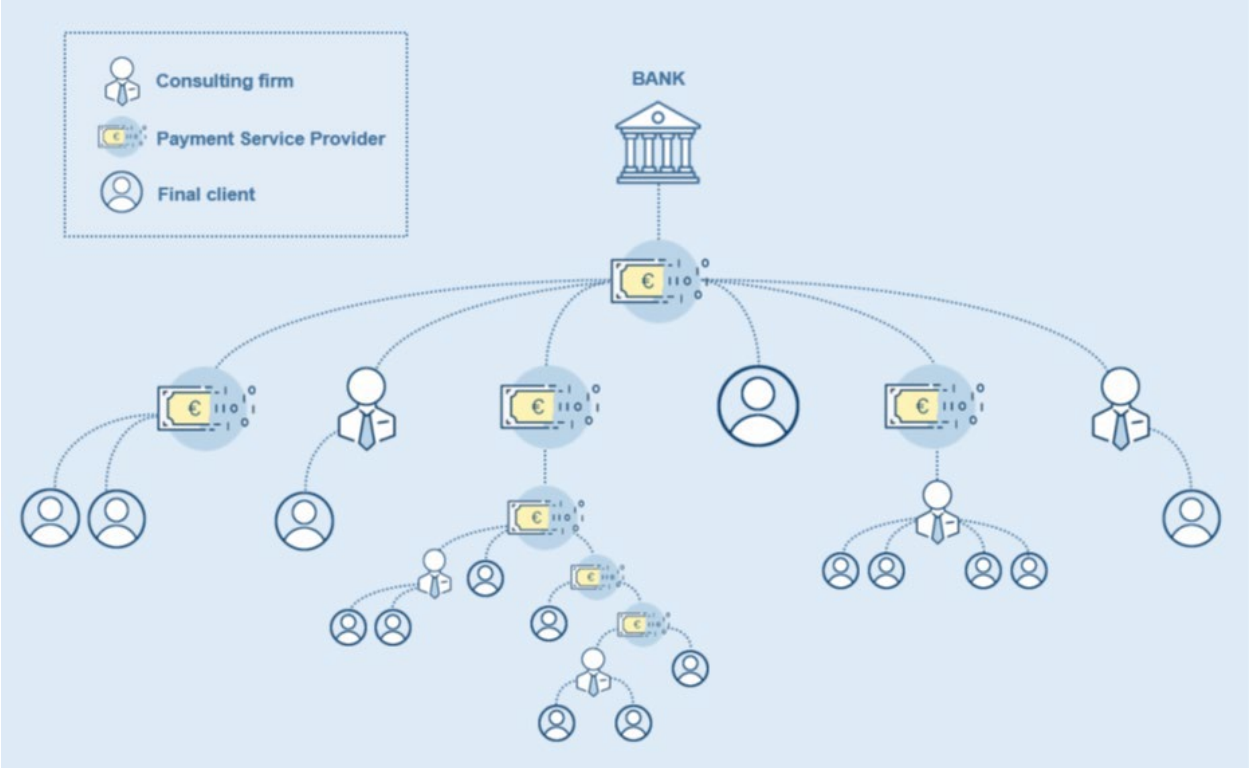


Traduction de l'image :
Paiement – IBAN virtuel 1 – Réacheminement – Compte bancaire physique possédant un IBAN unique – Banque
Paiement – IBAN virtuel 2 – Réacheminement
Paiement – IBAN virtuel 2 – Réacheminement
Paiement – IBAN virtuel 2 – Réacheminement

Source : Partenariat public-privé de renseignement financier d'Europol

42. Comme les IBAN et les vIBAN sont visuellement identiques, les criminels les utilisent pour amener les victimes à penser qu'elles transfèrent des fonds dans un compte bancaire, alors qu'en fait, un vIBAN peut être utilisé, par exemple, pour porter une somme au crédit d'un portefeuille électronique. Comme si ce n'était pas déjà suffisamment complexe, les vIBAN peuvent être réémis par un client d'une institution financière, en particulier si le client est une autre institution financière. Il est donc difficile de déterminer le pays d'origine d'un vIBAN ainsi que l'emplacement du compte principal.

Figure 2. Réseau en cascade de fournisseurs de vIBAN qui émettent et réémettent des vIBAN



Traduction de l'image :
Société d'experts-conseils
Prestataire de services de paiement
Client final
Banque

Source : Partenariat public-privé de renseignement financier d'Europol

43. Bref, les criminels peuvent faire un mauvais usage des vIBAN pour masquer les renseignements sur l'identité des bénéficiaires finaux et dissimuler les mouvements de fonds illicites. Il peut donc être difficile de déterminer où se trouvent le véritable compte principal ainsi que l'institution financière émettrice et d'assurer une surveillance appropriée des transactions. En fin de compte, ce système entraîne des difficultés que doivent surmonter les autorités compétentes pour localiser les comptes physiques et geler les fonds (puisque les vIBAN sont de simples numéros de référence émis par les banques et qu'il ne s'agit pas de comptes réels détenant des soldes concrets). À titre de bonne pratique, certaines administrations ont collaboré avec des banques émettant des vIBAN pour déterminer rapidement l'établissement de paiement lié au compte principal en cas de CF.

Encadre 19. Utilisation des vIBAN à mauvais escient aux fins de CF

De février à mars 2023, la CRF du Luxembourg a reçu plusieurs signalements de ce que l'on appelle l'arnaque « Bonjour maman », où les victimes reçoivent des messages WhatsApp d'un numéro de téléphone inconnu, mais local, provenant de fraudeurs qui prétendent être leur enfant. Les victimes recevaient des messages textes en luxembourgeois, provenant d'un numéro de téléphone cellulaire du Luxembourg, mentionnant un IBAN du Luxembourg.

Pendant l'enquête sur cette affaire, la CRF du Luxembourg a découvert que les IBAN fournis par les fraudeurs étaient des vIBAN. Ceux-ci étaient émis par une institution bancaire du Luxembourg à un fournisseur de services de paiement situé au Luxembourg qui offre des cartes de crédit prépayées à des clients européens. Ces cartes de crédit prépayées peuvent être approvisionnées en transférant de l'argent au moyen de l'IBAN virtuel et les criminels prévoyaient de les utiliser pour blanchir de l'argent.

Au moyen des six vIBAN utilisés dans le cadre de l'arnaque qui ont été identifiés, la CRF du Luxembourg a pu bloquer ou récupérer 40 000 des 55 000 euros détournés par les fraudeurs. L'intervention de la CRF du Luxembourg a été facilitée par la collaboration entre elle et la banque qui a émis les vIBAN, ce qui a permis de déterminer rapidement l'établissement de paiement détenant le compte correspondant du client final.

Source : Luxembourg

3.3. Secteurs non traditionnels

44. De nombreuses administrations ont souligné la pertinence de la collaboration avec les secteurs non traditionnels, y compris les plateformes de médias sociaux, le commerce électronique et les fournisseurs de services de télécommunication et d'accès à Internet, pour lutter contre le BC lié à la CF. Même si ces secteurs non traditionnels ne sont pas réglementés pour la LBC/LFT, ils possèdent des renseignements utiles qui peuvent aider à faire avancer les enquêtes sur le BC, en particulier lorsqu'ils sont utilisés pour commettre des CF et recruter des mules. Les plateformes de médias sociaux, ainsi que les fournisseurs de services de télécommunication et d'accès à Internet, peuvent fournir des renseignements judiciaires numériques essentiels, notamment des adresses IP, des numéros de téléphone, des adresses courriel, etc., qui peuvent aider à déterminer les principaux auteurs des crimes. Lorsque des publicités ou des sites Web frauduleux sont utilisés pour une CF, ces secteurs disposent aussi de renseignements sur les paiements et les transactions financières liés aux criminels (p. ex. détails concernant les paiements pour l'hébergement des sites Web et des publicités).

45. L'expérience et les études de cas des administrations ont aussi démontré comment le commerce en ligne et les plateformes de médias sociaux, de diffusion en continu ou de jeu en ligne peuvent être utilisés à des fins malveillantes pour blanchir les produits de CF. L'utilisation généralisée des plateformes de médias sociaux, de diffusion en continu et de jeu en ligne permet aux utilisateurs de recevoir des dons,

des cadeaux, des jetons ou des crédits des spectateurs et du public. Les criminels peuvent profiter de l'absence d'exigences en matière de LBC/LFT et utiliser ces plateformes pour blanchir les produits de la criminalité.

Encadré 20. Produits de l'hameçonnage blanchis grâce à des plateformes de médias sociaux et de diffusion en continu

On a découvert que 19 comptes bancaires ont subi des pertes à la suite d'une attaque par hameçonnage visant des clients de certaines banques. Une analyse de la CRF allemande a révélé que des transactions sur ces comptes bancaires avaient été réalisées par l'entremise de comptes de paiement appartenant à deux utilisateurs. Ces fonds avaient ensuite été transférés vers des plateformes de médias sociaux et de diffusion en continu. Les fonds avaient été utilisés pour réapprovisionner les comptes des utilisateurs sur la plateforme de diffusion en continu au moyen de « pièces » (utilisées comme monnaie locale par les utilisateurs de la plateforme) pouvant être utilisées pour acheter des cadeaux virtuels. Ces cadeaux peuvent être transférés aux créateurs de contenu, qui peuvent ensuite convertir ces pièces en monnaie ordinaire et retirer la valeur monétaire équivalente.

Des enquêtes sont en cours. Des données d'adresse IP ont démontré que les transactions frauduleuses étaient réalisées à partir des mêmes adresses IP de connexion. L'analyse de la CRF indique qu'un criminel commun blanchissait une grande partie des produits de l'hameçonnage par l'entremise des plateformes de médias sociaux et de diffusion en continu pour ensuite encaisser les fonds.

Source : Allemagne

4. Mesures et stratégies opérationnelles nationales

46. Le chapitre qui suit traitera d'abord des principales sources d'information que consultent les administrations pour détecter des cyberfraudes et enquêter sur celles-ci. Il examinera ensuite les structures de coordination et de collaboration nationales ainsi que la façon dont les administrations peuvent mettre ces structures à profit pour enquêter sur les CF et le BC connexe et les prévenir.

4.1. Principales sources pour faciliter la détection

47. Selon l'expérience et les études de cas des administrations, deux principales sources d'information sont utilisées pour détecter les CF ainsi que le BC connexe et enquêter sur ceux-ci : les signalements par les victimes et les déclarations d'opérations douteuses (DOD).

48. Les administrations ont aussi mis en place différentes initiatives pour améliorer les déclarations afin de maximiser la quantité de renseignements auxquels elles ont accès pour une application efficace de la loi. En utilisant ces renseignements et ces données, les autorités compétentes tirent profit des stratégies et des outils numériques pour analyser et déterminer les groupes criminalisés pour une application de la loi plus efficace et ciblée[19].

Signalement par les victimes

49. Le signalement par les victimes est une source d'information importante pour détecter les produits illicites découlant de CF et enquêter sur ceux-ci. Dans certaines fraudes comme la compromission de messagerie d'entreprise (BEC) et l'hameçonnage, les victimes découvrent généralement relativement rapidement qu'elles ont été trompées (p. ex. lorsque leur contrepartie légitime commence à parler de paiements non effectués). Dans d'autres cas de CF, comme des fraudes à l'investissement, des arnaques amoureuses ou de l'hameçonnage, il arrive que les victimes ne réalisent qu'elles ont été trompées qu'après un certain temps.

50. Le signalement rapide par les victimes est important pour permettre aux autorités compétentes d'agir rapidement afin de retrouver les produits illicites et d'accroître les probabilités de réussite des mesures d'application de la loi. Les victimes peuvent signaler les crimes présumés aux organismes d'application de la loi, y compris aux unités spécialisées qui s'occupent des signalements de fraude. Les victimes peuvent aussi aviser leurs institutions financières, leurs prestataires de paiements et leurs FSAV que des transactions frauduleuses présumées ont été réalisées à partir de leurs comptes. D'autres administrations ont indiqué que les victimes peuvent aussi communiquer avec des organismes de protection des consommateurs dans le domaine financier plutôt qu'avec les forces de l'ordre.

51. Toutefois, il y a probablement une sous-déclaration des CF par les victimes, en particulier lorsque la perte subie est négligeable. Si l'on ajoute les facteurs émotionnels, y compris l'embarras ou la peur, les victimes peuvent décider de ne

[19] Pour de plus amples renseignements sur la façon dont les CRF et les OAL peuvent utiliser la transformation numérique pour une efficacité accrue des capacités d'analyse et d'enquête en matière de LBC/LFT, voir les rapports confidentiels sur la transformation numérique du LBC/LFT pour les autorités opérationnelles : Groupe Egmont - GAFI (octobre 2021), *Detection of Suspicious Activities and Analysis of Financial Intelligence (Phase 1)*; et GAFI (mai 2022) *Law Enforcement Authorities and Information Exchange (Phase 2)* [en anglais seulement].

pas porter plainte.

52. Pour augmenter les signalements par les victimes, certaines administrations ont adopté la bonne pratique de concevoir des plateformes spécialisées permettant aux victimes de signaler les CF, notamment des portails en ligne. Les plateformes peuvent fournir un format de déclaration structuré pour normaliser la saisie des données, ce qui facilite l'analyse typologique des signalements des victimes et aide à déterminer les tendances et les pratiques des criminels. Les plateformes peuvent aussi proposer des ressources utiles en matière de prévention des CF et d'aide aux victimes.

Encadré 21. Action Fraud au Royaume-Uni

Action Fraud est le centre national chargé d'enregistrer les fraudes et les cybercrimes au Royaume-Uni. Il constitue un point de contact central en matière de fraude et de crime sur Internet imputables à des motifs financiers et il est dirigé par les corps policiers de la ville de Londres, aux côtés du National Fraud Intelligence Bureau (NFIB). Le site Web d'Action Fraud présente diverses ressources pour sensibiliser la population à la prévention de la criminalité ainsi qu'à la protection et au soutien des victimes.

Action Fraud gère aussi un portail en ligne permettant aux victimes de signaler directement une fraude en tout temps. Les signalements d'Action Fraud sont transmis au NFIB, qui effectue des évaluations et des analyses dans différentes régions du pays pour déterminer les principaux auteurs des crimes. Les signalements sont ensuite communiqués aux corps policiers locaux appropriés du Royaume-Uni aux fins d'enquête. Le NFIB utilise aussi ces signalements pour désactiver des comptes bancaires, des sites Web et des numéros de téléphone utilisés par les fraudeurs.

Source : Royaume-Uni

Déclarations d'opérations douteuses

53. Étant donné la probabilité qu'il y ait une sous-déclaration par les victimes, les DOD sont une source de renseignements indépendante et essentielle pour détecter les flux financiers liés aux CF.

54. Selon les données recueillies auprès des CRF, la plupart des DOD liées aux CF ont été réalisées par le secteur bancaire. Néanmoins, les banques devraient continuer de renforcer leurs capacités de détection des CF et du BC connexe, puisque les syndicats de la CF améliorent continuellement leur modus operandi. Les données ont aussi révélé que les services de transmission de fonds ou de valeurs (STFV) et les FSAV soumettent peu de DOD. C'est peut-être dû au fait que dans certaines administrations, le secteur des FSAV n'est pas entièrement réglementé conformément aux normes du GAFI[20].

55. Il est important d'assurer une analyse rapide des DOD liées aux CF compte tenu de

[20] Voir aussi GAFI (juin 2023) *Virtual Assets : Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* [en anglais seulement].

la dispersion possible des produits des CF. Certaines CRF mettent en œuvre un système de hiérarchisation pour parcourir le grand nombre de DOD reçues et se concentrer sur celles qui présentent les risques les plus élevés, ce qui comprend les DOD liées aux CF. D'autres offrent de la formation aux agents de leur CRF sur les risques de BC liés aux CF, les aidant ainsi à filtrer et à classer les DOD reçues liées aux CF. Toutes ces mesures favorisent une analyse rapide par les CRF, ce qui permet aux organismes d'application de la loi de faire rapidement le suivi des incidents concernant des CF.

Encadré 22. Priorisation et regroupement des DOD liées aux CF

La CRF du Chili a reçu plus de 1 500 DOD de 2021 à 2022 relativement à un modèle de fraude utilisant une plateforme de négociation en ligne. Pour gérer ce volume de déclarations, la CRF a appliqué des techniques de regroupement aux fins d'analyse et certaines tendances ont été observées dans ces DOD.

La CRF s'est servie d'un outil d'exploration de texte utilisant des mots clés et des phrases connues détectés. Des regroupements géographiques ont ensuite été déterminés, ce qui a permis de transmettre une présentation ciblée et combinée au Bureau du procureur public. Le regroupement a permis de découvrir, pendant les enquêtes, que les fonds étaient retirés ultérieurement en utilisant des GAB, puis versés à une personne occupant des fonctions à un niveau hiérarchique supérieur au sein de l'organisation criminelle organisée.

Source : Chili

56. En plus de renforcer la détection, les administrations s'efforcent aussi d'augmenter la sensibilisation et d'améliorer le signalement. De nombreuses administrations ont publié une forme ou une autre de lignes directrices en matière de CF ou ont organisé des séminaires de formation pour le personnel des banques et d'autres secteurs afin de promouvoir la sensibilisation aux plus récentes tendances en matière de CF et aux typologies du BC dans l'ensemble de l'industrie. Veuillez aussi consulter l'annexe A pour obtenir une compilation des indicateurs de risques pouvant aider à améliorer la détection des CF. Les CRF d'autres administrations ont conçu des documents d'analyse stratégique sur les CF. Ces initiatives visent à renforcer la détection et la prévention des CF et des activités liées au BC par le personnel de première ligne des banques, etc.

Encadré 23. Analyse stratégique sur les mules liées aux CF

Une analyse stratégique de la CRF de l'Espagne était axée sur la compréhension d'un nouveau profil de mule financière : des comptes bancaires avaient été ouverts par une seule personne dans au moins trois institutions financières dans un délai de 20 jours. En mettant à profit des renseignements recueillis entre décembre 2020 et février 2022 tirés du registre des comptes bancaires, l'étude a permis de découvrir près de 40 000 autres comptes bancaires liés à environ 10 000 individus. Au total, 15 % des comptes bancaires ciblés ont obtenu des correspondances dans les bases de données de la CRF de l'Espagne. Ces comptes ont été associés à un risque élevé et une étude pilote a été lancée en collaboration avec quatre institutions financières pour mieux comprendre le profil de risques fondé sur ces comptes.

Le projet pilote visait à prévenir les CF et d'autres fraudes possibles ainsi qu'à améliorer la collaboration avec le secteur privé. Il visait aussi à renforcer la capacité des institutions financières à détecter les lacunes de leurs systèmes et à obtenir plus de renseignements sur les CF pour détecter et prévenir d'autres crimes. Finalement, le projet pilote a aussi mené à la mise en œuvre d'un système de contre-vérification utilisant le registre des comptes bancaires pour détecter de façon proactive les réseaux de BC liés aux CF.

Source : Espagne

4.2. Coordination et collaboration à l'échelle nationale

Coordination entre les autorités compétentes

57. Étant donné la nature transversale des CF, une solide coordination entre les organismes est clairement nécessaire à l'échelle nationale. Certaines administrations ont adopté une approche stratégique pangouvernementale de la coordination qui oriente leurs politiques en matière de CF. Elle comprend un organisme interfonctionnel général, composé de ministres clés des secteurs de la justice, de l'application de la loi, de la réglementation et des infocommunications. L'approche coordonnée permet aux administrations de cibler les principales vulnérabilités et de concevoir des interventions globales en matière de politique dans les secteurs clés.

58. La coordination nationale des opérations peut aussi impliquer des organismes techniques pour favoriser la détection et les enquêtes, y compris ce qui suit.

- Concevoir des méthodes de communication entre les CRF, les corps policiers et les poursuivants pour garantir des signalements centralisés, un échange de renseignements et de données probantes rationalisé et l'adoption de directives pour geler et saisir les avoirs. Il est aussi possible d'utiliser le triage automatisé des données pour faciliter l'identification des affaires qui pourraient être intéressantes et rapidement déterminer un OAL approprié pour mener l'enquête. Une telle coordination limiterait aussi le dédoublement des efforts d'application de la loi, puisque les criminels qui s'adonnent aux CF peuvent cibler des victimes dans différentes parties d'une administration (voir la section sur la définition appropriée des responsabilités ci-dessous).
- Faire appel à des experts techniques en cybercriminalité, particulièrement en ce qui a trait aux intrusions dans les réseaux et à d'autres crimes liés aux infrastructures techniques, et à des organismes de protection de la vie privée. Cette approche reflète les multiples facettes des CF ainsi que la pertinence des preuves judiciaires numériques (comme les adresses IP, les identifiants liés à des domaines Internet, etc.) pour identifier les syndicats de la CF et approfondir les enquêtes sur le BC.

Encadré 24. Centre conjoint de coordination de la lutte contre la cybercriminalité

La police fédérale australienne (PFA) dirige le centre conjoint de coordination de la lutte contre la cybercriminalité (JPC3 pour Joint Policing Cybercrime Coordination Centre). Les membres du JPC3 comprennent des organismes d'application de la loi fédéraux et d'État, des analystes du gouvernement, y compris l'Australian Transaction Reports and Analysis Centre (AUSTRAC), et des partenaires de l'industrie, comme des analystes de banques australiennes. Le JPC3 :

- coordonne la réponse des corps policiers australiens aux cybercrimes à dommages importants et très fréquents afin d'optimiser l'incidence sur le milieu criminel;
- améliore l'échange de renseignements et l'établissement de cibles pour l'ensemble des corps policiers et de l'industrie du Commonwealth, des États et des territoires;
- coordonne les groupes de travail communs avec les partenaires des corps policiers et de l'industrie pour lutter contre les menaces prioritaires liées à la cybercriminalité;
- assure la coordination nationale des efforts de renforcement des capacités grâce à la polyvalence des compétences, à une formation conjointe et à l'élaboration d'outils de collaboration;
- communique des activités médiatiques, de prévention et de sensibilisation uniformes à l'échelle nationale à l'industrie et au public.

Le JPC3 a une capacité de prévention qu'il utilise de concert avec l'industrie et le domaine public pour lutter contre le cybercrime. Pour soutenir efficacement le JPC3, l'AUSTRAC dispose aussi d'une équipe responsable de la cybercriminalité financière, qui se concentre précisément sur la fourniture de renseignements financiers concernant les cybercrimes et la cybercriminalité liés aux finances, y compris le BC découlant de cyberfraudes.

En janvier 2020, la PFA a mis sur pied l'opération DOLOS, un groupe de travail multiorganisme dirigé par la PFA[1] qui lutte contre les cybercriminels transnationaux qui s'adonnent à la compromission de messageries d'affaires ou en facilitent la compromission. Les participants à l'opération DOLOS travaillent avec des Australiens et de petites ou moyennes entreprises qui ont été victimes de BEC et perturbent le flux des produits en provenance et à destination des syndicats du crime. Depuis le début de l'opération DOLOS, le groupe de travail a élaboré de nouvelles techniques qui ont mené à une réduction des préjudices pour les Australiens et les entreprises.

Du 1er juillet 2022 au 30 juin 2023, l'opération DOLOS a empêché la perte de plus de 30,6 millions de dollars australiens par des victimes australiennes et internationales en interrompant le modèle d'opérations financières utilisé par les criminels.

Source : Australie

1 Le groupe de travail comprend différents corps policiers d'État et de territoire, des organismes de renseignement et de cybersécurité, la CRF ainsi que le secteur financier.

Partenariats opérationnels avec le secteur privé

59. Les administrations ont aussi cherché à collaborer avec le secteur privé dans le cadre de partenariats public-privé (PPP). Ces PPP peuvent aider à renforcer les efforts de détection, à cerner les réseaux de BC cachés grâce à l'échange de renseignements tactiques et à améliorer la réponse opérationnelle en vue de récupérer les avoirs.

Encadré 25. Projet : Interventions rapides pour prévenir les arnaques

La CRF du Sri Lanka a lancé un projet, appelé Rapid Actions to Prevent Scams (RAPS), visant à agir immédiatement lorsqu'une victime signale une possible CF. Son objectif est d'interrompre les arnaques dans le système financier sri lankais, y compris les CF, en réunissant les agents de la CRF et les agents de conformité des IF pour détecter rapidement les activités illicites sur les comptes utilisés par les criminels et leurs complices.

Le mécanisme nécessite l'identification des authentifiants des fraudeurs en fonction des plaintes reçues du public et ces authentifiants sont ensuite communiqués aux agents de la conformité des IF. En se fondant sur cette information, les IF surveillent les activités des comptes des fraudeurs potentiels et prennent des mesures appropriées afin d'interrompre l'utilisation du système financier pour prévenir toute fraude. En outre, les renseignements sur les fraudeurs sont communiqués aux corps policiers du Sri Lanka pour qu'ils enquêtent sur le sujet.

Source : Sri Lanka

60. Compte tenu de l'augmentation considérable des CF et des risques de BC connexes, de nombreuses administrations ont établi des centres d'intervention centralisés chez des OAL ou des organismes de réglementation afin d'intensifier les mesures visant à lutter contre les CF et à sensibiliser la population (voir aussi la section sur les unités spécialisées dans la lutte contre les CF ci-dessous). En bonne pratique, les représentants des IF et les FSAV pourraient partager des bureaux dans ces centres d'intervention centralisés, ce qui favoriserait un accès presque instantané aux données financières et le suivi entre les multiples entités et secteurs financiers et permettrait aux autorités compétentes d'intercepter et de geler les fonds plus rapidement.

Encadré 26. Partage des locaux par les agents des banques

L'Arabie saoudite a mis sur pied une salle des opérations conjointes (SOC) à l'intention des banques. La SOC a pour tâche de faire le suivi et de surveiller les cas de fraude financière auxquels les clients des banques peuvent être exposés. La SOC rassemble toutes les banques et les institutions financières connexes sous une même enseigne pour s'attaquer aux cas de fraude financière confirmés.

La SOC est gérée par les banques d'Arabie saoudite pour faciliter les efforts conjoints dans un souci de stabilité du secteur bancaire. La SOC fonctionne 24 heures sur 24, 7 jours sur 7 et vise à assurer une coopération et une intégration promptes et efficaces entre toutes les banques saoudiennes pour limiter la multiplication des cas de fraude et réagir rapidement aux plaintes pour fraude et, lorsque c'est possible, prendre des mesures immédiates pour éviter les actes frauduleux.

Source : Arabie saoudite

61. Ces partenariats constituent aussi une plateforme utile pour échanger des pratiques exemplaires et des typologies communes ainsi que pour concevoir conjointement des mesures recommandées pour interrompre les activités illicites.

Encadré 27. Partenariat public-privé de renseignement financier d'Europol

Le partenariat public-privé de renseignement financier d'Europol (EFIPPP) est le premier mécanisme public-privé de partage de renseignements transnational pour la LBC/LFT. L'EFIPPP regroupe des organismes d'application de la loi, des CRF et des entités privées de différents pays appartenant ou non à l'Union européenne (UE).

Le groupe de travail sur les menaces et les typologies de l'EFIPPP a consacré ses travaux à différents sujets liés aux CF et aux divers modus operandi, y compris la BEC, la fraude en matière d'investissement, les comptes de mule, les IBAN virtuels et les cryptoactifs. Même si le but de l'EFIPPP est de concevoir des rapports de typologies stratégiques, il constitue aussi une plateforme pour discuter de la facilitation de la coopération entre ses membres.

Source : Europol

62. La composition des PPP peut varier. Beaucoup d'administrations sont toujours axées sur les intervenants traditionnels (en particulier les banques et les autres institutions financières), mais on observe une participation accrue des EPNFD, des FSAV et d'autres secteurs non traditionnels (comme les exploitants d'entreprises de télécommunications et les fournisseurs de services Internet). La composition précise dépend des buts et des objectifs du PPP.

Encadré 28. Coopération avec le secteur des télécommunications

Dans les dernières années, la Chine n'a cessé de promouvoir le renforcement de la lutte contre les fraudes utilisant le réseau de télécommunications et leur gestion. Le 1er décembre 2022, elle a officiellement adopté une loi antifraude sur le réseau de télécommunication de la République populaire de Chine, qui a imposé de solides mécanismes de protection de l'état de droit pour contrer et réprimer les activités criminelles liées aux fraudes utilisant le réseau de télécommunications, ce qui a permis de réduire efficacement les actes criminels connexes.

La loi réunit des autorités du secteur privé (y compris des organismes d'application de la loi ainsi que des organismes financiers, de télécommunications et d'information sur Internet), de même que des IF (banques et fournisseurs de services de paiement autres que des banques), des exploitants d'entreprises de télécommunications et des fournisseurs de services Internet pour mettre en place un système d'alerte rapide et de dissuasion. Ce système cible les victimes potentielles en envoyant rapidement un avertissement, permettant ainsi de prendre des mesures dissuasives appropriées en temps opportun.

Les IF peuvent aussi utiliser ce système lorsqu'elles ouvrent des comptes bancaires, des comptes de paiement et lorsqu'elles offrent des services de paiement et de règlement. Le système est utilisé pour améliorer les processus de diligence raisonnable à l'égard de la clientèle et permet aux IF de prendre des mesures d'atténuation des risques pour empêcher que les comptes bancaires, de paiement, etc., soient utilisés pour des activités frauduleuses.

Source : Chine

4.3. Stratégies nationales d'application de la loi efficaces

63. La présente section examine certaines bonnes pratiques et stratégies d'application de la loi efficaces utilisées par les administrations. En général, ces stratégies mettent à profit les sources d'information susmentionnées à la section 4.1 pour identifier les CF et le BC connexe, enquêter sur ceux-ci et les prévenir plus efficacement.

64. Ces stratégies d'application de la loi efficaces impliquent généralement de multiples organismes et entités du secteur privé. Cela signifie qu'une coordination et une coopération nationales solides sont habituellement nécessaires pour mettre en œuvre ces stratégies (comme indiqué dans la section 4.2 ci-dessus).

Définition appropriée des responsabilités

65. Bon nombre d'administrations ont signalé une augmentation du montant des pertes et du volume des cas de CF dans les dernières années. Bien que certaines affaires se soient soldées par de petites pertes, le volume de ces arnaques fait que les produits totaux de la criminalité accumulés par chaque syndicat du crime sont potentiellement élevés.

66. Plusieurs administrations ont indiqué que l'important volume de signalements de CF rend inévitable la définition des responsabilités en matière d'enquête. À titre de bonne pratique, les administrations comprenant différents organismes de lutte contre les fraudes et les cybercrimes qui surveillent les cas de CF ont cherché à identifier les autorités compétentes pour gérer ces dossiers. D'autres administrations ont adopté des lois pour mettre en commun les enquêtes complexes impliquant de nombreuses victimes d'un même syndicat du crime, de façon à ce qu'une seule autorité compétente supervise la totalité de l'enquête. Ces initiatives préviennent le dédoublement des efforts des différentes autorités compétentes et empêchent que certaines affaires « tombent dans les mailles du filet », et elles tiennent compte de la nature transnationale des crimes.

Encadré 29. Utilisation de la technologie pour définir la responsabilité des enquêtes

La Force de police de Hong Kong (FPHK) a mis en place un centre de traitement et d'analyse de la cybercriminalité (e-Hub) en septembre 2022 dans le but d'améliorer l'efficacité de la gestion des rapports concernant des crimes axés sur la technologie et des fraudes. L'e-Hub utilise un système informatique amélioré pour effectuer des analyses de corrélation sur des types courants de cyberfraudes et déterminer des groupes d'affaires.

En 2022, le nombre de cas de fraude a augmenté de 45,1 % pour atteindre 27 923 cas, ce qui représente près de 40 % de tous les crimes. Près de 80 % des cas de fraude étaient liés à des CF. Un plus grand nombre de personnes signalent des CF sur Internet et la plupart des cas signalés en ligne sont reliés, par exemple, en étant l'œuvre de la même organisation criminelle. Les cas reliés sont assignés à une seule équipe d'enquête pour les enquêtes consolidées, afin que les ressources soient mieux coordonnées.

En utilisant des algorithmes de groupement, e-Hub peut cerner des tendances et des similitudes dans les données qui ne sont pas toujours évidentes à première vue pour mieux comprendre la portée et la nature des cas. Le centre se sert notamment des types d'outils numériques et des comptes de mules financières utilisés par les criminels ainsi que des méthodes de planification, d'exécution et de dissimulation des CF.

Source : Hong Kong, Chine

Unités spécialisées dans la lutte contre les CF et le BC connexe

67. Dans le but de renforcer les capacités en matière de LBC/LFT devant l'évolution du milieu criminel, bon nombre d'administrations ont mis en place une unité ou un groupe de travail particulier pour enquêter sur les CF et le BC connexe. Ces administrations ont affecté des ressources additionnelles au renforcement des capacités liées aux enquêtes financières, à la collecte de renseignements et à la formation pour les OAL et à l'acquisition de capacités dans le secteur privé. Ces unités centralisées réunissent l'expertise en matière de lutte contre les CF des organismes d'application de la loi et les rendent plus aptes à interrompre les activités de CF, à localiser les fonds blanchis et à recouvrer les produits connexes.

68. Les administrations ont indiqué que les avantages de tels groupes sont multiples. Ce regroupement de toutes les affaires de CF par une seule unité d'application de la loi permet une analyse globale, un déploiement des analyses de données et une analyse des liens entre les réseaux plus efficaces pour identifier les syndicats du crime. Ces unités peuvent aussi servir de point de contact unique pour les intervenants du secteur privé et les homologues étrangers et elles aident à établir des relations stratégiques à long terme. Cette approche améliore les efforts d'intervention des organismes d'application de la loi, comme le débranchement de lignes téléphoniques et le retrait de publicités et de pseudonymes suspects en ligne, et donne de meilleurs résultats au chapitre du recouvrement des avoirs.

Encadré 30. Centre national d'intervention en cas de fraude

Le centre national d'intervention en cas de fraude (NSRC pour National Scam Response Centre) de la Malaisie est une intervention en plusieurs volets regroupant un éventail de ressources et d'experts provenant du centre national de lutte contre les crimes financiers, de la Police royale malaisienne (PRM), de la banque centrale et d'autres entités des secteurs public et privé.

Le NSRC sert de plateforme centrale pour les renseignements sur les fraudes reçus de diverses sources et mise sur des analyses de réseaux pour identifier les réseaux de mules et de blanchiment de capitaux. Des entités du secteur privé, y compris des institutions financières, localisent les fonds, niveau après niveau, et restreignent l'accès aux comptes de mules. La PRM enquête ensuite sur les affaires et prend des mesures d'application de la loi, comme l'émission d'une ordonnance de gel des comptes.

Source : Malaisie

Amélioration de l'accès aux renseignements financiers

69. En raison du grand nombre et des effets instantanés des cas de CF, un accès rapide aux renseignements financiers et bancaires est essentiel pour accélérer les enquêtes et la localisation des produits des CF. Certaines administrations ont utilisé des technologies pour tenir compte du flux rapide des produits des CF, en collaborant fréquemment avec le secteur privé pendant le processus. D'autres s'appuient sur des registres centraux ou conçoivent des bases de données pour rationaliser le processus de collecte de renseignements. Ces bonnes pratiques sont généralement fondées sur la création d'une plateforme centralisée qui regroupe de multiples intervenants pour un échange de renseignements accéléré.

- **Cueillette de renseignements fondée sur la technologie :** Pour permettre aux institutions financières de fournir rapidement les renseignements pertinents pour l'application de la loi, il peut être utile que les autorités compétentes au sein d'une administration s'entendent sur les champs de données pertinents dans le cadre de leurs enquêtes. La présentation de demandes variées nécessitant chacune une réponse personnalisée de l'institution financière concernée peut être un processus fastidieux pour le secteur privé. À titre de bonne pratique, les organismes d'application de la loi de certaines administrations ont conçu un modèle normalisé comprenant des champs de données convenus à l'avance que doivent remplir les institutions

financières. Les demandes peuvent ensuite être regroupées et transmises aux institutions financières en lots et dans un format informatisé. Les institutions financières peuvent aussi répondre aux demandes légitimes des organismes d'application de la loi par voie électronique, ce qui permet une analyse plus efficace des données.

Encadré 31. Mettre à profit l'automatisation robotisée des processus pour accélérer l'accès aux documents financiers détenus par les institutions financières

Il est essentiel de pouvoir accéder rapidement aux renseignements bancaires et financiers pour une interception et un recouvrement efficaces des avoirs. Singapour mise sur l'automatisation robotisée des processus (ARP) pour obtenir des renseignements bancaires en une fraction du temps requis auparavant. Les ordres sont désormais transmis aux banques par voie électronique en utilisant un modèle normalisé. Les banques automatisent le processus de récupération des renseignements financiers, puis les renvoient aux OAL par voie électronique. L'OAL peut aussi utiliser immédiatement les données électroniques aux fins d'analyse.

Le processus a amélioré le temps de traitement de 97 %, ce qui a aussi renforcé l'efficacité des enquêtes. L'information est maintenant communiquée sous forme numérique et prête pour les analyses. En ce qui concerne les banques, cette initiative a entraîné des économies importantes en éliminant le travail manuel. Elle a aussi permis l'exploration de données pour les banques grâce à ses processus automatisés, qui peuvent être utilisés pour détecter plus facilement les réseaux de BC cachés.

Source : Singapour

- **Suivi plus facile des actifs entre les IF :** Les transactions coup sur coup et les transferts rapides d'un compte à l'autre entre de nombreuses IF augmentent les efforts de suivi aux fins d'application de la loi, puisqu'il faut du temps pour recueillir de l'information auprès des IF respectives, examiner les différents niveaux de transactions et déterminer l'origine et la destination finale des fonds. Ce peut être difficile étant donné la vitesse des transactions. Parmi les bonnes pratiques se trouvent l'élaboration de plateformes afin de faciliter la localisation et l'échange de renseignements rapides entre les différentes IF dans le but d'intercepter les produits illicites.

Encadré 32. Système de signalement et de gestion des cyberfraudes financières des citoyens (CFCFRMS pour Citizen Financial Cyber Fraud Reporting and Management System)

Le CFCFRMS est un système en ligne conçu par le centre de coordination de la cybercriminalité de l'Inde pour signaler rapidement les cyberfraudes financières et empêcher la circulation des produits de la fraude dans les différents secteurs financiers. Le système a intégré les OAL dans l'ensemble du pays et dans certaines entités financières (p. ex. banques, portefeuilles, agrégateurs de paiement, passerelles de paiement, plateformes de commerce en ligne, etc.) pour qu'ils puissent travailler de concert et réagir immédiatement aux plaintes signalées dans le CFCFRMS. Actuellement, tous les OAL d'État et sur le territoire de l'Union et 243 entités financières utilisent le module.

Lorsqu'une victime signale une fraude à un OAL, les renseignements sur le bénéficiaire de la transaction frauduleuse sont soumis et consignés dans le système CFCFRMS sous forme de billet. Le billet est transmis à l'entité financière visée (banque, solution de paiement, portefeuille, etc.), qui verra apparaître le billet dans le tableau de bord du système. L'entité examinera si les sommes soutirées sont toujours dans le compte et gèlera le compte. Si l'argent a été envoyé à une autre entité, le billet est transmis à l'entité du prochain niveau. Le processus est répété jusqu'à ce que l'argent soit intercepté. Si l'argent a été retiré, les IF indiquent les renseignements concernant le retrait pour que les OAL puissent prendre d'autres mesures.

Le système a très efficacement aidé à empêcher que des fraudeurs mènent à bien des transactions frauduleuses. Depuis ses débuts en avril 2021, le système a permis d'intercepter plus de 6,02 milliards de roupies indiennes (environ 66,1 millions d'euros).

Source : Inde

- **Utilisation des registres centralisés :** Les registres bancaires centralisés permettent aux organismes d'application de la loi d'accéder rapidement à des renseignements bancaires de base et aident à accélérer les enquêtes sur les CF. L'information permet aux organismes d'application de la loi de vérifier dans quelles banques un suspect possède des comptes ou l'identité du titulaire d'un compte. Il est ainsi plus facile de rationaliser le processus de collecte d'information en permettant aux organismes d'application de la loi de déterminer plus rapidement la portée de leurs enquêtes et de se concentrer uniquement sur les institutions financières où le suspect possède des comptes.

Encadré 33. Identification de comptes de mules dissimulés

À Malte, une DOD a été remplie relativement à une mule financière présumée après une série de transactions suspectes à différents bénéficiaires. Les fonds avaient été transférés vers différentes banques locales et internationales liées à une arnaque amoureuse présumée.

Des recherches dans le registre central des comptes bancaires national ont permis à la CRF d'identifier immédiatement un autre compte actif appartenant à la mule présumée dans une autre banque. La CRF a rapidement pu dresser un portrait global et déterminer la portée de l'analyse financière additionnelle requise. De cette manière, la CRF a pu déterminer rapidement des points communs avec des cas de blanchiment d'argent impliquant d'autres individus à l'étranger.

Source : Malte

- **Élaboration de bases de données pour le partage de renseignements dans le secteur privé :** En ce qui concerne les réseaux de BC professionnels, bon nombre de comptes de mules peuvent avoir été ciblés ou soupçonnés dans le cadre d'arnaques antérieures (p. ex. arnaques amoureuses, de loterie et d'emploi) ou d'activités liées à l'usurpation d'identités. On constate aussi des chevauchements similaires entre les données et les processus utilisés pour identifier les fraudes et ceux servant à identifier les réseaux de mules. À titre de bonne pratique, certaines administrations ont cherché à centraliser les données qui se retrouvent dans les bases de données antifraude et anti-blanchiment de capitaux afin de cibler les réseaux de BC plus étendus au sein des différentes IF pour prévenir les fraudes et favoriser le recouvrement des avoirs.

Encadré 34. Base de données centralisée dans le secteur privé

Le Brésil a récemment approuvé une résolution rendant obligatoire la création d'une base de données centralisant les renseignements concernant les fraudes (y compris les tentatives) pour toutes les institutions financières et de paiement. Cette base de données est gérée par la Banco Central do Brasil (BCB) et devrait être fonctionnelle en novembre 2023.

La résolution prévoit que le partage de renseignements concernant les fraudes (y compris les tentatives) est obligatoire pour les institutions et détermine l'information minimale à partager. Elle oblige notamment à communiquer les noms des personnes impliquées dans la perpétration de fraudes (y compris les mules financières), la ou les institutions financières impliquées et le ou les comptes utilisés. Le système vise à faciliter le partage de renseignements dans le secteur privé afin de lutter contre les fraudes et de les éviter ainsi que de recouvrer les produits illicites de ces fraudes.

Source : Brésil

Décourager les mules financières

70. Comme mentionné précédemment, les mules financières jouent un rôle important dans les réseaux de BC liés aux CF. Les mules sont recrutées de diverses façons. Selon la méthode de recrutement utilisée et si elles ont été involontairement trompées ou exploitées, les mules peuvent posséder différents niveaux de connaissance du système de cyberfraude et de participation à celui-ci (voir la section 2.3 ci-dessus).

71. Par conséquent, les autorités compétentes peuvent éprouver des difficultés à porter des accusations pour blanchiment de capitaux. Il peut être difficile de trouver des preuves suffisantes pour démontrer l'intention criminelle d'une mule de blanchir des capitaux (c.-à-d. le degré de conscience de sa participation au processus de blanchiment). Pour pallier ce problème, certaines administrations ont adopté des lois visant à réduire le degré d'intention criminelle requis en cas d'infraction de BC, par exemple de « connaissance du fait » à « soupçon ».

Encadré 35. Paragraphe 9(3) de la Convention de Varsovie du Conseil de l'Europe

Un des problèmes sous-jacents des poursuites efficaces en cas d'infraction de BC est l'obligation de prouver l'intention criminelle, c.-à-d. que le blanchisseur d'argent savait que les produits traités étaient des produits de la criminalité. Dans les cas de BC complexes auxquels participent des blanchisseurs de capitaux professionnels, les défendeurs nient souvent avoir eu réellement conscience que les fonds qu'ils géraient étaient des produits de la criminalité. Par conséquent, la démonstration que « l'élément moral » du défendeur a atteint le seuil requis est une des tâches les plus difficiles en cas d'infraction de BC.

Conscients de la difficulté à prouver l'intention criminelle, les auteurs de la Convention de Varsovie ont intégré de nouveaux éléments à l'article 9, qui définit les infractions de BC. En plus des éléments faisant déjà partie de la Convention de Vienne et de la Convention de Palermo, le paragraphe 3 de l'article 9 de la Convention de Varsovie va plus loin en établissant que l'infraction de blanchiment a été commise, même lorsque l'auteur avait simplement des soupçons ou qu'il aurait dû être conscient que le bien constituait un produit de la criminalité.

Source : MONEYVAL

72. D'autres administrations ont abordé le défi posé par les mules financières de façon générale en mettant en œuvre des activités d'information et de sensibilisation de la population aux possibles mules. Des campagnes mondiales sur les médias sociaux, comme #NeSoyezPasUneMule, avec l'appui d'Europol, et #VotreCompteVotreFaute d'INTERPOL, peuvent être des plateformes utiles pour coordonner la sensibilisation internationale à la lutte contre les activités des mules financières, en particulier lorsque les fonds peuvent être blanchis facilement par des mules au-delà des frontières. La collaboration avec le secteur privé peut maximiser l'effet et les résultats de ces efforts de sensibilisation. Les autorités peuvent aussi miser sur des mécanismes de détection existants (DOD et signalements de victimes) pour identifier des mules financières potentielles qui pourraient avoir géré des produits de CF. Une sensibilisation et des mises en garde ciblées peuvent inciter les mules potentielles à éviter de répéter de tels comportements dans le futur. Des documents sur d'anciennes activités de sensibilisation ou mises en garde peuvent être utilisés comme précieux éléments probants pour déterminer l'intention criminelle de blanchir des capitaux en cas de récidive.

4.4. Prévention et interruption

73. Compte tenu de la vitesse à laquelle les fonds sont disséminés, beaucoup d'administrations se sont efforcées d'examiner des initiatives permettant d'éviter la réalisation de CF et d'activités de BC connexes. Une telle approche limite la rentabilité globale pour les syndicats de la CF et réduit considérablement les ressources à mobiliser en aval, de l'enquête à la gestion des victimes.

Activités d'information et de sensibilisation de la population

74. Il est possible d'adopter une démarche préventive en éduquant la population et en renforçant la vigilance contre l'exploitation, y compris au moyen de campagnes de sensibilisation nationales préconisant la cyberlittératie. Pour appuyer cet objectif, certaines administrations ont tiré profit de la technologie pour déployer des campagnes d'information auprès des citoyens afin de les aider à détecter les opérations frauduleuses, de les sensibiliser aux signes révélateurs et d'encourager le signalement des victimes.

Encadré 36. Utilisation de la technologie pour renseigner la population sur la CF

La Force de police de Hong Kong (FPHK) a lancé un moteur de recherche unique sur les arnaques et les pièges, appelé « Scameter » en septembre 2022. L'application vise à aider la population à identifier les fraudes et les pièges en ligne.

Lorsque les gens sont confrontés à des appels ou des vendeurs en ligne suspects, des demandes d'amitié non sollicitées, de messages de recrutement arbitraires, des sites Web d'investissement frauduleux louches, etc., ils peuvent indiquer dans Scameter le nom ou le numéro de compte, le numéro de compte de paiement, le numéro de téléphone, l'adresse courriel, l'URL, etc., des fraudeurs soupçonnés pour évaluer le risque de fraude et pour la cybersécurité.

Les données et les évaluations de Scameter proviennent de diverses sources fiables, y compris de signalements aux corps policiers, de renseignements fournis par des organismes, d'une base de données sur les numéros de téléphone suspects, ainsi que des analyses de bases de données et en temps réels d'entreprises de sécurité informatique.

Source : Hong Kong, Chine

Sécurité antifraude et contrôle des résultats de la LBC/LFT

75. Les expériences des secteurs public et privé commencent à montrer que les processus antifraude et de LBC sont complémentaires. Ils comprennent, notamment, l'utilisation de la technologie pour aider les utilisateurs à rejeter automatiquement les messages frauduleux reçus, la collaboration avec le secteur privé aux fins d'analyse prospective afin d'atténuer de manière proactive les nouvelles tendances en matière de fraude, la création de dispositifs de sécurité, de contrôles et de règles ainsi que de messages de mise en garde dans les logiciels antivirus relativement à de possibles sites d'hameçonnage (voir l'annexe B, qui présente de bons exemples de la façon dont les organismes de réglementation financière ont adopté des exigences antifraude en plus de contrôles pour la LBC/LFT).

76. Une autre bonne pratique encourage les IF à adopter des mesures de surveillance en temps réel des transactions pour identifier et prévenir les activités frauduleuses ou illicites en temps réel. En surveillant les renseignements anormaux sur les titulaires de comptes (p. ex. adresses physiques, IP et courriel, numéros de cellulaire, etc.) et les transactions en temps réel, les IF peuvent rapidement identifier les activités inhabituelles ou suspectes, enquêter sur celles-ci et les signaler.

77. La surveillance en temps réel des transactions, qui implique l'utilisation de logiciels et d'algorithmes sophistiqués pour surveiller les transactions financières, est jugée utile pour détecter et prévenir les CF. Étant donné le surplus d'information causé par la numérisation, les CF peuvent être difficiles à détecter par des procédés manuels. La surveillance des transactions en temps réel peut aider les IF à déterminer les modèles d'activités suspectes entre de multiples comptes et transactions, à enquêter sur ceux-ci, même si ces comptes ou transactions ne sont pas directement reliés, et à prévenir de futurs crimes[21].

Élimination des instruments des criminels

78. Comme des secteurs non traditionnels peuvent aussi commettre des CF (voir la section 3.3 ci-dessus), certaines administrations ont renforcé les mesures de prévention et de contrôle antifraude dans ces secteurs, ce qui implique, notamment, de cibler les instruments des CF, notamment en coupant les lignes de téléphone mobile et en fermant les pages Web utilisées par des criminels, en filtrant les messages d'hameçonnage et les liens vers des sites Web malveillants, etc.

Encadré 37. Fermeture de sites Web suspects et de campagnes d'hameçonnage

En Arabie saoudite, les organismes d'application de loi et les autorités de réglementation adoptent une approche coopérative avec les fournisseurs de services de télécommunication visant à améliorer leur capacité à prédire, prévenir et détecter les événements frauduleux et à y réagir efficacement. Pour lutter contre les instruments des criminels, l'autorité nationale de cybersécurité de l'Arabie saoudite a imposé des exigences de protection très strictes axées sur la lutte contre les sites Web clonés et les messages d'hameçonnage sur les plateformes de médias sociaux. De plus, la banque centrale de l'Arabie saoudite (SAMA) a mis en place de solides cadres de cybersécurité et de lutte contre la fraude, qui décrivent les exigences de base obligatoires en matière de contrôle pour les entités réglementées. Ce cadre vise à lutter de façon proactive contre les nouvelles menaces liées aux fraudes pour garantir la stabilité et la protection du secteur financier du Royaume d'Arabie saoudite.

Un aspect essentiel de ces exigences réglementaires nationales est la surveillance proactive des instruments des criminels par les organismes. Elle implique une surveillance continue des possibles activités frauduleuses, notamment à l'aide de campagnes sur les sites Web suspects et l'hameçonnage grâce à des technologies de pointe et des mesures de protection des marques mises en œuvre par les organismes. Lorsqu'elles sont détectées, ces activités sont rapidement signalées aux autorités pertinentes. Un signalement en temps opportun assure une intervention rapide pour enquêter et interrompre les opérations criminelles, empêchant d'autres préjudices et réduisant les conséquences des activités frauduleuses.

Source : Arabie saoudite

[21] Pour de plus amples renseignements sur la façon d'utiliser les technologies pour la LBC/LTF, voir aussi GAFI (juillet 2021), *Opportunities and Challenges of New Technologies for AML/CFT* [en anglais seulement].

Lutte contre la dissipation des actifs

79. De nombreuses administrations ont constaté qu'un des aspects les plus complexes des enquêtes sur les CF est la vitesse à laquelle les produits de la CF peuvent être blanchis. Elles s'entendent pour dire qu'il est primordial que les autorités compétentes puissent intervenir rapidement pour recouvrer les produits des CF avant qu'ils disparaissent des différents comptes bancaires. Les administrations ont mis en œuvre diverses mesures pour récupérer plus efficacement les actifs liés aux CF (voir la section 5.1 ci-dessous).

80. Il peut aussi y avoir des avantages à embaucher des représentants clés du secteur financier privé pour faciliter et encourager l'interception proactive des fonds illicites par ces représentants après qu'ils ont reçu un avis de fraude d'un client victime et avant que les autorités compétentes aient communiqué avec eux. Cette approche prévoit l'échange de renseignements entre les IF ou les FSAV nationaux et internationaux (voir aussi l'encadré 41 ci-dessous).

Encadré 38. Bulletin du Groupe Egmont sur la fraude de compromission de messagerie d'entreprise (BEC)

En juillet 2019, le Groupe Egmont a diffusé un bulletin pour alerter les CRF membres et leurs administrations de la menace croissante associée aux fraudes de BEC en partageant des scénarios clés et des indicateurs de risque liés à la BEC. Le bulletin décrivait aussi comment les institutions financières (IF) peuvent jouer un rôle important dans l'identification, la prévention et le signalement des fraudes par BEC en favorisant des communications et une collaboration améliorées entre les unités internes opérationnelles, de LBC, de prévention des fraudes et de cybersécurité.

Pour faciliter l'enquête sur les incidents de BEC et le recouvrement des fonds des victimes, les IF bénéficiaires qui avaient reçu de l'information à savoir qu'un transfert frauduleux avait été effectué vers le compte d'un de leurs clients (p. ex. message de rappel sur le réseau SWIFT) ont été informées de n'effectuer aucune transaction pouvant entraîner la perte de fonds et de communiquer avec un organisme d'application de la loi ou la CRF pour évaluer la validité de la transaction demandée.

Source : Groupe Egmont

5. Collaboration internationale et recouvrement des avoirs

81. Comme indiqué précédemment, l'administration où survient la CF (c.-à-d. où se trouve généralement la victime) diffère souvent de l'administration où sont blanchis les produits. Cette situation peut compliquer les enquêtes transfrontalières et nuire à l'efficacité de la collaboration internationale pour obtenir de l'information et des données probantes, démanteler les syndicats de la CF et récupérer les produits illicites. Par exemple, une administration où des produits de CF ont été blanchis peut avoir de la difficulté à identifier toutes les victimes associées à un compte utilisé pour le BC, puisqu'elles peuvent être dispersées dans différentes administrations.

82. La nature décentralisée des CF s'ajoute à la complexité de la situation. Les priorités en matière de collaboration internationale respectives des administrations ne concordent pas toujours. Par exemple, dans les cas où les victimes de l'administration A transfèrent de l'argent à l'administration B, mais que les victimes de l'administration B se trouvent dans l'administration C (ce qui signifie que l'administration A pourrait prioriser sa collaboration avec l'administration B, mais que cette dernière prioriserait sa collaboration avec l'administration C). La nécessité de demander la participation de nombreux intervenants et partenaires étrangers, publics et privés, complexifie aussi l'identification et la localisation des fonds illégaux.

    - Les syndicats qui s'adonnent aux CF utilisent diverses catégories de services et d'actifs financiers. Les transactions peuvent être réalisées presque instantanément à l'étranger entre différents fournisseurs et secteurs, ce qui complique le suivi et l'imputation des transferts de fonds.

    - Des preuves judiciaires numériques pertinentes sont aussi susceptibles d'être communiquées dans les différentes administrations, ce qui complique la tâche de dresser un portrait complet du fonctionnement et des méthodes de blanchiment des produits des syndicats du crime. C'est encore plus difficile en raison de la volatilité des preuves judiciaires numériques, qui peuvent facilement disparaître si elles ne sont pas protégées rapidement.

83. Il faut habituellement beaucoup de temps pour mettre en place une collaboration officielle, y compris sur le plan de l'entraide judiciaire. Étant donné la nature rapide des crimes numériques et des activités de BC connexes (dont les éléments de preuve peuvent disparaître rapidement s'ils ne sont pas protégés), le fait de se fier à une collaboration officielle peut donc s'avérer beaucoup moins efficace. Pour demeurer aptes à offrir une aide transfrontalière afin de lutter efficacement contre les activités criminelles liées aux CF, les autorités compétentes font de plus en plus appel à des mécanismes de coopération informels en partageant directement leurs renseignements avec leurs homologues étrangers. Cela peut se produire à l'échelle des organismes d'application de la loi ou des CRF en utilisant différentes méthodes, notamment le site Web sécurisé du Groupe Egmont, l'outil I-24/7 d'INTERPOL ainsi que d'autres réseaux non officiels comme le Camden Asset Recovery Inter-Agency Network (CARIN) et les réseaux interinstitutionnels de recouvrement des avoirs (ARIN) régionaux.

Encadré 39. Interception des produits des CF grâce à des réseaux multilatéraux informels

Pour lutter contre l'augmentation des CF, les autorités françaises chargées des enquêtes ont exploité activement des réseaux informels, dont le sous-réseau des bureaux de recouvrement des avoirs (BRA) européen du Camden Asset Recovery Inter-agency Network (CARIN), afin de mettre en place une collaboration internationale et un recouvrement des avoirs connexes efficaces. Le bureau de recouvrement des avoirs français collabore étroitement avec les membres de ces deux réseaux, ce qui permet l'échange rapide d'information entre les homologues des OAL et des CRF de nombreuses administrations qui se spécialisent dans la localisation, la saisie et la confiscation des avoirs d'origine criminelle, en particulier dans les cas urgents où une réponse aux demandes est fournie dans un délai de huit heures. Une telle coopération permet de protéger rapidement les fonds dans le compte de destination ciblé au départ et les comptes de tous les autres niveaux par la suite.

Par exemple, en 2022, le BRA français a communiqué avec le BRA slovaque relativement à un transfert bancaire frauduleux de 1 875 000 € au détriment d'une entreprise française et a demandé que les fonds soient gelés dans le compte bancaire du bénéficiaire en Slovaquie. Les échanges entre les deux BRA ont entraîné le gel des fonds et ont permis aux autorités slovaques d'obtenir tous les renseignements requis pour élaborer et mettre en œuvre une demande judiciaire de gel. Finalement, le montant de 1 874 907 livres sterling a été gelé et rendu à l'entreprise victime.

Source : France

84. Pour maximiser l'efficacité des enquêtes sur le BC lié aux CF et du recouvrement des produits, la collaboration devrait avoir un objectif multilatéral plutôt que bilatéral. La présente section examine les problèmes et les bonnes pratiques liés à la collaboration internationale en se concentrant sur deux résultats opérationnels : (i) le recouvrement des avoirs et (ii) l'application de la loi et les poursuites.

5.1. Recouvrement des avoirs

85. Un des principaux défis associés au recouvrement des avoirs liés aux CF est la rapidité du processus de blanchiment. Pour atténuer ce problème, des programmes multilatéraux « d'intervention rapide » ont été créés par divers organismes afin de localiser et de récupérer les produits des CF, notamment le mécanisme mondial d'INTERPOL pour le blocage rapide des paiements (I-GRIP), le projet BEC du Groupe Egmont et la chaîne de lutte contre les fraudes financières des É.-U. Les expériences de ces organismes montrent généralement qu'une intervention est plus efficace dans les 24 à 72 heures suivant une transaction frauduleuse. Ces bonnes pratiques limitent le risque que les fonds se dispersent sur de multiples niveaux, ce qui réduit considérablement la portée de l'enquête sur le BC et facilite le recouvrement des produits illicites.

Encadré 40. Chaîne de lutte contre les fraudes financières et équipe de recouvrement des avoirs

La chaîne de lutte contre les fraudes financières (FFKC pour Financial Fraud Kill Chain) a été conçue par le FBI et le Financial Crimes Enforcement Network (la CRF des É.-U.) en 2016 pour répondre à l'augmentation des mécanismes de compromission de messagerie d'entreprise. La FFKC tente d'aider à retrouver les virements électroniques internationaux découlant des mécanismes de fraude en mettant à profit les relations entre le FinCEN et le Groupe Egmont des cellules de renseignement financier. Ce processus n'est possible que si le virement électronique respecte les critères suivants : (1) le montant du virement est supérieur ou égal à 50 000 $ US; (2) il s'agit d'un virement international; (3) un avis de rappel dans SWIFT a été lancé; et (4) le virement a été effectué dans les 72 dernières heures.

En 2018, l'Internet Crime Complaint Center (IC3) du FBI a mis sur pied l'équipe de recouvrement des avoirs (RAT pour Recovery Asset Team) afin de combler les lacunes des virements électroniques nationaux. La RAT rationalise les communications avec les institutions financières pour aider les bureaux régionaux du FBI à geler les fonds des virements nationaux effectués sous des prétextes frauduleux. La RAT a connu un certain succès, gelant 73 % des fonds dans le cadre de signalements d'activités frauduleuses au IC3 (433,3 M$ US sur 590,62 M$ US) jusqu'à maintenant. Selon une étude de cas américaine, ce programme peut, dans certains cas, permettre d'identifier rapidement les comptes de deuxième niveau et de geler les fonds, rendant possible un recouvrement de la totalité des fonds.

Source : États-Unis

86. Principalement, ces programmes multilatéraux ont deux objectifs : recueillir les renseignements minimums requis pour prendre des mesures d'application de la loi et communiquer ces renseignements aux « bonnes personnes ». Pour garantir une intervention transfrontalière efficace, tous les nœuds des réseaux multilatéraux doivent aussi accepter les règles et les procédures en matière de gouvernance. Même si ces réseaux multilatéraux sont généralement de nature mondiale, des initiatives régionales peuvent aussi permettre d'atténuer les obstacles en renforçant la collaboration régionale déjà en place.

Encadré 41. Projet antifraude intergouvernemental

Étant donné la nature transfrontalière des fraudes, une initiative régionale du groupe consultatif sur les renseignements financiers (FICG pour Financial Intelligence Consultative Group)[1], appelée Multi-jurisdictional Anti-Fraud Project, a été conçue. Cette initiative est codirigée par les CRF de la Malaisie, de l'Indonésie et de Singapour et elle vise à détecter, localiser et recouvrer les fonds pour les victimes.

Un mécanisme d'intervention a été mis en place impliquant des transactions transfrontalières entre les pays membres du FICG. Ce projet aidera les membres du FICG à échanger rapidement et facilement des renseignements financiers, ce qui augmentera la rapidité des mesures prises par les autorités pour lutter contre la fraude et récupérer les sommes volées.

Source : Malaisie

1 Le FICG est un organisme régional des CRF de l'Asie du Sud-Est, de la Nouvelle-Zélande et de l'Australie.

Collecte et échange de renseignements transfrontaliers : « recueillir les renseignements minimums requis »

87. Lorsque les CF sont considérés comme un crime grave en vertu des lois nationales, elles doivent être criminalisées comme une infraction de blanchiment d'argent sous-jacente en vertu de la recommandation 3 du GAFI. En outre, contrairement aux formes de fraudes traditionnelles commises entre connaissances, où il est difficile de distinguer la fraude d'un possible litige civil entre débiteur et créancier, il est relativement facile d'établir la criminalité a priori dans les affaires de CF, où la fraude est généralement commise entre des personnes qui ne se connaissent pas. Il n'est donc pas nécessaire de présenter une fastidieuse demande d'aide pour énoncer clairement et définir le lien avec la criminalité, comme c'est généralement le cas pour les autres types de crimes (qui ne sont pas universellement reconnus comme étant des infractions sous-jacentes).

88. À titre de bonne pratique, les divers programmes d'intervention rapide utilisent des modèles pour accélérer la collecte et l'échange de renseignements. Les modèles favorisent la collecte rapide des renseignements minimums requis pour établir la criminalité. Ils aident à concentrer les efforts des unités d'intervention sur place sur les types d'éléments probants ou de renseignements qu'il faut absolument obtenir dans les premières étapes d'une plainte au criminel. Ces modèles limitent aussi les problèmes liés à la qualité de l'information échangée et améliorent les interventions transfrontalières des organismes d'application de la loi.

89. En plus de décrire sommairement la CF, le modèle vise généralement à obtenir les données de base nécessaires pour faire avancer les efforts de localisation des fonds. La normalisation des demandes permet aux administrations de traiter rapidement toute demande reçue, ce qui accélère la capacité des organismes d'application de la loi à intercepter les fonds illicites qui sont entrés sur leur territoire.

90. Parmi les champs de données des modèles peuvent figurer les renseignements sur l'auteur de la transaction et le compte du bénéficiaire ainsi que de l'information sur la transaction (date, heure, montant transféré). Pour améliorer davantage l'efficacité, les modèles peuvent aussi comprendre de l'information sur la prochaine

destination des fonds si ceux-ci ont déjà été transférés du compte du bénéficiaire. Il peut aussi être utile de réduire au minimum les restrictions imposées aux administrations quant à la divulgation des renseignements échangés avec les autorités compétentes concernées à l'échelle nationale dès leur réception.

Encadré 42. Outil I-GRIP d'INTERPOL

INTERPOL a conçu l'outil INTERPOL Global Rapid Intervention of Payments (I-GRIP), qui est un mécanisme mondial pour le blocage rapide des paiements permettant aux pays membres de présenter et de gérer des demandes dans le but de localiser, d'intercepter ou de geler temporairement les produits illégaux de CF. Connu sous le nom de I-GRIP, le mécanisme a d'abord été mis à l'essai sous le nom de Protocole d'intervention rapide anti-blanchiment de fonds (ARRP pour Anti-Money Laundering Rapid Response Protocol), en 2022, puis lancé officiellement en novembre 2022 grâce à de nombreuses affaires d'arrêt de paiement couronnées de succès pendant le projet pilote.

I-GRIP favorise des communications rapides entre les Bureaux centraux nationaux d'INTERPOL (BCN) pour empêcher que de supposés actifs illicites soient transférés entre des pays membres. Les demandes présentées au moyen d'I-GRIP devraient comprendre suffisamment de détails pour que le BCN puisse agir, notamment la date de la transaction, la devise et le montant, les numéros des comptes et le nom des institutions financières des comptes du bénéficiaire et de l'auteur des versements.

Source : INTERPOL

91. De plus, les champs de données normalisés dans les modèles permettent aux organismes internationaux dont les capacités sont centralisées d'analyser facilement les données et d'optimiser les efforts des enquêteurs et de recouvrement des avoirs. Par exemple, INTERPOL utilise les renseignements échangés par l'entremise de ses canaux pour concevoir une base de données interne, le fichier d'analyse des infractions financières (FinCAF), pour faciliter l'analyse des renseignements à caractère transnational concernant différentes formes de crimes financiers et pour déterminer les liens entre les affaires transfrontalières et les enquêtes, les menaces, les tendances en matière de criminalité et les réseaux criminels (voir aussi l'encadré 45 ci-dessous).

92. Pour accélérer encore plus les mesures de recouvrement des avoirs, certaines administrations ont autorisé les victimes étrangères à déposer une plainte pour CF directement à leur OAL, notamment au moyen de leur plateforme de signalement en ligne permettant de remplir directement les champs de données requis pour une mesure d'application de la loi (voir la section précédente sur le signalement des victimes). Cette méthode élimine une communication supplémentaire et permet aux autorités compétentes de prendre rapidement les mesures prévues pour lutter contre les transactions suspectes réalisées dans des comptes de bénéficiaires sur leur territoire.

Pouvoirs requis pour agir :* les *« bonnes personnes »

93. Comme la vitesse est essentielle, toute information recueillie devrait idéalement être confiée directement aux autorités qui disposent déjà des pouvoirs et de l'expertise appropriés pour localiser les avoirs et les récupérer. Il leur est ainsi possible de prendre des mesures temporaires dès la réception d'une demande afin de prévenir le blanchiment ou la dissipation des avoirs. Cette mesure confère aux organismes d'application de la loi le temps nécessaire pour poursuivre leur enquête, établir et recueillir des éléments probants et présenter ensuite des demandes officielles d'entraide juridique (EJ).

Encadré 43. Demande de report de l'entité assujettie

La CRF de l'Italie a reçu une demande de report d'une entité assujettie concernant quatre virements électroniques suspects s'élevant à 490 000 EUR. Les transactions étaient demandées par une entreprise italienne de commerce de gros de vêtements à l'intention de différentes sociétés situées dans un pays d'Extrême-Orient.

L'entité assujettie a jugé les quatre opérations suspectes, puisque les fonds provenaient de transferts entrants dont la banque émettrice se souvenait parce que les fonds étaient envoyés en raison d'une « fraude du président » par une entreprise victime d'Europe de l'Ouest. La CRF de l'Italie avait aussi participé à un échange de renseignements international spontané avec la CRF dudit pays d'Europe de l'Ouest. L'entreprise italienne avait en outre fait l'objet d'un signalement à la CRF pour son lien possible avec des systèmes de fraude à la taxe sur la valeur ajoutée (TVA) impliquant le pays asiatique visé par l'entremise d'un pays distinct d'Europe de l'Est, qui apportait d'autres indications sur des liens entre la CF et d'autres formes de criminalité organisée.

Les transactions ont été reportées avec succès, ce qui a permis aux autorités étrangères d'émettre une ordonnance de saisie étrangère afin de recouvrer les fonds en Italie.

Source : Italie

94. Toutefois, une telle interface directe peut rencontrer des obstacles en raison des différences entre les cadres législatifs et d'application de la loi des différentes administrations. Parmi les bonnes pratiques permettant d'atténuer ces obstacles figurent la mise en œuvre de mécanismes de coordination nationaux pour faciliter la transmission des demandes aux autorités appropriées, ainsi qu'en misant sur des canaux de collaboration public-privé et sur la capacité des IF de prendre volontairement des mesures temporaires lorsqu'elles sont informées des possibles transactions suspectes par les autorités compétentes.

Gouvernance et règles : « l'entente collective »

95. Une structure de gouvernance et des règles pour les cadres multilatéraux fournissent des garanties et l'engagement à reconnaître mutuellement les activités criminelles et à agir rapidement dès la réception de l'information. Elles aident à relever les défis lorsque les priorités des organismes internationaux ne correspondent pas, puisque les conditions pour recevoir ou fournir de l'aide sont convenues à l'avance. À titre de bonne pratique, ces règles et critères devraient être clairs et faciles à comprendre.

96. Les principes susmentionnés s'appliquent aux mécanismes de collaboration internationaux informels et formels. Le *Règlement (UE) 2018/1805* du Parlement européen et du Conseil, qui permet la reconnaissance mutuelle des décisions de gel et des décisions de confiscation, en est un bon exemple. Ce mécanisme d'application directe permet une intervention transfrontalière rapide.

97. Le partage d'information accéléré ne doit pas se faire aux dépens de la protection et

de la confidentialité des données. Pour assurer la sécurité de l'information transmise, des cadres multilatéraux tirent habituellement profit de voies de communication sécurisées existantes, comme celles fournies par INTERPOL, Europol et le Groupe Egmont. Ces voies de communication sécurisées permettent aussi aux cadres multilatéraux de se développer facilement, puisqu'ils permettent d'éviter d'avoir à concevoir des voies de communication bilatérales.

Encadré 44. Équipe du projet BEC du Groupe Egmont

Pour pallier la hausse et la gravité des menaces associées à la compromission de messagerie d'entreprise (BEC) pour les institutions financières et leurs clients, 11 CRF ont mis sur pied l'équipe du projet BEC du Groupe Egmont, qui se concentre sur l'analyse des tendances, des indicateurs et des méthodologies liés à la BEC et la communication des principales constatations aux CRF. Les typologies financières communes associées à la BEC et les études de cas montrent qu'une réaction rapide pour stopper et faire le suivi des virements électroniques est la façon la plus efficace de lutter contre ce type de crime.

Par conséquent, l'équipe du projet[1] établit des protocoles entre les organismes d'application de la loi et les CRF et entre les CRF internationaux afin de suivre et de geler les produits de la BEC.

- À la réception d'une DOD concernant le flux de la BEC transfrontalière soupçonnée, la CRF émettrice conçoit une demande « d'intervention rapide » à la CRF destinataire.
- La demande doit contenir les données et les renseignements de base convenus qui doivent être échangés pour les mesures d'application de la loi.
- On demande à la CRF destinataire de prendre (lorsque c'est possible) des mesures immédiates pour bloquer et récupérer les produits illicites, idéalement dans les 72 heures suivant le crime.

Le projet BEC met à profit la plateforme sécurisée du Groupe Egmont pour les communications visant à échanger les demandes « d'intervention rapide ».

Source : Le Groupe Egmont

1 L'équipe du projet est actuellement composée des membres suivants : AUSTRAC (Australie), BFIU (Bangladesh), CTIF-CFI (Belgique), TRACFIN (France), GHFIU (Ghana), HFIU (Hongrie), IMPA (Israël), SIC (Liban), FIU (Luxembourg), UPWBNM (Malaisie), FinCEN (É.-U.) et Europol.

5.2. Application de la loi et poursuites

98. En plus du recouvrement des avoirs, le caractère transnational des CF a aussi entraîné des difficultés tout au long du processus d'application de la loi, de l'obtention des renseignements et de l'enquête jusqu'à la collecte d'éléments probants pour les poursuites. L'évolution de la technologie a accéléré les transactions et facilité les opérations fragmentées au-delà des frontières. Elle a aussi augmenté le temps et les efforts nécessaires pour appliquer la loi ainsi que pour localiser et identifier les transactions.

Collecte de données numériques

99. Même si elles ne sont pas exclusivement liées au BC, les preuves judiciaires numériques peuvent fournir des indices essentiels pour amener les organismes d'application de la loi à approfondir leurs enquêtes sur le BC. La grande disponibilité et la facilité d'utilisation des services de dissimulation d'identité, comme les RPV, compliquent encore la tâche de localiser les principaux auteurs de CF.

100. Malheureusement, il n'existe pas actuellement de régime mondial unique régissant la durée de conservation des données numériques, y compris en ce qui a trait aux fournisseurs de services techniques. Plusieurs administrations ont souligné le risque élevé de dissipation des preuves numériques. Les retards associés aux mécanismes de collaboration officiels représentent aussi un obstacle à l'obtention rapide des preuves numériques.

101. Il existe plusieurs bonnes pratiques permettant d'atténuer ces problèmes.

- **Miser sur les méthodes informelles** pour obtenir et réunir des renseignements. Les canaux de coopération officiels sont ensuite utilisés pour obtenir les données probantes et les déclarations nécessaires pour préparer la procédure judiciaire.
- **Les conventions et les outils d'enquête,** comme la Convention sur la cybercriminalité, aussi appelée Convention de Budapest, favorisent une conservation rapide des données électroniques et la transmission spontanée d'information, ce qui aide à accélérer l'identification des principaux auteurs des CF. La Convention de Budapest établit aussi un réseau fonctionnel 24 h par jour, 7 jours par semaine, qui assure une assistance aux fins d'investigation pour la prestation de conseils techniques, la collecte d'éléments probants, la conservation des données, etc.
- **Une collaboration directe** avec les fournisseurs de services étrangers pour obtenir les preuves judiciaires nécessaires, comme les renseignements sur l'abonné, sans passer par le processus d'EJ. Selon une administration, la collaboration directe volontaire d'un fournisseur de services étrangers est le mécanisme le plus efficace pour recueillir des preuves numériques pertinentes[22].

[22] Voir aussi Conseil de l'Europe (juillet 2020), *La Convention de Budapest sur la cybercriminalité : avantages et impact concrets*, pour en savoir plus sur la coopération volontaire avec les fournisseurs de services étrangers.

Encadré 45. La Convention de Budapest

La Convention de Budapest définit les pouvoirs procéduraux pour : la conservation rapide de données informatiques stockées, la conservation rapide et la divulgation partielle de données relatives au trafic, les injonctions de produire ainsi que la perquisition et la saisie de dispositifs informatiques, la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu. La Convention fournit aussi un régime de coopération internationale rapide et efficace.

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques fournit aussi une base juridique pour la divulgation de renseignements sur l'enregistrement d'un nom de domaine et pour la coopération directe avec les fournisseurs de services au chapitre des données relatives aux abonnés, des méthodes efficaces pour obtenir des renseignements sur les abonnés et des données relatives au trafic, une coopération immédiate en cas d'urgence, des outils d'entraide ainsi que des mesures de protection des données personnelles.

Source : Conseil de l'Europe

Mesures d'application conjointes

102. Les équipes conjointes d'enquête (ECE) transfrontalières nécessitent une entente juridique entre les autorités compétentes d'au moins deux administrations dans le but de mener des enquêtes pénales. Elles peuvent faciliter le partage de renseignements et les enquêtes financières transfrontalières. Pour le partage de renseignements, on utilise généralement divers cadres et accords (p. ex. Eurojust ou le Groupe d'action conjoint sur la cybercriminalité d'Europol).

103. Les ECE constituent un point de coordination important pour les mesures d'application de la loi multilatérales visant à lutter contre les CF, compte tenu de leurs opérations transnationales et décentralisées. Avec la réduction des obstacles aux opérations criminelles, les syndicats de la CF peuvent facilement se relocaliser et établir de nouveaux centres d'opérations numériques à distance. Les mesures de coordination sont donc nécessaires pour éradiquer simultanément les différents sous-groupes (qui peuvent être situés dans de multiples administrations).

Encadré 46. Action conjointe contre une fraude en matière d'investissement à grande échelle[1]

La Serbie, en collaboration avec l'Autriche, la Bulgarie et l'Allemagne et avec le soutien d'Eurojust, a participé à des opérations fructueuses contre deux groupes criminels organisés soupçonnés d'avoir commis une fraude en matière d'investissement à grande échelle dans le domaine du commerce électronique. Les autorités serbes ont arrêté cinq suspects et fouillé neuf lieux et ont saisi cinq appartements, trois voitures, un montant d'argent comptant considérable et de l'équipement informatique. Plus de 30 comptes bancaires en Serbie ont aussi été mis sous surveillance. De plus, 4 suspects ont été arrêtés en Bulgarie, et 2,5 millions d'euros ont été gelés dans le compte bancaire d'une entreprise impliquée dans un stratagème de fraude en Allemagne.

Selon l'information recueillie pendant l'opération, les autorités ont rapidement mis en place une autre opération contre une entreprise de Belgrade deux jours plus tard, qui a conduit à l'arrestation d'un suspect et à la saisie de serveurs, d'autre matériel informatique et de documents.

Dans ce cas, les autorités serbes ont notamment invoqué l'article 26 de la Convention de Budapest (Information spontanée) pour échanger de l'information avec d'autres partenaires. Eurojust a aussi participé aux enquêtes en finançant une équipe conjointe d'enquête (ECE) et en organisant une rencontre de coordination dans ses installations de La Haye ainsi qu'une vidéoconférence.

Source : Serbie; Conseil de l'Europe (juillet 2020), La Convention de Budapest sur la cybercriminalité : avantages et impact concrets.

1 Pour de plus amples renseignements, voir aussi Eurojust (avril 2020), communiqué accessible en ligne à l'adresse : https://www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries [en anglais seulement].

104. Cela dit, des défis sont aussi associés aux mesures d'application conjointes.

- **Des obstacles juridiques** peuvent restreindre l'échange de renseignements informel, même au sein des équipes conjointes d'enquête. Une administration a mentionné la nécessité de s'appuyer sur les demandes d'EJ pour permettre l'échange d'information, ce qui peut gêner l'efficacité et la participation. L'information qu'il est possible de partager peut aussi être limitée, particulièrement en raison de la granularité de l'information sur les transactions financières.
- **L'inégalité des capacités et des priorités** peut aussi dissuader les administrations de participer à une action conjointe. Comme mentionné précédemment, les priorités nationales à l'interne ne concordent pas toujours avec les actions conjointes et il peut être difficile pour les administrations de trouver un juste équilibre entre leurs intérêts et les ressources limitées malgré l'augmentation des CF.

105. En plus des ECE, les opérations conjointes organisées par des organismes multilatéraux comme INTERPOL constituent aussi un point de coordination important pour les mesures d'application de la loi multilatérales visant à lutter

contre les CF. Bien que de telles opérations puissent être moins formelles que les ECE en l'absence d'accords juridiques officiels, elles peuvent tout de même constituer une plateforme importante pour que les administrations concernées puissent lutter conjointement contre les CF.

Encadré 47. Opération HAECHI d'INTERPOL

Depuis 2020, INTERPOL dirige une opération annuelle baptisée opération HAECHI, qui vise les cybercrimes financiers et le BC connexe et qui encourage l'échange de renseignements entre les administrations participantes. Dans le cadre de la récente opération HAECHI III (2022), à laquelle 30 administrations ont participé, près de 1 000 suspects ont été arrêtés et 2 800 comptes bancaires et d'actifs virtuels liés à des produits illicites évalués à 130 millions de dollars américains ont été bloqués. Pendant l'opération HAECHI III, INTERPOL a coordonné de nombreux dossiers entre des pays membres pour lutter ensemble contre les CF.

L'opération HAECHI a aussi servi de plateforme au FinCAF, qui recueille de l'information auprès de différentes sources et établit les liens entre les enquêtes en cours dans les différents pays membres. Le FinCAF est structuré de façon à inclure les données et d'autres éléments d'information liés à tout type d'infractions ou de crimes financiers à caractère transnational. INTERPOL utilise le FinCAF pour collaborer avec les pays membres afin de renforcer l'intervention tactique globale en réponse au crime organisé international, comme les CF. Le FinCAF est un important outil donnant un meilleur aperçu des activités criminelles transfrontalières, des organisations criminelles, de la structure des groupes, des rôles individuels et des personnes importantes, des modes opératoires et des transactions financières frauduleuses.

Source : INTERPOL

Collaboration public-privé

106. La collaboration public-privé peut s'étendre au-delà des frontières nationales, ce qui peut donner de meilleurs résultats étant donné la portée transnationale des CF. Comme les PPP nationaux, cette collaboration peut comprendre l'échange de typologies ou de stratégies ainsi qu'une coordination opérationnelle. La composition de ces partenariats dépend aussi des objectifs fixés et peut inclure des secteurs traditionnels et non traditionnels de la LBC/LFT.

Encadré 48. Opération European Money Mule Action

L'opération European Money Mule Action est une opération internationale axée sur le partage de renseignements public-privé afin de lutter contre les crimes modernes complexes.

En 2022, sous la coordination continue de la Fédération bancaire européenne, environ 1 800 banques et institutions financières ont appuyé les forces de l'ordre dans le cadre de cette opération, aux côtés d'entreprises de services de transfert de fonds, d'échange de cryptomonnaie, de technologie financière et de connaissance de la clientèle en ligne et de sociétés d'informatique multinationales.

L'opération comprenait les forces de l'ordre de 25 administrations[1] et recevait aussi l'appui d'Europol, Eurojust et INTERPOL. Elle a permis d'identifier 8 755 mules financières ainsi que 222 recruteurs de mules. Au total, 17,5 millions EUR ont été interceptés et 2 469 mules financières ont été arrêtées.

Source : Europol

1 Australie, Autriche, Bulgarie, Colombie, Chypre, République tchèque, Estonie, Grèce, Hongrie, Singapour, Hong Kong (Chine), Irlande, Italie, Moldavie, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède, Suisse, Espagne, Royaume-Uni et États-Unis.

6. Conclusion et domaines prioritaires

107. Les CF sont commises par des syndicats du crime organisé transnationaux. La portée et l'ampleur des CF devraient augmenter avec la nouvelle tendance à la numérisation et à l'utilisation des services virtuels partout dans le monde. Les administrations devraient aussi être conscientes des vulnérabilités supplémentaires dans différents secteurs, notamment le secteur des institutions financières numériques et les secteurs non traditionnels, que les criminels exploitent pour améliorer les CF et les techniques de BC grâce à la numérisation croissante.

108. Les administrations doivent se concentrer sur l'élimination du cloisonnement pour accélérer et améliorer la collaboration entre les différents secteurs et entités, autant à l'échelle nationale qu'internationale. En raison de la nature décentralisée des CF et du BC connexe, les renseignements financiers et les éléments probants essentiels sont souvent dispersés à différents endroits. Cela complique les efforts déployés pour enquêter sur les syndicats de la CF et les démanteler ainsi que pour localiser et recouvrer les produits des CF.

109. Les CF peuvent avoir un impact financier important et écrasant sur les victimes, mais cet impact ne se limite pas aux pertes monétaires; les CF peuvent aussi avoir des conséquences sociales et économiques dévastatrices. Les conclusions du présent rapport soulignent trois domaines prioritaires sur lesquels les administrations devraient se concentrer pour lutter contre les CF et le BC connexe plus efficacement : l'amélioration de la coordination nationale; l'appui à la collaboration multilatérale; et le renforcement de la détection et de la prévention.

Domaines prioritaires pour lutter efficacement contre les CF et le BC connexe

Amélioration de la coordination nationale dans les secteurs public et privé

- Les administrations doivent élaborer des mécanismes de coordination réunissant les autorités compétentes concernées afin de lutter contre les CF et le blanchiment des produits de la criminalité connexes de façon globale. Cela comprend les experts techniques en cybercriminalité ainsi que les secteurs non traditionnels, comme des plateformes de médias sociaux, le commerce électronique et les fournisseurs de services de télécommunication et d'accès à Internet. Les administrations devraient aussi miser sur les partenariats public-privé pour améliorer la détection ainsi que les enquêtes et accélérer les interventions opérationnelles en vue de recouvrer des avoirs.
- Une bonne pratique consiste à créer une unité spécialisée centralisée pouvant exploiter les renseignements pertinents et coordonner les mesures dans différents domaines des secteurs public et privé, y compris les enquêtes, le recouvrement des avoirs et la prévention des fraudes.

Soutien à la collaboration multilatérale internationale

- Pour améliorer les résultats du recouvrement des avoirs et éviter la dissipation des produits liés aux CF, les administrations doivent collaborer pour intercepter rapidement ces produits. L'expérience opérationnelle montre que l'intervention est généralement plus efficace dans les 24 à 72 heures suivant une CF. Une approche unie à l'échelle mondiale est nécessaire pour localiser et recouvrer efficacement les produits des CF, qui sont blanchis et répartis dans différentes administrations.
- Pour ce faire, les administrations doivent exploiter les mécanismes multilatéraux existants (et futurs) (comme les projets I-GRIP d'INTERPOL et BEC du Groupe Egmont) pour favoriser une collaboration et un échange de renseignements internationaux rapides afin de lutter contre les CF. Ces mécanismes multilatéraux permettent aussi aux administrations de collaborer et de démanteler collectivement des syndicats de la CF transnationaux.

Renforcement de la détection et de la prévention

- Pour améliorer la détection, les administrations doivent s'assurer qu'il est facile pour les victimes de faire un signalement, par exemple, au moyen de plateformes consacrées à la rationalisation des signalements. Les administrations doivent aussi travailler avec le secteur privé pour améliorer le signalement des transactions suspectes.
- Les administrations doivent promouvoir la sensibilisation et la vigilance à l'égard des CF en sensibilisant le public, y compris en communiquant les signes révélateurs de CF et en améliorant la cyberlittératie. La prévention joue un rôle clé dans la réduction de la rentabilité globale des syndicats de la CF. Les administrations peuvent aussi collaborer avec le secteur privé pour appuyer les stratégies de prévention des CF, comme la protection des clients et l'élimination des instruments criminels.

Annexe A : Indicateurs de risques pour les CF

Les indicateurs de risques potentiels suivants s'inspirent de l'expérience et des données reçues des administrations au sein du réseau mondial du GAFI, du Groupe Egmont et du secteur privé. Ces indicateurs visent à améliorer la détection des transactions suspectes liées aux CF. La liste a été subdivisée sous divers angles, de l'ouverture du compte à la surveillance des transactions. Les indicateurs peuvent être pertinents pour les entités réglementées, y compris les IF, les FSAV, les EPNFD et d'autres institutions financières et de paiement.

L'existence d'un indicateur unique en lien avec un client ou une transaction ne peut, en soi, justifier des soupçons de CF ni indiquer clairement l'existence d'une telle activité. Toutefois, il peut accélérer un contrôle et un examen renforcés, si nécessaire.

Modèles de transaction

- Transactions rapides ou immédiates, à valeur faible ou élevée, réalisées après l'ouverture d'un compte et incompatibles avec le but du compte.
- Retraits ou virements d'espèces rapides ou immédiats d'un montant important, après la réception d'un transfert de fonds dans le but de vider le compte.
- Transactions fréquentes et importantes, incompatibles avec le profil économique du titulaire du compte (p. ex. virements internationaux soudains, retraits d'espèces par carte de paiement dans des GAB étrangers, achats importants d'AV ou de marchandises devant être exportées à l'étranger, ou paiements effectués au profit de STFV étrangers non autorisés).
- Transferts de fonds en provenance et à destination d'administrations où le risque de blanchiment de capitaux est élevé.
- Les transactions fréquentes et importantes avec des entreprises récentes ou dont les principales activités ne correspondent pas aux activités du bénéficiaire ou qui ont un objectif général.
- Petit versement à un bénéficiaire qui, une fois effectué avec succès, est rapidement suivi de versements plus importants au même bénéficiaire.
- Achats fréquents d'une valeur arrondie et d'un montant important, qui peuvent indiquer des achats de cartes-cadeaux.

Directives et remarques concernant les transactions de clients

- Une demande de transaction d'un client relativement à des versements additionnels suivant immédiatement un versement réussi dans un compte que le client n'utilisait pas auparavant pour payer ses fournisseurs. Ce type de comportements peut correspondre à une tentative d'un criminel d'effectuer des versements additionnels non autorisés après avoir constaté la réussite d'un versement frauduleux.
- La formulation, le moment de l'exécution et les montants mentionnés dans des instructions d'un client concernant une transaction qui semble légitime diffèrent des instructions de transaction vérifiées précédemment.

- Des instructions de transaction contiennent des notes, des affirmations ou des formulations indiquant que la demande de transaction est « urgente », « secrète » ou « confidentielle ».
- Un client envoie des messages ou des courriels mal présentés (erreurs d'orthographe ou de grammaire) pour justifier une transaction.
- Les instructions de transaction dirigent le paiement vers un bénéficiaire connu; toutefois, les renseignements sur le compte du bénéficiaire diffèrent des renseignements habituels.
- Le bénéficiaire prévu dans la description de la transaction et le nom du titulaire du compte connu de la banque bénéficiaire ne concordent pas.
- Les virements demandés par des personnes physiques (prétendus investisseurs) sans expérience ni expertise financière, au profit d'entreprises (dans de nombreux cas, établis dans des administrations à risque élevé), dont la raison du virement est liée à des placements et des produits financiers.
- Des contreparties sans rapport avec les activités ou le nom de l'entreprise associés au compte qui peuvent dissimuler des mouvements de fonds importants à l'échelle internationale (p. ex. une entreprise enregistrée comme étant une entreprise de meubles a fait plusieurs virements importants à une entreprise œuvrant dans le secteur pétrolier).
- Des transactions effectuées à l'aide de systèmes dont les fuseaux horaires ne correspondent pas.

Soupçons liés au profil du titulaire du compte

- Le titulaire du compte ne souhaite pas ou est incapable de se soumettre à une vérification de la diligence raisonnable à l'égard de la clientèle (CDD).
- Le titulaire d'un compte ne connaît pas bien la source des fonds qui sont transférés dans son compte ou affirme effectuer la transaction pour une autre personne.
- Modification fréquente des personnes morales ou noms d'entreprises individuelles utilisant des expressions ou de la terminologie étrangères.
- Le client montre qu'il connaît mal la nature, l'objet, le montant ou le but de la ou des transactions ou de la relation ou fournit des explications irréalistes, confuses ou incohérentes, ce qui laisse présumer qu'il agit à titre de mule.

Soupçons liés à l'identité de l'utilisateur du compte

- L'utilisateur tente de dissimuler son identité en utilisant des pièces d'identité (adresse, numéro de téléphone, courriel) partagées, falsifiées, volées ou modifiées.
- Modification fréquente des coordonnées, numéros de téléphone ou adresses de courriel après l'ouverture du compte.
- Adresses de courriel qui ne semble pas correspondre au nom du titulaire du compte, ou des adresses de courriel semblables observées pour de nombreux comptes.
- Irrégularités dans les renseignements de profil du client, comme des identifiants partagés (p. ex. partagés par deux ou plusieurs utilisateurs) avec

d'autres comptes.

- Anomalies identifiées par rapport aux comportements en ligne, comme une hésitation dans la saisie de données, un retard de frappe, des signes d'automatisation, de multiples tentatives de connexion infructueuses, etc.
- Comptes liés à des entités dont on peut s'attendre à ce qu'ils ne soient plus actifs au sein de l'administration (p. ex., comptes d'étudiants étrangers vendus lorsque les études sont terminées).
- Adresses IP ou coordonnées GPS provenant d'administrations où le risque de blanchiment de capitaux est élevé.
- Utilisation de réseaux privés virtuels (RPV), d'appareils compromis (comme des appareils connectés à l'Internet des objets [IDO]) et d'entreprises d'hébergement qui peuvent dissimuler l'adresse IP d'un utilisateur.
- Multiples adresses IP ou appareils électroniques associés à un seul compte en ligne.
- Une seule adresse IP statique ou un appareil électronique associés à de nombreux comptes appartenant à des titulaires variés.
- Connexion à un bureau à distance pour accéder à un compte par l'entremise de bornes d'entrée utilisées par des applications comme TeamViewer, qui empêchent d'identifier le véritable appareil et son emplacement.
- Vitesse de frappe ou de navigation très rapide pendant l'utilisation de comptes, indiquant une possible prise de contrôle par un robot.

Renseignements défavorables sur le titulaire du compte

- Présence de nouvelles négatives importantes, pertinentes et vérifiables concernant le client ou les contreparties, p. ex. si le compte appartient à une victime connue ou présumée d'une arnaque antérieure ou d'un vol d'identité ou à une mule.
- Signalement de fraude ou rappel provenant d'une institution de correspondance ou des bases de données en matière de fraude d'un autre tiers.
- Présence de demandes de rappel pour les virements électroniques.
- Présence de renseignements défavorables fournis par les CRF ou les OAL concernant des personnes impliquées dans une transaction.

Transactions portant sur des AV

- Envoie ou réception d'AV de faible valeur en grand nombre ou à fréquence élevée en utilisant des adresses de portefeuilles non hébergés; ou des adresses associées à des marchés sur le Web clandestin, des plateformes proposant du matériel montrant l'exploitation sexuelle d'enfants, des marchés encourageant la cyberexploitation, des groupes d'opérateurs de rançongiciels, des services de mélange de monnaie virtuelle, des administrations à risque élevé, des sites de jeux de hasard et des arnaqueurs.
- Atteinte des limites de financement quotidiennes dans les guichets automatiques Bitcoin.
- Aucun document démontrant l'origine des AV ou des sommes converties en cryptoactifs.

- Transferts d'AV vers des portefeuilles liés à des activités illégales sur le Web clandestin (p. ex. terrorisme, pornographie infantile, stupéfiants, etc.).
- Les transactions impliquant plus d'un type d'AV, en particulier celles qui garantissent un anonymat accru.
- Activité transactionnelle anormale d'AV provenant de portefeuilles associés à des plateformes entre pairs sans explication commerciale logique.

Autre

- Incompatibilité du numéro de compte et du nom du titulaire du compte.
- On peut voir que l'utilisateur est au téléphone ou qu'il est accompagné d'un individu grâce à un système de télévision en circuit fermé et qu'il reçoit des instructions ou de la formation pendant la transaction.
- Les entreprises bénéficiaires gèrent des sites Web offrant des services de négociation et d'investissement qui, dans bien des cas, ne sont pas autorisés ou ne figurent pas sur la liste de l'autorité de surveillance nationale.

Annexe B : Mettre à profit les synergies entre les contrôles antifraude et en matière de LBC/LFT

La présente annexe regroupe de bons exemples montrant comment les organismes de réglementation du secteur financier ont adopté des exigences antifraude en plus des contrôles en matière de LBC/LFT, dont certaines ciblent la capacité des criminels à inscrire, à contrôler et à accéder à des comptes de mule à distance. Ces exigences comprennent diverses mesures liées à la vérification des clients et à la surveillance des transactions.

Ces contrôles peuvent être utiles pour les IF, les FSAV et d'autres institutions financières et de paiement.

- Mise en place de processus d'identification des clients ou des entreprises rigoureux et d'identificateurs biométriques pendant le processus d'accueil numérique, etc., et identification d'un appareil mobile ou sécurisé pour authentifier les transactions bancaires en ligne (les autres sont bloqués ou assujettis à des mesures d'atténuation des risques accrues).
- Période d'attente pour une première inscription à des services bancaires en ligne ou des dispositifs sécurisés (c.-à-d. que tous les services bancaires ne sont pas immédiatement accessibles à l'ouverture du compte) limitant le nombre ou la valeur des transactions financières du client.
- Élaboration d'une définition des transactions prévues (nombre de transactions, montant, types de contreparties, pays visés) pour aider à détecter les transactions suspectes et à renforcer les règles et les déclencheurs de détection des fraudes afin de bloquer de façon préventive les transactions illicites.
- Utilisation de services de vérification du bénéficiaire, ce qui permet à l'auteur/payeur/débiteur d'un ordre de transfert de vérifier que le bénéficiaire/créancier mentionné dans les messages de paiement concorde avec le nom du titulaire du compte.
- Limitation à des renseignements généraux uniquement de toutes les communications par courriel et sur les médias sociaux avec les clients, en indiquant clairement qu'aucune donnée d'identification ou personnelle ne doit être échangée avec l'IF/FSAV par courriel.
- Ajout d'un logiciel de reconnaissance vocale et d'un système d'intelligence artificielle dans les communications avec les clients pour garantir leur véritable identité.
- Imposition de mécanismes d'authentification multifacteurs pour vérifier les clients, effectuer des transactions financières et ajouter ou activer des bénéficiaires en utilisant différents canaux.
- Authentification de l'identité de l'utilisateur pendant la configuration à distance pour éviter que des criminels aient accès à plusieurs comptes en utilisant des renseignements sur les comptes de mules financières ou de victimes :

- en renforçant la fiabilité du processus d'identification des clients au moyen de vérifications du caractère vivant (c.-à-d. pour s'assurer qu'il s'agit bien d'un véritable être humain vivant), y compris en vérifiant si l'individu est victime d'une manipulation psychologique pendant les vérifications; ou
- en surveillant les adresses IP utilisées pour se connecter aux sites bancaires en ligne, etc., y compris en détectant l'utilisation d'outils d'accès à distance et d'attaques par infection du navigateur.

- Ajout de types de données que les entités déclarantes recueillent et analysent au sujet des clients, comme des numéros de téléphone cellulaire, des adresses IP, des coordonnées GPS, des numéros d'identification d'appareils, etc. Aux fins de prévention des fraudes, les IF pourraient répéter ces mesures d'identification en utilisant une approche fondée sur le risque (p. ex. effectuer ces vérifications si un comportement anormal est détecté).
- Mise en œuvre d'un système de surveillance des transactions en temps réel fondé sur le risque pour s'assurer de détecter, d'examiner et, le cas échéant, de signaler rapidement au moyen d'une déclaration d'opérations douteuses toutes les activités anormales. La complexité du système de surveillance devrait correspondre au volume et à la nature des transactions gérées par l'IF.

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

Novembre 2023

Flux financiers illicites provenant des cyberfraudes

Le présent rapport analyse les méthodes utilisées dans le cadre des cyberfraudes, leurs liens avec d'autres crimes et les techniques permettant aux criminels d'exploiter les vulnérabilités des nouvelles technologies. Il donne des exemples d'interventions opérationnelles et de stratégies nationales qui se sont avérées efficaces pour lutter contre les cyberfraudes. Ce rapport décrit aussi des indicateurs de risque ainsi que des exigences et des contrôles antifraude, qui peuvent être utiles pour permettre aux entités des secteurs public et privé de détecter et de prévenir les cyberfraudes et le blanchiment de capitaux connexe.