

SANCTIONS FINANCIERES CIBLEES

TYPOLOGIES DE SANCTIONS FINANCIERES
CIBLEES LIEES AU FT

- MARS 2023 -

TABLE DES MATIERES

Sanctions financières ciblées	1
Typologies de sanctions financières ciblées liées au FT	1
- Mars 2023 -	1
Table des matières.....	2
Introduction.....	3
Champ d'application du document de typologie	3
Coordonnées.....	3
Financement du terrorisme.....	4
Qu'est-ce que le financement du terrorisme ?	4
Méthodes de financement du terrorisme	4
Financement du terrorisme – Études de cas.....	6
Services bancaires	6
Prestataires de services de transfert de fonds.....	6
Facilités de paiement en ligne.....	6
Dons par ou par l'intermédiaire d'organismes à but non lucratif.....	7
Contrebande d'espèces	8
Devises virtuelles	8
Signaux d'alarme pour la violation des SFC liées au FT.....	10

INTRODUCTION

1. L'Organisation des Nations Unies (ONU), par les Résolutions de son Conseil de sécurité (RCSNU) et ses Comités des sanctions, vise à préserver la paix et la sécurité, en exigeant la mise en œuvre de mesures de gel liées au terrorisme et au financement du terrorisme (FT). En adoptant des résolutions visant à bloquer la cession de leurs actifs financiers par les terroristes et les organisations terroristes, l'objectif des sanctions financières ciblées liées au FT consiste à freiner les mouvements de paiements et de capitaux liés au terrorisme.
2. La Principauté de Monaco (Monaco), en tant que membre de l'ONU, s'engage à mettre en œuvre les mesures de sanctions imposées par les RCSNU. Cet engagement s'étend sur tous les régimes de sanctions de l'ONU, y compris la mise en œuvre de mesures allant de sanctions économiques et commerciales globales à des mesures plus ciblées telles que les embargos sur les armes, les interdictions de voyager, et les restrictions financières ou relatives aux produits de base.
3. Toutefois, les personnes physiques et morales désignées sur les RCSNU ont recours à des tactiques de contournement des sanctions pour échapper de manière stratégique aux sanctions qui leur sont imposées. À ce titre, Monaco s'engage à protéger ses institutions financières (IF) et les entreprises et professions non financières désignées (EPNFD) contre les abus commis par des acteurs illicites impliqués dans le financement du terrorisme et la violation de sanctions.
4. Compte tenu des subtilités liées à l'identification des tactiques de contournement des sanctions, ce document présente des études de cas et des exemples sur la manière dont ces activités, personnes, groupes ou entités sanctionné(e)s ont bénéficié d'un financement et d'un soutien, violant ou se soustrayant ainsi aux RCSNU relatives au terrorisme et au financement du terrorisme.¹ Il est extrêmement important que l'ensemble de la population de personnes physiques et morales à Monaco fasse preuve de prudence et de vigilance pour que les individus ou les organisations qui sont soumis aux sanctions liées au FT du Conseil de sécurité des Nations Unies (CSNU) ne soient en aucun cas soutenus.
5. Le présent document comprend également une liste de signaux d'alarme qui peuvent aider les IF et les EPNFD à détecter toute opération suspecte impliquant des SFC liées au FT.

Champ d'application du document de typologie

6. Le présent document de typologie a été publié par le Comité consultatif en matière de gel des fonds et des ressources économiques (le Comité consultatif) afin d'aider les entités déclarantes à mettre en œuvre les obligations liées aux SFC. Les informations contenues dans le présent document ne constituent en aucun cas des conseils juridiques et doivent être lues conjointement avec la législation nationale applicable, les normes internationales et les directives publiées par le Comité consultatif ou d'autres organismes compétents (par exemple, le SICCFIN et la DSP).

Coordonnées

7. Pour l'ensemble des demandes de renseignements, rapports et demandes concernant la mise en œuvre de SFC liées au FT, veuillez envoyer un courriel au Comité consultatif en matière de gel des fonds et des ressources économiques.

E-mail : dbt.geldefonds@gouv.mc

Site Internet : <https://geldefonds.gouv.mc/>

¹ Les Résolutions du CSNU liées au FT sont les RCSNU 1267 (1999) et 1989 (2011) relatives à l'État islamique en Irak et au Levant (Daech) et à Al-Qaïda, et la RCSNU 1988 (2011) concernant les talibans.

FINANCEMENT DU TERRORISME

Qu'est-ce que le financement du terrorisme ?

8. Le terme « financement du terrorisme » (FT) comprend la fourniture de fonds pour commettre des activités terroristes ainsi que le soutien et l'entretien de la personne (terroriste) ou du groupe terroriste. Ce terme englobe la fourniture de nourriture, d'hébergement, de formation, ainsi que la mise à disposition de moyens tels que le transport ou le matériel de communication. Ce financement peut avoir lieu au moyen d'espèces, de virements ou d'apports en nature. Il convient de noter que les fonds concernés peuvent provenir de sources légales ou illégales.

9. Le Fonds monétaire international indique que l'objectif premier des personnes ou entités impliqués dans le financement du terrorisme n'est pas nécessairement de dissimuler les sources de l'argent, mais de dissimuler à la fois l'activité de financement et la nature de l'activité financée.

10. Ci-après figurent des méthodes et des études de cas qui illustrent la façon dont les groupes terroristes ont abusé de secteurs ou d'activités économiques pour financer leurs intérêts. Le présent document contient des informations issues de documents élaborés par le CSNU, l'Office des Nations Unies contre la drogue et le crime (ONUDC) et le Groupe d'action financière (GAFI).

Méthodes de financement du terrorisme

11. Au cours des dernières décennies, les IF et les EPNFD ont été confrontées à une vague grandissante de nouvelles législations et exigences réglementaires, dont une grande proportion s'est concentrée sur le thème de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT). La tendance générale était de supposer que les composantes liées à la LCB (y compris les signaux d'alarme et typologies) s'appliquent également au financement du terrorisme.

12. Cependant, les cas en situation réelle ont mis en évidence le fait que les techniques employées par les auteurs de blanchiment de capitaux sont tout à fait différentes de celles qui participent du financement du terrorisme. La principale raison de cette différence réside dans le fait que les objectifs de l'auteur de blanchiment de capitaux et ceux du financier terroriste diffèrent sensiblement. Les deux délinquants doivent parvenir à dissocier la source des fonds de leur entrée dans le système financier. Toutefois, l'auteur de blanchiment de capitaux cherche à obtenir des avantages à long terme de son crime et est prêt à les obtenir sous de nombreuses formes, tandis que le financier terroriste se concentre sur la fourniture de devises ou de moyens aux personnes impliquées dans le soutien ou la commission d'actes de terrorisme.

13. Compte tenu de cette différence fondamentale en termes d'objectifs, les typologies liées au FT diffèrent également de celles du blanchiment de capitaux. Le GAFI a identifié que l'État islamique en Irak et au Levant (EIL) tire principalement des revenus de cinq sources :

- les produits illicites de l'occupation de territoires, tels que le pillage bancaire, l'extorsion, le contrôle des champs et raffineries pétroliers, ainsi que le vol d'actifs économiques et l'imposition illégale des biens et des espèces qui transitent sur le territoire où l'EIL est présent ;
- les enlèvements pour obtenir une rançon ;
- les dons, y compris par des organismes à but non lucratif ou par leur intermédiaire ;
- le soutien matériel, par exemple le soutien associé aux combattants terroristes étrangers ; et
- la collecte de fonds par le biais de réseaux de communication modernes.²

14. De même, un rapport rédigé par l'ONU en 2020 (le Rapport conjoint)³ a conclu que les canaux les plus fréquemment utilisés pour le financement du terrorisme sont :

- le système bancaire formel ;
- la contrebande d'espèces ;
- l'activité de services monétaires ;

² « Financement de l'organisation terroriste de l'État islamique en Irak et au Levant (EIL) », Groupe d'action financière, 2015

³ « Le rapport conjoint de la Direction exécutive du Comité contre le terrorisme et l'Équipe du soutien analytique et de suivi des sanctions en vertu des Résolutions 1526 (2004) et 2253 (2015) concernant l'État islamique en Irak et au Levant (EIL) (Daech), Al-Qaida et les talibans et les personnes et entités associées sur les mesures prises par les États membres pour perturber le financement du terrorisme, préparées conformément au paragraphe 37 de la Résolution 2462 (2019) du Conseil de sécurité des Nations Unies, 2020 ».

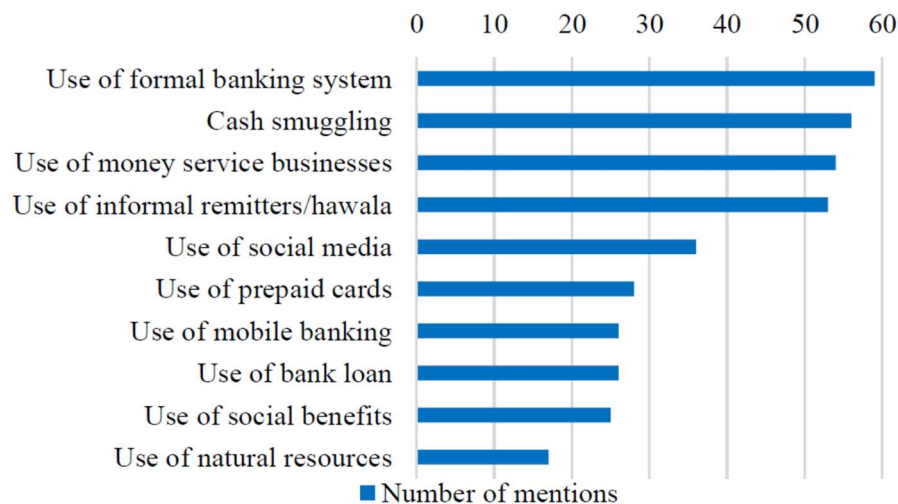
- les prestataires de services de transfert de fonds informels ou le hawala ;
- les dons, y compris par des organismes à but non lucratif ou par leur intermédiaire ;

15. Un autre facteur humain qui a également eu une incidence sur les typologies de FT, souligné par l'analyse consécutive au 11 septembre 2001 des pirates et de leurs actions dans les banques américaines, est qu'il y a eu certains incidents dans lesquels des personnes suspectes impliquées dans le financement du terrorisme ont été repérées par le personnel bancaire de veille en raison de comportements anormaux de faible importance, tels que :

- leur indifférence à l'égard du solde réel lors de retraits importants ;
- leur préoccupation anormale quant à la vitesse du virement, alors qu'ils transfèrent les montants en plusieurs étapes vers la même destination ; et
- un manque apparent de connaissances de base sur la/les destination(s) de la part du déposant/de l'auteur du virement lui-même

16. Le Rapport conjoint souligne également l'abus de technologie (y compris les réseaux sociaux, les cartes prépayées et les services bancaires mobiles) à des fins terroristes, en notant que le FT a été facilité par l'évolution récente des paiements mobiles et l'anonymat des virements et des dons illicites via des plateformes de financement participatif.

17. Le graphique ci-dessous donne une vue d'ensemble des méthodes les plus fréquemment utilisées par les financiers terroristes⁴ :



ANGLAIS	FRANCAIS
Use of formal banking system	Utilisation d'un système bancaire formel
Cash smuggling	Contrebande d'espèces
Use of money service businesses	Recours à des entreprises de services monétaires
Use of informal remitters/hawala	Recours à des prestataires de services de transfert de fonds informels ou au hawala
Use of social media	Utilisation de réseaux sociaux
Use of prepaid cards	Utilisation de cartes prépayées
Use of mobile banking	Recours aux services bancaires mobiles
Use of bank loan	Utilisation d'un prêt bancaire
Use of social benefits	Utilisation d'avantages sociaux
Use of natural resources	Utilisation de ressources naturelles
Number of mentions	Nombre de mentions

⁴ Ibid.

FINANCEMENT DU TERRORISME – ÉTUDES DE CAS

18. La section suivante permettra de mettre en lumière les cas réels de FT survenus dans différents secteurs, dans le but de sensibiliser davantage à ces sanctions et à l'importance de leur mise en œuvre.

Services bancaires

19. Le système bancaire formel est vulnérable au FT en raison de la difficulté de faire la distinction entre les transactions légitimes et illégitimes et de détecter les transactions indirectes. Les programmes de surveillance des transactions sont souvent incapables d'identifier le financement du terrorisme. Il existe également un risque dans l'utilisation des prêts bancaires consentis et des prestations sociales versées par les banques à des fins de FT.

Étude de cas 1 : Accès continu aux comptes bancaires par des combattants terroristes étrangers

20. Selon des informations financières sensibles, des risques de FT ont été découverts en ce qui concerne les retraits d'espèces à l'étranger, par l'intermédiaire de distributeurs automatiques, effectués par des individus inconnus dans des régions situées près des territoires où l'EIIL est présent. Ces retraits ont été prélevés sur des comptes bancaires basés aux États-Unis au moyen d'une carte à puce. Un autre risque de FT identifié résidait dans l'existence de dépôts importants sur des comptes bancaires, suivis de retraits immédiats d'espèces étrangères également dans des zones proches des territoires où l'EIIL est présent. Cette information a révélé les risques liés au FT posés par la capacité continue des personnes qui sont censées se rendre dans des zones occupées par l'EIIL à accéder à leurs comptes bancaires dans leur pays d'origine.

Prestataires de services de transfert de fonds

21. Outre le secteur bancaire, le secteur des transferts de fonds a été exploité pour transférer des fonds illicites et est également vulnérable au FT. Dans les pays où l'accès aux services bancaires est limité, les prestataires de services de transfert de fonds peuvent être la principale institution financière par l'intermédiaire de laquelle les consommateurs peuvent exercer des activités de transfert de fonds transfrontaliers. Les prestataires de services de transfert de fonds sont particulièrement vulnérables aux abus à des fins de FT lorsqu'ils ne sont pas réglementés, ne sont pas soumis à une surveillance appropriée en matière de LCB/FT ou lorsqu'ils exercent leurs activités sans autorisation (exerçant ainsi sans être soumis à des contrôles LCB/FT).

Étude de cas 1 : un Agent d'une ESM complice

22. Une personne a collecté des fonds pour Al-Shabaab au sein de la diaspora somalienne au Missouri et dans d'autres régions. Elle a fait appel à diverses entreprises de services monétaires (ESM) agréées disposant de bureaux aux États-Unis afin de remettre l'argent à la Somalie pour apporter un soutien global aux combattants d'Al-Shabaab. Le co-conspirateur, qui a travaillé pour l'une des ESM impliquées, a aidé la personne concernée à ne pas laisser de trace papier en structurant des transactions à hauteur de faibles montants en dollars et en utilisant de fausses informations d'identification. Le collaborateur de l'ESM et les autres conspirateurs utilisaient des noms et des numéros de téléphone fictifs pour dissimuler la nature de leurs transactions.

Facilités de paiement en ligne

23. Les moyens de paiement en ligne proposés par l'intermédiaire de sites Internet dédiés ou de plateformes de communication facilitent le transfert électronique de fonds entre les parties. Les transferts de fonds sont souvent effectués par virement électronique, carte de crédit ou autres moyens de paiement en ligne. Les moyens de paiement en ligne peuvent être vulnérables à l'usurpation d'identité, au vol de carte de crédit, à la fraude par virement bancaire, à la fraude boursière, aux atteintes à la propriété intellectuelle et à la fraude aux enchères.

Étude de cas 1 : Levée de fonds via Internet

24. Certaines sources de renseignements indiquent que certaines personnes associées à l'EILL ont demandé des dons via Twitter et ont demandé aux donateurs de les contacter par l'intermédiaire de Skype. Il serait demandé aux donateurs d'acheter une carte internationale prépayée (par exemple, un crédit pour une ligne mobile ou d'acheter une application ou un autre programme qui héberge un crédit) et d'envoyer le numéro de la carte prépayée via Skype. Le collecteur de fonds enverrait alors le numéro à l'un de ses abonnés dans un pays proche de la Syrie et vendrait le numéro de la carte à un prix inférieur. Le solde de la trésorerie serait alors versé à un membre de l'EILL.

Étude de cas 2 : Utilisation des Comptes PayPal pour la collecte de fonds

25. En France, une association caritative a été créée en 2010, dont le président était spécialisé dans le marketing en ligne. L'association caritative a proposé plusieurs options sur son site Internet pour faire des dons par carte de crédit, PayPal, au moyen de virements en espèces ou de chèques. Pendant plus d'un an et demi, les comptes bancaires de cette association caritative ont reçu de nombreux dons par chèques et virements électroniques inférieurs à 500 EUR. Sur les 2 millions d'euros collectés, 600 000 EUR provenaient de transactions PayPal d'un autre pays. Les comptes PayPal personnels ont également été utilisés pour collecter des fonds, dans le seul but d'être ensuite retirés en espèces, ou transférés sur d'autres comptes.

Étude de cas 3 : Utilisation des comptes financiers en ligne pour la collecte de fonds

26. Des profits provenant de cartes de crédit volées ont été blanchis par une personne au Royaume-Uni par plusieurs moyens, y compris le virement par l'intermédiaire de comptes de paiement en ligne d'or électronique. Ces comptes ont été utilisés pour acheminer les fonds dans plusieurs pays avant d'atteindre leur destination prévue. L'argent blanchi a été utilisé à la fois pour financer l'enregistrement par le délinquant de 180 sites Internet hébergeant des vidéos de propagande d'Al-Qaïda et pour fournir du matériel à des fins d'activités terroristes dans plusieurs pays. Environ 1 400 cartes de crédit ont été utilisées pour générer environ 1,6 million GBP de fonds illicites pour financer des activités terroristes.

Dons par des organismes à but non lucratif ou par leur intermédiaire

27. Les personnes et les organisations qui cherchent à financer le terrorisme et à soutenir l'extrémisme peuvent tenter de déguiser leurs activités en prétendant se livrer à des activités caritatives ou humanitaires légitimes et peuvent créer des organismes à but non lucratif à ces fins.

Étude de cas 1 : Soutenir le recrutement des combattants terroristes étrangers

28. Al Rehmat Trust, un OBLN présent au Pakistan, a été désigné conformément au Décret présidentiel (DP) des États-Unis n° 13224 comme étant contrôlé par des organisations terroristes désignées, agissant en leur nom et leur apportant un soutien financier. L'on a découvert qu'Al Rehmat Trust servait de société écran pour faciliter les efforts et la collecte de fonds pour une organisation terroriste désignée par l'ONU, Jaish-e Mohammed (JEM). Après son interdiction au Pakistan en 2002, JEM, un groupe terroriste basé au Pakistan ciblé par la RCSNU 1267, a commencé à faire appel à Al Rehmat Trust à titre de société écran pour mener ses opérations.

29. Al Rehmat Trust a apporté un soutien aux activités militantes en Afghanistan et au Pakistan, y compris un soutien financier et logistique aux combattants étrangers présents dans les deux pays. Au début de 2009, plusieurs membres éminents d'Al Rehmat Trust ont recruté des étudiants pour qu'ils mènent des activités terroristes en Afghanistan. Al Rehmat Trust a également participé à la collecte de fonds pour JEM, y compris pour la formation au militantisme et l'endoctrinement au sein de ses mosquées et médersas.

30. Au début de 2009, Al Rehmat Trust a lancé un programme de don au Pakistan pour aider les familles de militants qui avaient été arrêtés ou tués. En outre, au début de 2007, Al Rehmat Trust a collecté des fonds pour le compte de Khuddam-ul Islam, un pseudonyme de JEM.

Étude de cas 2 : Détournement de fonds vers des OBNL

31. Un individu (M. A) a créé une association caritative sous prétexte de recueillir des dons pour les réfugiés syriens, les personnes qui ont besoin d'aide médicale et financière et pour construire des mosquées, des écoles et des garderies. Toutefois, M. A était le chef d'un plan organisé dans le cadre duquel des dons ont été envoyés à un groupe de personnes liées à M. A (Groupe A) au lieu d'être versés sur le compte de l'association.

32. Dans la plupart des cas, la première étape impliquait l'envoi d'argent par l'intermédiaire de prestataires de services de transfert de fonds, puis leur transport en espèces. L'argent a ensuite été transféré sur des comptes de cartes de crédit ou sur des portefeuilles électroniques. Les membres du Groupe A ont publié les informations pertinentes (selon lesquelles les fonds étaient recueillis pour servir les finalités déclarées) sur Internet, mais les fonds ont été envoyés à titre d'aide aux terroristes et à leur famille et destinés à servir de soutien financier aux activités terroristes.

33. Ces informations ont été découvertes dans le cadre d'enquêtes menées par la cellule de renseignements financiers (CRF) du pays, d'après un suivi régulier des entités figurant sur leur liste nationale des entités terroristes désignées et des personnes liées, ou à la lumière des informations fournies par les autorités de poursuite pénale. L'analyse des informations recueillies a permis à la CRF d'identifier la relation entre les différents cas, y compris les payeurs et les destinataires communs et le mode opératoire de collecte et de distribution des fonds.

34. La coopération avec les autorités de poursuite pénale a permis à la CRF d'établir le lien direct entre M. A et l'activité de l'EILL. Cela a donné lieu à plusieurs enquêtes pénales liées à M. A. En outre, ce dernier a été inscrit sur la liste nationale des entités terroristes désignées du pays. Les avoirs des membres du Groupe A ont également été gelés.

Contrebande d'espèces

35. L'argent liquide continue d'être un aspect répandu des opérations terroristes. Bien que les fonds puissent être levés de plusieurs manières, ils sont souvent convertis en espèces ensuite envoyées dans des régions touchées par un conflit. Cette situation est attribuable à des frontières nationales poreuses, à des difficultés à détecter la contrebande d'espèces (en particulier de petits montants qui sont parfois introduits clandestinement à des fins de FT) ainsi qu'à l'existence d'économies informelles et non réglementées.

Étude de cas 1 : Convoyeurs de fonds

36. Sur une période de trois jours consécutifs, trois personnes ont déclaré un montant total d'environ 90 000 EUR en espèces aux agents des douanes de l'aéroport de Bruxelles. Ces fonds provenaient de l'OBNL A de l'Allemagne dans le cadre de l'aide humanitaire au Burundi, au Bénin et au Zimbabwe. Les trois convoyeurs étaient tous des ressortissants belges et vivaient depuis longtemps en Belgique.

37. L'organe de coordination belge d'une organisation islamique radicale a transféré de l'argent sur des comptes détenus par ces trois personnes. Sur une durée d'un an, environ 20 000 EUR ont été retirés en espèces et 10 000 EUR ont été transférés en Turquie. Selon la CRF allemande, l'OBNL A était l'une des plus grandes organisations islamiques d'Allemagne. L'OBNL A aurait été lié à l'OBNL B, qui avait fait l'objet d'une interdiction d'activité en Allemagne pour avoir prétendument soutenu une organisation terroriste. Tous les membres du conseil d'administration de l'OBNL B ont également joué un rôle important au sein de l'OBNL A.

38. Selon les informations communiquées par les services de renseignements belges, les trois personnes susmentionnées étaient connues pour être impliquées dans des branches locales d'une organisation islamique radicale. Compte tenu de la nature des transactions et des liens entre les deux OBNL, les autorités belges soupçonnaient qu'au moins une partie des fonds aurait pu être utilisée pour soutenir les activités terroristes.

Devises virtuelles

Étude de cas 1 : Utilisation du Bitcoin pour les dons

39. Des enquêtes financières sur l'attaque terroriste perpétrée par le tireur de la mosquée de Christchurch en Nouvelle-Zélande en 2019 ont révélé que le tireur avait fait plusieurs dons à des entités d'extrême droite à l'étranger, dont Génération identitaire en France et Martin Sellner en Autriche. Ces dons étaient assortis de commentaires tels que « cadeau » et « continuez à faire du bon travail ». En outre, le Bitcoin a été utilisé pour le transfert de fonds.

40. Il s'est avéré que le tireur était en contact avec des personnes « partageant les mêmes points de vue » via les réseaux sociaux et les forums de discussion.

Étude de cas 2 : Promotion des devises virtuelles à des fins de FT

41. En 2015, Ali Shukri Amin a été condamné à 11 ans de prison, suivis d'une période de mise en liberté surveillée à vie et de contrôle de ses activités sur Internet pour avoir conspiré afin d'apporter un soutien matériel et des ressources à l'EILL.

42. Amin a admis avoir eu recours à des réseaux sociaux pour conseiller et encourager l'EILL et ses partisans. Il a utilisé son pseudonyme sur les réseaux sociaux, à savoir @Amreekiwitness, afin de fournir des instructions sur la façon d'utiliser le Bitcoin pour dissimuler l'apport de fonds à l'EILL.

43. Plus de 4 000 personnes se sont abonnées au compte de réseau social d'Amin, qui a servi de plateforme pro-EILL au cours de plus de 7 000 communications. Plus précisément, Amin a utilisé son compte pour mener des conversations sur les moyens de renforcer un soutien financier pour l'EILL à l'aide d'une monnaie virtuelle et les moyens d'établir un système de don sécurisé ou de fonds destinés à l'EILL.

SIGNAUX D'ALARME POUR LA VIOLATION DES SFC LIÉES AU FT

44. Ci-après figure une liste non exhaustive d'éventuels signaux d'alarme pour la violation des SFC liées au FT qui peuvent aider les IF et les EPNFD à détecter toute opération suspecte relative au FT :

- Un grand nombre de transferts de fonds entrants ou sortants sont effectués par l'intermédiaire d'un compte commercial, et il semble qu'il n'y ait pas d'activités logiques ou d'autres fins économiques pour les transferts, particulièrement lorsque cette activité implique des territoires présentant un risque élevé.
- Les transferts de fonds ne comprennent pas de renseignements sur le donneur d'ordre ou la personne au nom de laquelle l'opération est effectuée, alors que l'on s'attendrait à ce que de tels renseignements soient inclus.
- Les fonds sont envoyés ou reçus par le biais de transferts internationaux en provenance ou à destination de territoires présentant un risque élevé.
- Les opérations de change sont effectuées pour le compte d'un client par un tiers, suivies de transferts de fonds vers des sites n'ayant aucun lien commercial apparent avec le client ou vers des territoires présentant un risque élevé.
- Les opérations de change sont immédiatement suivies par des transferts de fonds vers des territoires présentant un risque élevé.
- Les fonds sont générés par une entreprise appartenant à des personnes de même origine ou par une entreprise impliquant des personnes de même origine provenant de territoires présentant un risque élevé.
- Plusieurs comptes servent à recueillir et à acheminer des fonds vers un petit nombre de bénéficiaires étrangers, à la fois des personnes et des entreprises, en particulier dans les territoires présentant un risque élevé.
- Un client obtient un instrument de crédit ou se livre à des transactions financières commerciales impliquant le transfert de fonds vers ou depuis des territoires présentant un risque élevé lorsqu'il ne semble pas y avoir de raisons commerciales logiques pour traiter avec ces territoires.
- Les transactions impliquant certains territoires présentant un risque élevé, tels que des sites situés au milieu ou à proximité des conflits armés où des groupes terroristes sont présents ou des sites qui font l'objet de contrôles LCB/FT moins importants.
- Un compte ouvert au nom d'une entité, d'une fondation ou d'une association, qui peut être liée à une organisation terroriste suspecte ou impliquée dans celle-ci.
- L'utilisation des fonds par un organisme à but non lucratif n'est pas conforme à l'objectif pour lequel il a été établi.
- Dons de clients pour des causes faisant l'objet d'informations dénigrantes accessibles au public.