Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Pratique du Bureau de communication
en matière de blanchiment d'argent MROS

Typologies négatives

Août 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Pratique du Bureau de communication
en matière de blanchiment d'argent MROS

Typologies négatives

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol
Bureau de communication en matière de blanchiment d'argent (MROS)
3003 Berne

Tél: +41 (0)58 463 40 40
E-mail: meldestelle-geldwaescherei@fedpol.admin.ch

Internet: http://www.fedpol.admin.ch

Table of contents

1 Contexte et but des typologies négatives

Le dispositif suisse de lutte contre le blanchiment d'argent repose sur le fait que c'est l'intermédiaire financier qui effectue les premières clarifications de base concernant d'éventuelles valeurs patrimoniales ou transactions illicites. Le législateur s'est clairement prononcé en faveur d'un système de communication fondé sur la qualité. Dans le droit suisse, on a délibérément renoncé à des communications basées sur des seuils (montants de transaction ou autres seuils quantitatifs définis). Les obligations de diligence inscrites dans la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA)[1] sont structurées en cascade et de façon répétitive. Elles sont énoncées aux art. 3 à 5 LBA et prévoient la vérification de l'identité du cocontractant, l'identification de l'ayant droit économique et le renouvellement périodique de ces obligations. Les obligations de diligence particulières visées à l'art. 6 LBA prévoient quant à elles la clarification de l'arrière-plan et du but des transactions et des relations d'affaires, laquelle doit se fonder sur les risques. Les intermédiaires financiers doivent examiner scrupuleusement les indices et les soupçons. Ce n'est que si ces clarifications n'aboutissent à aucun résultat – c'est-à-dire que les soupçons ne peuvent être dissipés et qu'un soupçon fondé émerge – qu'une communication de soupçons doit être transmise au Bureau de communication en matière de blanchiment d'argent (MROS), conformément à l'art. 9 LBA. La communication de soupçons doit donc être le résultat d'une évaluation détaillée et non d'une simple présomption.

En pratique, le MROS constate régulièrement des disparités qualitatives dans le contenu des communications qui lui sont transmises. Dans certains cas, les faits transmis n'ont quasiment pas été étayés ou le MROS ne peut déterminer si les clarifications requises par l'art. 6 LBA ont été effectuées.

Les analyses du MROS montrent clairement une tendance au defense reporting. Concrètement, cela signifie :

- que les communications de soupçons ne sont pas effectuées en premier lieu en raison d'un soupçon étayé de blanchiment d'argent, mais davantage pour se prémunir contre les risques encourus au niveau pénal ou relevant du droit de la surveillance ;
- que l'intermédiaire financier abaisse délibérément le seuil de communication bien en deçà du niveau requis par la loi et jugé approprié pour lutter contre la criminalité ;
- que le contenu informatif des communications est faible, voire insignifiant, ce qui n'apporte aucune plus-value à la lutte contre la criminalité.

De telles communications ne permettent pas de lutter contre la criminalité financière. Pour que le MROS puisse traiter efficacement une affaire, il faut non seulement qu'il existe des soupçons initiaux suffisants, mais aussi que les faits soient exposés de manière fondée, structurée et documentée sur le fond. C'est la seule façon d'analyser les données, de les classer par ordre de priorité et, si nécessaire, de les transmettre aux autorités de poursuite pénale.

Les « typologies négatives » décrites ci-après ont pour objectif de présenter aux intermédiaires financiers des exemples de cas, dans le cadre desquels la MROS a constaté à plusieurs reprises des faits insuffisamment ou pas du tout élucidés dans une communication de soupçon. Elles doivent servir à sensibiliser les intermédiaires financiers, à améliorer la qualité des données et des informations contenues dans les communications entrantes et, partant, à renforcer l'efficacité du traitement des communications de soupçons par le MROS.

[1] RS 955.0

2 Typologies négatives – examen au cas par cas

Les exemples de cas suivants sont tirés de constatations pratiques du MROS. Il s'agit typiquement de configurations dans lesquelles la MROS reçoit des communications de soupçon portant sur des faits insuffisamment élucidés, sans éléments suffisants indiquant une infraction de blanchiment d'argent, ses infractions préalables, une criminalité organisée ou un financement du terrorisme au sens de l'article 9 de la LBA.

Il appartient exclusivement à l'intermédiaire financier de décider, en tout temps au cas par cas, si des faits concrets relèvent de l'obligation de communiquer au sens de l'art. 9 LBA.

Si des soupçons sont communiqués, les éléments étayant ces derniers doivent être documentés sur la base des résultats des clarifications effectuées en vertu de l'art. 6 LBA et présentés au MROS de manière vérifiable.

3 Tipologies négatives - Constellations individuelles

3.1 Typologie 1 – « Tentative d'ouverture de compte »

Le MROS reçoit de plus en plus de communications de soupçons en lien avec des procédures d'ouverture de compte en ligne (onboarding) interrompues, dans lesquelles aucune relation d'affaires n'a été établie et aucun flux financier n'a été généré (art. 9, al. 1, let. b, LBA). Dans ces cas, il est frappant de constater que les intermédiaires financiers auteurs de la communication n'avaient souvent aucun contact avec le client, n'étaient pas en mesure de procéder à une identification complète de ce dernier et ne disposaient généralement d'aucune information sur les ayants droit économiques ni d'indices laissant présumer une infraction préalable au sens des art. 305bis ou 260ter du code pénal (CP)[2].

Ces communications ne reposent souvent sur aucun indice objectivement vérifiable de blanchiment d'argent ou de financement du terrorisme au sens de la LBA. Une interruption purement technique – par exemple lors du téléchargement de la carte d'identité ou du passeport, de l'identification vidéo ou de la transmission de documents – ne constitue pas un soupçon suffisamment fondé pour transmettre une communication. De même, en l'absence d'autres indices laissant présumer des activités de blanchiment d'argent, la seule annulation de la procédure par le client potentiel en raison d'un désintérêt ou de difficultés d'utilisation ne remplit pas les critères requis pour qu'un soupçon doive être signalé. Dans ces cas, aucun indice objectif et vérifiable ne permet de fonder un soupçon au sens de l'art. 9, al. 1, let. b, LBA. Le recours désormais presque systématique à la technologie dans la procédure d'ouverture de compte – notamment via des applications mobiles ou des portails web – entraîne fréquemment l'échec des relations d'affaires en raison d'interruptions du processus. Dans de telles situations, on ne dispose pas d'indices concrets et objectivement vérifiables laissant présumer une infraction préalable au sens des art. 305bis CP ou un lien avec une organisation criminelles et terroristes au sens de l'art. 260ter, al. 1, CP.

L'extension de la communication de soupçons à ces cas purement formels ou techniques va à l'encontre de l'esprit et de la finalité de l'art. 9 LBA et surcharge le MROS et les autorités de poursuite pénale car les informations sont inexploitables. Le MROS ne peut guère exploiter le contenu de telles communications car elles reposent sur de simples suppositions ou des évaluations générales des risques et ne fournissent aucun indice probant de blanchiment d'argent ou de financement du terrorisme.

3.2 Typologie 2 – « Clients suspects sans lien apparent avec les valeurs patrimoniales incriminées »

Le MROS reçoit régulièrement des communications de soupçons dans lesquelles les intermédiaires financiers signalent uniquement des particularités d'ordre général dans le comportement de leurs clients, sans désigner d'indications concrètes sur les valeurs patrimoniales incriminées ou sur leur provenance (Quel élément a déclenché les vérifications à quel moment, et quels indices ou éléments n'ont pas pu être écartés dans le cadre de ces vérifications ?). Ces communications reposent souvent sur des incohérences diffuses ou des facteurs de risque subjectifs, comme un « modèle d'affaires peu plausible » sans explication consistante, des changements fréquents d'ayants droit économiques ou une structure juridique du client plus complexe que la moyenne.

Bien que ces facteurs puissent en principe constituer des éléments invitant à une surveillance des clients axée sur les risques, ils ne suffisent généralement pas, pris isolément, pour atteindre le seuil légal nécessaire permettant de déclencher une obligation de communiquer au sens de l'art. 9 LBA. Le MROS constate que nombre de ces communications restent vagues dans leurs explications et se limitent à des appréciations générales, sans lien tangible avec une infraction préalable concrète au sens de l'art. 305bis CP (par ex. escroquerie, abus de confiance, corruption, délit fiscal qualifié).

Un soupçon fondé au sens de la LBA requiert davantage qu'une simple évaluation axée sur les risques. Il présuppose des éléments objectivement

[2] RS 311.0

vérifiables qui permettent d'établir un lien avec des valeurs patrimoniales dont on soupçonne qu'elles ont été acquises par des moyens délictueux.

3.3 Typologie 3 – « Informations de tiers »

Le MROS reçoit régulièrement des communications de soupçons qui reposent sur des informations de tiers, par exemple en lien avec des articles médiatiques ou des ordonnances de production de pièces et des décisions de séquestre prononcées par des autorités de poursuite pénale suisses ou étrangères. Pour les intermédiaires financiers, ces informations peuvent servir de base à des analyses plus poussées. Pour qu'il y ait une communication de soupçons au sens de l'art. 9 LBA, il est déterminant que l'intermédiaire financier établit, dans le cadre de ses vérifications liées au blanchiment d'argent, un lien entre ces informations et ses propres relations d'affaires et ne se contente pas de transmettre des informations de tiers. Les exemples suivants sont des typologies spécifiques :

3.3.1 Typologie 3.1 – « Ordonnance de production de pièces »

La simple remise d'une ordonnance de production de pièces ou d'une décision de séquestre prononcée par une autorité de poursuite pénale ne constitue pas en soi un fait devant être communiqué. Ces mesures de procédure pénale servent à la sauvegarde de preuves dans le cadre d'enquêtes ou de procédures pénales en cours et concernent généralement des relations clients, des mouvements de compte ou des historiques de transactions spécifiques.

Un intermédiaire financier qui reçoit une ordonnance de production de pièces ou une décision de séquestre doit vérifier s'il dispose, en plus du contenu de ces dernières, d'informations supplémentaires propres qui permettent de fonder un soupçon de blanchiment d'argent, d'infraction préalable au blanchiment d'argent, de criminalité organisée ou de financement du terrorisme (art. 9, al. 1, LBA, en relation avec l'art. 6 LBA).

3.3.2 Typologie 3.2 – « Compte TWINT »

L'application de paiement TWINT constitue une autre typologie de communications de soupçons. Ces dernières reposent souvent sur des informations selon lesquelles un compte TWINT serait impliqué dans une enquête policière, par exemple à la suite d'une information par une autorité de poursuite pénale, d'une demande de renseignements adressée par une autorité ou d'un indice informel. Dans la majorité des cas toutefois, aucun soupçon concret n'est évoqué ; seule une prétendue implication est mise en avant, sans autre précision quant à l'arrière-plan, aux faits incriminés ou à la personne concernée. À elles seules, ces présomptions ne suffisent pas encore à justifier une communication de soupçons au sens de l'art. 9, al. 1, LBA. En effet, il est nécessaire que l'intermédiaire financier recueille des informations supplémentaires permettant de conclure à un lien avec le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme.

Le simple fait qu'un compte TWINT soit mentionné dans le cadre d'investigations policières ne suffit pas à fonder totalement un soupçon. Les intermédiaires financiers devraient examiner attentivement les situations liées à TWINT afin de déterminer si leurs propres observations ou analyses internes fournissent des éléments supplémentaires permettant de fonder un soupçon (art. 6 LBA), lesquels remplissent les conditions pour le dépôt d'une communication de soupçon conformément à l'art. 9 LBA.

3.3.3 Typologie 3.3 – « Articles médiatiques »

Les articles médiatiques sur des clients d'intermédiaires financiers ou sur leur comportement présumément fautif ne suffisent pas non plus à justifier une communication au sens de l'art. 9 LBA. L'intermédiaire financier doit établir un lien concret entre les informations contenues dans les articles de presse et ses propres relations d'affaires ou des transactions inhabituelles, et présenter dans la communication les éléments qu'il a recueillis dans le cadre de ses vérifications conformément à l'article 6 de la LBA.

3.4 Typologie 4 – « Utilisation de bourses de cryptomonnaies »

Le MROS recense un nombre croissant de communications de soupçons dans lesquelles l'utilisation de cryptomonnaies ou le recours à des prestations

liées à ces dernières figure comme unique élément fondant le soupçon. Ces communications se basent généralement sur le seul fait que des clients échangent par exemple des monnaies fiduciaires contre des cryptomonnaies (ou inversement), déposent des cryptomonnaies sur des comptes gérés par des bourses spécialisées dans ce domaine ou reçoivent des paiements (par ex. salaires, honoraires ou prestations) en cryptomonnaies.

Dans ces cas, le MROS constate régulièrement que la présentation des faits reste très vague et se limite à la simple mention du lien aux cryptomonnaies. Il manque souvent des informations substantielles sur les transactions effectivement réalisées, sur l'ayant droit économique, sur l'origine des fonds ou sur un éventuel contexte délictueux. La seule mention de l'utilisation de cryptomonnaies ou de l'implication d'un prestataire de services crypto ne suffit toutefois pas à fonder un soupçon au sens de l'art. 9, al. 1, LBA.

L'utilisation de cryptomonnaies n'est en soi pas suspecte. À l'instar de l'utilisation de comptes bancaires étrangers, des paiements en espèces ou des constructions fiduciaires, elle constitue un élément de risque potentiel qui doit faire l'objet d'un examen différencié axé sur les risques. Une communication de soupçons au MROS n'est justifiée que si, après que les risques ont été évalués, des éléments concrets indiquent un acte présumé de blanchiment d'argent ou une infraction préalable au blanchiment d'argent présumée.

3.5 Typologie 5 – « Comptes des personnes lésées »

Du point de vue de la MROS, les comptes des personnes lésées constituent une catégorie particulière de communications de soupçon. Il s'agit généralement de situations dans lesquelles des clientes ou clients disposent de fonds acquis légalement, mais se retrouvent, sans faute de leur part, impliqués dans un contexte délictuel à la suite d'une fraude ou de la perte de moyens de paiement.

3.5.1 Typologie 5.1 – « Le client lésé »

La MROS reçoit régulièrement des communications de soupçon dans lesquelles l'origine des fonds ne fait l'objet d'aucun doute et dont les titulaires sont des victimes d'agissements frauduleux. En pratique, il s'agit souvent de ce que l'on appelle des comptes des personnes lésées, par l'intermédiaire desquels des clients honnêtes, victimes de love scams où de fraudes à l'investissement en ligne, transfèrent des valeurs patrimoniales aux escrocs (généralement situés à l'étranger).

L'obligation de communiquer au sens de la LBA vise la répression du blanchiment d'argent en lien avec des valeurs patrimoniales acquises par des moyens délictueux. Dans le cas des comptes des personnes lésées, cet état de fait n'est généralement pas donné, car il s'agit d'avoirs légitimes qui ne parviennent aux criminels qu'à la suite d'un mouvement de fonds. Le transfert en soi peut certes sembler pénalement répréhensible, mais les mesures de procédure pénale pertinentes visent cependant en premier lieu les destinataires des fonds et non le la personne lésée, qui a acquis ses avoirs de manière légale et peut en fournir la preuve.

3.5.2 Typologie 5.2 – « Carte de débit ou de crédit volée »

Le MROS reçoit régulièrement des communications de soupçons en lien avec des cartes de débit ou de crédit volées ou perdues. Ces communications sont généralement effectuées directement après que les clients concernés ont signalé la perte, sans qu'aucune transaction frauduleuse n'ait eu lieu. Il s'agit là d'un cas classique de signalement d'un « compte victime », dans lequel la personne lésée perd ou se fait voler un bien (dans ce cas une carte de paiement) sans qu'elle ait commis une faute.

Les communications faisant uniquement état de la perte de la carte sans autre conséquence ni information sur le contexte n'ont aucune valeur exploitable pour l'analyse du MROS. Dans ce type de cas, il n'est pas possible de donner suite à la communication car ni l'objet de la communication (la carte de paiement) ni son utilisation ne présentent de composante criminelle. La simple disparition d'une carte de paiement ne suffit pas pour présumer un soupçon fondé de blanchiment d'argent, d'infraction préalable au blanchiment d'argent ou de criminalité organisée. Ce n'est que lorsque l'intermédiaire financier honore ses obligations de diligence particulières prévues à l'art. 6 LBA et obtient des informations supplémentaires pertinentes en matière de blanchiment d'argent qu'un soupçon initial pertinent peut émerger. Tant que la carte n'est pas

utilisée ou qu'on ne constate aucune utilisation abusive, il ne peut y avoir de lien avec des valeurs patrimoniales acquises de manière délictueuse et, partant, de soupçon fondé qui justifie une communication de soupçons au sens de l'art. 9 LBA.

3.6 Typologie 6 – « L'intermédiaire financier lésé par une escroquerie »

Le MROS reçoit régulièrement des communications de soupçons de la part d'intermédiaires financiers travaillant pour un établissement qui a lui-même été victime d'escroqueries. En pratique, ces situations concernent souvent des cyberattaques ou des cas d'ingénierie sociale (par ex. arnaque au président) ou résultent d'erreurs internes en lien avec des trafics de paiements manipulés.

Dans ces cas, des valeurs patrimoniales de l'intermédiaire financier lui-même – provenant par exemple des comptes de l'établissement pour lequel il travaille – sont transférées à des criminels opérant souvent depuis l'étranger. L'intermédiaire financier subit ainsi un préjudice financier direct. Il s'agit toutefois d'avoirs d'origine légitime, sans lien avec des infractions préalables commises par des tiers ou avec des opérations relevant du blanchiment d'argent.

L'obligation de communiquer prévue à l'art. 9 LBA présuppose un soupçon fondé selon lequel les valeurs patrimoniales ont été acquises par des moyens délictueux. Toutefois, si l'établissement qui effectue la communication a lui-même subi un préjudice et transfère ses propres fonds à un auteur d'infraction par erreur ou à la suite d'une escroquerie, aucun lien avec une infraction préalable de blanchiment d'argent au sens de la LBA n'est alors généralement établi. De tels cas de figure ne sont par conséquent pas concernés par l'obligation de communiquer l'état de fait au MROS.

3.7 Typologie 7– « Caisses noires »

Le MROS reçoit régulièrement des communications de soupçons en lien avec de prétendues « caisses noires », c'est-à-dire des valeurs patrimoniales qui, selon l'intermédiaire financier auteur de la communication, pourraient être utilisées à l'avenir comme pots-de-vin. Ces communications sont souvent faites dans le cadre de relations d'affaires internationales, en particulier lorsque les risques de corruption sont élevés (par ex. dans les domaines du négoce de matières premières, de la construction, de l'approvisionnement énergétique ou des marchés publics transfrontaliers).

Le simple fait de présumer que certains fonds pourraient être utilisés à l'avenir pour exercer une influence indue ne suffit pas à lui seul pour remplir les conditions légales requises pour une communication de soupçons au sens de l'art. 9, al. 1, LBA. Tant que les valeurs patrimoniales concernées proviennent d'une source légale (par ex. une activité commerciale ordinaire) et que l'on ne fait que présumer qu'elles pourraient être utilisées pour commettre une infraction, on ne peut parler d'origine délictueuse au sens de la LBA. Pour que les éléments constitutifs de l'infraction de blanchiment d'argent au sens de l'art. 305bis CP soient réunis, il faut impérativement qu'une infraction préalable visant l'acquisition délictueuse de biens ait été commise (par ex. corruption, gestion déloyale ou escroquerie). Les éléments constitutifs de l'infraction préalable au blanchiment d'argent sont réunis dès lors que l'acte de corruption a effectivement été commis, en particulier lorsqu'un virement a été effectué sur le compte bancaire de l'agent public ou du titulaire de fonction présumément corrompu. Dans ces cas, l'intermédiaire financier qui gère le compte peut former des soupçons fondés quant à l'origine des valeurs patrimoniales et donner suite à l'obligation de communiquer.

3.8 Typologie 8 – « Délit boursier sans titres cotés en Suisse »

En pratique, le MROS reçoit régulièrement des communications de soupçons en lien avec de présumés délits boursiers au sens des art. 142 (opérations d'initiés) et 143 (manipulation du marché) de la loi du 19 juin 2015 sur l'infrastructure des marchés financiers (LIMF)[3]. À certaines conditions, ces deux types de délits peuvent être considérés comme des infractions préalables au blanchiment d'argent qualifiées au sens de l'art. 305bis CP.

[3] RS 958.1

Conformément aux art. 154, al. 2, et 155, al. 2, LIMF, les opérations d'initiés et la manipulation du marché qualifiées sont considérées comme des crimes au sens du CP dès lors que l'avantage pécuniaire tiré de l'infraction est supérieur à 1 million de francs. L'infraction préalable au blanchiment d'argent justifiant une communication au sens de l'art. 9 LBA est alors qualifiée, pour autant qu'il existe des soupçons fondés quant à l'origine délictueuse des valeurs patrimoniales concernées.

S'agissant de l'obligation de communiquer, il convient de noter que les dispositions pénales des art. 142 et 143 LIMF ne s'appliquent que si les activités commerciales présumées illégales concernent des valeurs mobilières admises à la négociation sur une plate-forme de négociation ou auprès d'un système de négociation fondé sur la TRD ayant son siège en Suisse. Si ces conditions ne sont pas remplies et qu'on ne dispose d'aucun indice laissant présumer que les valeurs patrimoniales concernées sont d'origine illicite, la transmission d'une communication de soupçons au MROS n'apporte aucune plus-value à la lutte contre le blanchiment d'argent.