

## CAS

### 1. Soupçon d'abus de confiance

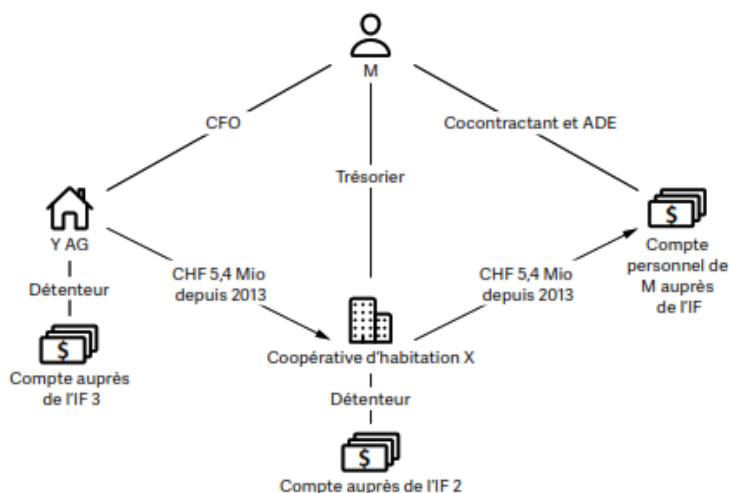
#### Etat de fait

Le conseiller clientèle de l'intermédiaire financier (désormais IF) constate des transactions inhabituelles au crédit du compte privé de M provenant d'une coopérative d'habitation X. D'après les informations du profil client à disposition de l'IF, le client M serait le trésorier de la coopérative d'habitation X. Par ailleurs, M serait également Chief Financial Officer (CFO) et membre du conseil d'administration d'une société de construction Y AG.

L'analyse transactionnelle effectuée par l'IF permet de relever que la relation d'affaires au nom de M a été principalement alimentée par des fonds provenant de la coopérative d'habitation X. Les bonifications anormalement élevées ne s'apparentent pas à des salaires que le client aurait pu percevoir pour son poste de trésorier. Au total, plus de 5 millions de francs provenant d'un compte ouvert auprès d'un intermédiaire financier tiers au nom de la coopérative d'habitation X ont été crédités sur le compte privé de M.

L'IF contacte le client qui, dans un premier temps, affirme toucher des commissions pour des projets de construction menés pour son propre compte. Toutefois, l'IF ne parvient pas à clarifier pourquoi et pour quels projets son client toucherait à ce titre des fonds provenant de la coopérative X. La documentation remise par M à l'IF lors d'un rendez-vous, semble montrer que les fonds versés depuis les comptes de la coopérative proviennent en réalité de la société Y AG, dont M est CFO. Ces fonds transitent par le compte de la coopérative d'habitation X. L'IF n'arrive pas à vérifier l'authenticité de ladite documentation et le rendez-vous ne permet pas non plus de clarifier davantage l'arrière-plan économique de ces transactions.

Ce schéma transactionnel renforce les soupçons de l'IF. Les fonds crédités sur le compte privé du client M pourraient être le produit d'un abus de confiance perpétré par le client en sa qualité de trésorier auprès de la coopérative d'habitation X ou en sa qualité de CFO de la société Y AG. Le fait que la société de construction Y AG ait renoncé à un contrôle ordinaire et à un contrôle restreint suite à une décision du conseil d'administration datant d'avant le début des transactions suspectes renforce le soupçon de l'IF, qui conclut à un potentiel abus de confiance et signale au MROS les relations d'affaires entretenues avec M.



## Solution

### Bonne pratiques de l'intermédiaire financier déclarant

- **Le conseiller client a été attentif et a détecté des transactions suspectes**, ce qui a permis au département compliance de prendre le relais et d'effectuer des investigations complémentaires. Cela montre l'importance des conseillers clients en tant que première ligne de défense du dispositif anti-blanchiment des IF. Il est essentiel de détecter et de clarifier en temps utile des activités suspectes sur les relations d'affaires des clients pour pouvoir prendre rapidement d'éventuelles mesures nécessaires.
- **La documentation exacte de l'IF a permis au MROS de procéder à des clarifications ciblées.** Même si le MROS détecte souvent des nouvelles pistes lors de ses analyses, la documentation et l'évaluation de l'IF constituent le point de départ de l'analyse du MROS. Des informations complètes et précises peuvent augmenter considérablement l'efficacité du Bureau de communication.

## 2. Soupçon de traite d'êtres humains / prostitution forcée

### Etat de faits

Un IF dispose d'une relation d'affaires avec une cliente ayant indiqué tenir un salon de beauté. Il conçoit des soupçons du fait du schéma transactionnel suivant: pendant un an, la relation d'affaires a été alimentée par des paiements fréquents en espèces à hauteur de plus de 70 000 francs au total. Ces versements sont effectués soit par la cliente elle-même, soit par de tierces personnes de sexe féminin. Ce qui frappe l'IF, c'est que certains paiements sont effectués dans une ville donnée en Suisse et que le même montant est ensuite retiré dans une autre ville suisse (ou ailleurs en Europe) dans les jours suivants. L'analyse des transactions et les autres clarifications entreprises révèlent que la cliente et les tierces personnes de sexe féminin impliquées entretient des liens avec le milieu de la prostitution. Dans le cas de l'une de ces transactions de passage vers un pays tiers européen, l'IF découvre, après avoir mené quelques recherches, que le destinataire est le prétendu compagnon de la cliente. Après des investigations plus poussées sur cette personne, l'IF remarque une concordance, dans la base de données World Check, révélant que ce prétendu compagnon de la cliente et destinataire de l'argent serait en lien avec des affaires de criminalité organisée et de traite d'êtres humains. Par ailleurs, l'IF constate des paiements réguliers et fréquents pour des publicités sur des plateformes de divertissement pour adultes. La fréquence de ces achats publicitaires laisse deviner que les paiements sont effectués pour plusieurs personnes. D'autres paiements couvrent le loyer de plusieurs logements, ce qui retient également l'attention de l'IF au regard du profil de sa cliente. Enfin, le comportement et les indications incohérentes et peu plausibles de la cliente incitent l'IF à regarder de plus près cette relation d'affaires. La cliente indique tenir un salon de beauté et affirme que les sommes versées par différentes personnes de sexe féminin correspondent au paiement de soins de beauté. Elle fournit des factures à titre de preuves. Or, en faisant des recherches en sources ouvertes, l'IF ne trouve aucun salon de beauté au nom indiqué en lien avec sa cliente. De plus, il nourrit des doutes quant à l'authenticité des factures justificatives fournies : par exemple, une personne semble avoir reçu un nombre inhabituellement élevé de soins ; or, la cliente se trouvait alors à l'étranger, lorsqu'elle affirme avoir effectué ces soins en Suisse ; dans d'autres quittances fournies, des prestations identiques ont été facturées à des prix différents.

## Solution

### Bonnes pratiques de l'intermédiaire financier déclarant

- **L'IF a détecté rapidement les transactions suspectes et a établi une communication de soupçons immédiatement après avoir mené ses recherches.** La transmission rapide des communications est essentielle pour que le Bureau de communication puisse travailler efficacement. D'une part, cela augmente les chances de traçage ou même de blocage des fonds et d'autre part, les informations obtenues peuvent éventuellement constituer un complément utile pour des procédures déjà en cours en Suisse ou à l'étranger.
- **L'IF a procédé à des recherches approfondies en sources ouvertes.** Il a notamment vérifié l'identité des personnes impliquées ainsi que leur adresse présumée. C'est ainsi qu'il a découvert des liens avec le milieu de la prostitution. Par ailleurs, l'IF a mené une recherche sur World Check concernant le prétendu compagnon de la cliente et l'un des destinataires de l'argent, recherche qui lui a permis de recueillir des informations importantes.
- **Tiping Off: l'IF a discrètement questionné la cliente au sujet des transactions suspectes et a documenté toutes les affirmations incohérentes, incomplètes ou suspectes de cette dernière ;** les informations obtenues des clients sont un élément important de la documentation transmise au MROS en cas de communication (dans la mesure où cela est possible sans alerter les clients en question des soupçons formés à leur rencontre). Le MROS n'est pas autorisé à contacter directement les clients et doit donc s'appuyer sur les informations que l'IF a pu obtenir. C'est souvent le comportement des clients, par exemple la cohérence ou la vérité de leurs affirmations qui fournit les indices pouvant être utiles au MROS lors de l'analyse d'une communication de soupçons. Il est toutefois important que l'IF adopte une attitude critique face à ces informations et indices et qu'il fournisse au MROS tous les éléments à sa disposition afin que ce dernier puisse en évaluer la fiabilité et éventuellement mener des vérifications. L'IF est la personne qui connaît le mieux ses clients et devrait exploiter cet avantage dans son analyse.
- **L'IF a mené une analyse détaillée des transactions et a résumé de manière précise les principaux mouvements bancaires.** Il a notamment procédé à des clarifications concernant les contreparties, analysé en détail les factures fournies par la cliente pour justifier les paiements reçus et vérifié la plausibilité de leur contenu.
- **Les documents / annexes fournis étaient complets et chaque élément de soupçon était documenté.** Aucun document manquant n'a dû être réclamé. Les demandes d'informations supplémentaires effectuées en vertu de l'art. 11a, al. 1, LBA sont coûteuses en temps, aussi bien pour le MROS que pour l'IF déclarant. Selon l'art. 3, al. 1, let. h, OBCBA, l'IF déclarant doit donner une description aussi précise que possible des soupçons sur lesquels se base la communication et fournir tous les documents pouvant être utiles.

## Conclusion

La connaissance des différentes caractéristiques et indicateurs des infractions préalables au blanchiment d'argent est une condition importante pour une stratégie de conformité efficace. Différents éléments, ou une combinaison d'éléments, peuvent conduire à des soupçons d'infraction préalable. Ainsi, les indicateurs à identifier pour un cas de traite d'êtres humains ne sont pas les mêmes que pour un cas de corruption ou de fraude. **Dans le cas d'espèce, l'IF a relevé des indicateurs importants dans la détection de cas de traite d'êtres humains ou de prostitution forcée, notamment les suivants** <sup>1</sup>:

- Paiements fréquents en espèces;
- Versements sur le compte depuis une ville X et retraits correspondant au même montant dans une ville Y (transactions de passage);
- Transferts de montants relativement faibles;

---

<sup>1</sup> Cf. notamment le rapport du GAFI, Financial Flows from Human Trafficking, juillet 2018, qui fournit des explications détaillées sur les indicateurs et les études de cas en vue de reconnaître les situations de traite d'êtres humains et les infractions préalables apparentées.

- Paiements effectués ou reçus par un grand nombre de personnes;
- Transferts de fonds à des personnes ou à des entreprises dans des pays d'où proviennent un grand nombre de victimes de traite d'êtres humains;
- Paiements récurrents et fréquents pour des publicités sur des plateformes en ligne de divertissement pour adultes;
- Dépenses fréquentes pour différents hôtels ou logements de location;
- Dépenses ne correspondant pas au profil KYC du client;
- Liens avec le milieu de la prostitution.

La relation d'affaires a été signalée sur la base d'une approche holistique. Les différents éléments reliés entre eux ne sont pas forcément suspects si on les examine séparément; un lien avec le milieu de la prostitution, par exemple, n'est pas en soi un motif de soupçon suffisant, puisque le travail du sexe est légal en Suisse à certaines conditions. Cet élément peut cependant être indicatif d'une infraction préalable en combinaison avec d'autres facteurs, comme ici le résultat positif dans World Check. L'approche holistique de l'IF a permis de détecter des liens qui seraient passés inaperçus avec une approche plus unilatérale (focalisée sur certains éléments isolés de la relation d'affaires, comme les transactions ou des aspects de l'évaluation KYC).

### 3. Soupçon de blanchiment d'argent professionnel

#### Etat de faits

L'IF monitorise le compte personnel d'un avocat désinscrit du barreau depuis plusieurs années, avec lequel il entretient une relation d'affaires. Il constate l'existence d'une pluralité de donneurs d'ordre dont les virements sont rapidement transférés sur d'autres comptes en Suisse et à l'étranger. Le compte a ainsi été utilisé comme compte de passage, l'avocat jouant le rôle d'Escrow Agent. L'IF demande alors des explications à son client. Il constate que ce dernier se présente aux tiers sous l'étiquette d'un avocat inscrit au barreau, alors qu'il ne l'est plus depuis plusieurs années. L'avocat explique qu'il ne plaide plus mais qu'il a conservé une clientèle qu'il conseille en matière juridique. Il a notamment mis son compte à disposition de ses clients. Selon les dires de l'ancien avocat, l'un de ses clients ne pourrait pas exécuter certaines transactions en raison de dispositions anti-blanchiment d'argent. L'avocat remet plusieurs actes juridiques corroborant ses dires à l'IF. De son côté, l'IF fait des recherches sur les contreparties de l'avocat et identifie des articles de presse et d'autres « hits » négatifs. L'un des clients serait visé par une procédure pénale à l'étranger.

Ne pouvant pas dissiper le soupçon que l'avocat ait blanchi de l'argent pour le compte de ses clients, l'IF communique son compte au MROS.

#### Solution

##### Bonnes pratiques de l'intermédiaire financier déclarant

- **L'IF a orienté ses recherches et ses clarifications auprès de son client en fonction du profil de ce dernier**, lorsque son analyse transactionnelle lui a permis de constater diverses entrées de plusieurs tiers et l'utilisation du compte comme compte de passage.
- **L'IF a fait des recherches approfondies concernant les contreparties**, recherches qui lui ont permis d'identifier des informations négatives qu'il a dûment documentées.

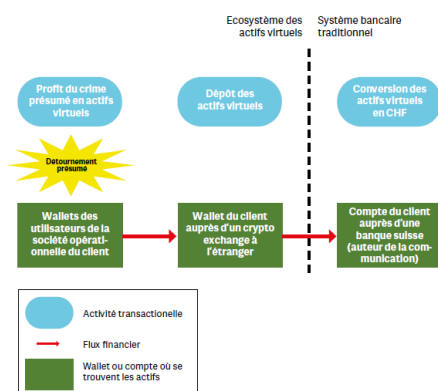
### 4. Soupçon de détournement d'actifs virtuels

#### Etat de fait

Plusieurs clients d'un IF de type bancaire seraient actifs dans le secteur des actifs virtuels notamment via l'une de leurs sociétés opérationnelles, à savoir une plateforme d'échange et d'investissement en cryptomonnaies. Ils auraient généré l'essentiel de leur fortune grâce à cette dernière ainsi qu'au travers d'investissements précoces dans les cryptomonnaies. Après une demande urgente de la part de ses

clients qu'il juge inhabituelle, l'IF porte une attention particulière à ce groupe de relations d'affaires et implique le département de conformité. Parallèlement à cet événement, l'IF relève un comportement transactionnel inhabituel récent sur les comptes. Dans un intervalle de temps court, plusieurs centaines de milliers de francs sont déposés en plusieurs versements sur les comptes des clients en question. Ces fonds proviennent pour une part importante de plateformes d'échange de cryptomonnaies (Exchanges) bien connues et enregistrées dans différentes juridictions. Une partie des dépôts résulte donc vraisemblablement de la conversion ou de la vente d'actifs virtuels. Au regard du contexte, ces transactions semblent suspectes et l'IF entreprend des clarifications. L'hypothèse retenue par l'IF à l'égard de ces transactions semble s'orienter vers un possible détournement de fonds des clients/utilisateurs de la plateforme gérée par les clients de l'IF. D'autres transactions suspectes sont observées dans un second temps et renforcent ce soupçon.

Dans l'ensemble, lors de ses clarifications, l'IF définit très vite un champ d'investigation comprenant l'origine des fonds en cryptomonnaies ainsi que leur conformité fiscale. Les clarifications qu'il a menées s'orientent assez rapidement sur des aspects techniques tel que l'obtention de captures d'écran des comptes de ses clients auprès des échanges et les preuves de provenance des cryptomonnaies sur ces derniers afin de permettre, in fine, la compréhension du Paper Trail. L'IF tente également d'obtenir des preuves de l'existence de la fortune en cryptomonnaies de ses clients, qu'elle soit détenue auprès d'un Exchange ou via des portefeuilles non dépositaires (Private / Self-hosted / Unhosted / Non-custodial Wallet). Le champ d'investigation comprend également la question de la légitimité de l'entreprise de ses clients active dans le secteur des actifs virtuels. Les clarifications effectuées incluent par exemple la question des éventuelles autorisations requises pour cette activité en fonction des juridictions impliquées ainsi que la remise en question des informations publiées sur le site Internet de ladite société. Au terme de ses clarifications, l'IF conclut à un possible détournement de fonds des clients ou d'utilisateurs de la société et signale les relations d'affaires entretenues avec ce groupe de personnes au MROS.



## Solution

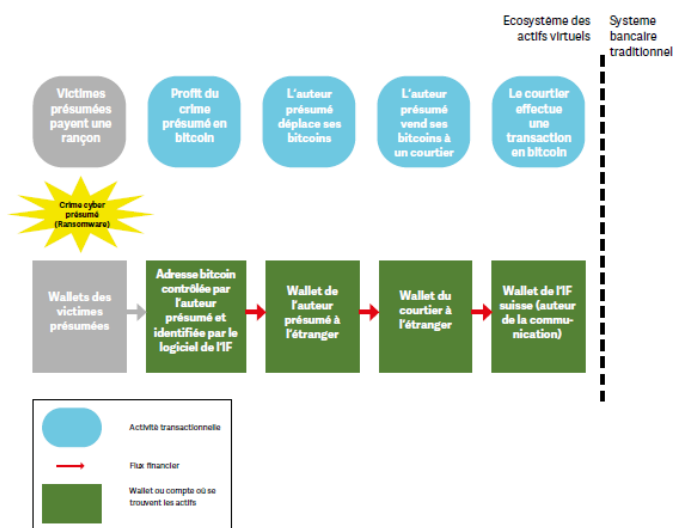
### Bonnes pratiques de l'intermédiaire financier déclarant

L'IF dit « traditionnel » a démontré une excellente compréhension des risques de l'environnement lié aux cryptomonnaies. Bien qu'il n'ait pas été en mesure d'obtenir toutes les clarifications demandées, il a rassemblé et documenté des éléments pertinents et précieux pour l'analyse du MROS relatifs à l'origine des fonds et à l'activité de la société du client. Ces clarifications ont entre autres permis au MROS d'adresser trois demandes de renseignements à des CRF étrangères et d'obtenir des informations liées par exemple à l'origine des avoirs en cryptomonnaies auprès d'une des plateformes ou à la légitimité de la société évoquée précédemment.

## 5. Possible contamination indirecte

### Etat de fait

L'IF est actif dans le courtage de cryptomonnaies et peut être qualifié de prestataire de services liés aux actifs virtuels (on parle de Virtual Asset Service Providers, ou VASP, ou encore d'intermédiaires financiers exerçant une activité de VASP). Dans le cadre d'une revue périodique des transactions, l'un des logiciels d'analyse Blockchain de l'IF identifie un niveau de risque élevé sur des transactions en bitcoins effectuées pour le compte de ses clients. L'alerte générée par l'outil d'analyse semble montrer l'existence d'un lien indirect entre ces transactions et des actes de cybercriminalité de type ransomware<sup>2</sup>. Il apparaît que les transactions suspectes ont pris place dans le contexte de l'acquisition de plusieurs dizaines de bitcoins auprès d'un partenaire commercial à l'étranger. Ces bitcoins ont été acquis pour le compte d'un client de l'IF. Le partenaire commercial société est un courtier de gré-à-gré (OTC broker) et donc également un intermédiaire financier de type VASP soumis à des obligations de diligence et enregistré auprès d'une autorité de surveillance. L'IF financier met dès lors en œuvre un protocole de clarification. Le champ d'investigation défini poursuit, entre autre, deux objectifs. Premièrement, l'IF a cherché à clarifier la situation auprès du courtier afin de comprendre si des clarifications avaient déjà été entreprises de son côté et quel en avait été le résultat. Deuxièmement, l'IF a mené une analyse indépendante et critique afin de comprendre pourquoi le logiciel indiquait un niveau de risque important et si ce résultat pouvait justifier à lui seul une transmission au MROS. Pour ce faire, une analyse approfondie a été menée à l'égard de la source utilisée par le logiciel d'analyse Blockchain lui-même. La question était dès lors de savoir si une infraction avait effectivement eu lieu. De plus, l'analyse menée a notamment compris l'utilisation de différents logiciels d'analyse Blockchain afin de tracer le flux de transactions et d'en comparer les résultats. L'analyse des flux de transactions ainsi que les clarifications effectuées ont notamment conduit l'IF à développer l'hypothèse que si l'infraction avait effectivement eu lieu, il existerait dès lors un lien entre cette dernière et un client de son partenaire commercial à l'étranger. Au terme de son protocole de clarification, l'IF a décidé de signaler le cas au MROS.



<sup>2</sup> Le terme ransomware se réfère à un logiciel malveillant (malware) qui s'installe sur un ordinateur, chiffre les données et/ou bloque l'ordinateur. Il s'agit dans la plupart des cas d'une infection dite de Drive By Download (infection par téléchargement involontaire). Il suffit que la victime consulte un site manipulé depuis un ordinateur insuffisamment protégé pour que le malware s'installe. Les malfaiteurs demandent ensuite une rançon pour que les données soient déchiffrées ou l'ordinateur débloqué. Parfois, le logiciel malveillant envoie aussi une notification apparemment officielle, utilisant des logos policiers en fonction du pays, exigeant de la victime le paiement d'une amende.

## Solution

### Bonnes pratiques de l'intermédiaire financier déclarant

- **L'IF a fait un excellent travail de documentation des clarifications menées auprès d'un autre intermédiaire financier (courtier à l'étranger), de l'analyse Blockchain (remise de schémas visuels), ainsi que de remise en question critique des sources utilisées par l'un de ses logiciels d'analyse.** Sur cette base, le MROS a notamment effectué des analyses complémentaires afin d'évaluer la possibilité

## 6. Aperçu de connaissances tirées des jugements notifiés selon art. 29a, al. 1, LBA

### Traite d'êtres humains et encouragement à la prostitution

En 2021, plusieurs jugements relatifs à la traite d'êtres humains et à l'encouragement à la prostitution, qui ne présentaient pas de liens entre eux, ont été notifiés au MROS. De manière résumée, les victimes, presque exclusivement des femmes et des personnes transgenres dans les cas qui nous occupent, provenaient de deux régions: l'Europe de l'Est et la Thaïlande. Dans les deux cas, les auteurs d'infractions et les victimes étaient originaires du même pays. Les organisations actives dans la traite d'êtres humains présentaient certaines similarités, concernant aussi bien les victimes d'Europe de l'Est que de Thaïlande, mais présentaient également de nettes différences quant à leur structure et à leur manière de procéder.

Les explications suivantes se rapportent aux caractéristiques des victimes thaïlandaises de traite d'êtres humains:

Les structures organisationnelles mises au jour dans le cadre des procédures correspondaient à deux « organisations », l'une en Thaïlande et l'autre en Suisse. Dans les deux pays, les auteurs des infractions étaient principalement des femmes. Des entremetteuses recrutaient les victimes en Thaïlande. Ces dernières savaient certes qu'elles allaient s'adonner à la prostitution, mais n'étaient informées que de manière élémentaire de l'aspect financier et des modalités de remboursement de leurs dettes (frais de « placement », de voyage et de subsistance). Le voyage en Suisse se faisait au moyen de visas obtenus au préalable par les entremetteuses. Souvent, les victimes étaient enregistrées comme prétendues propriétaires d'entreprise, ce qui servait à demander des visas touristiques pour l'espace Schengen. Parfois, l'« organisation » basée en Suisse aidait à acquérir de faux passeports européens qui permettaient d'obtenir en Suisse des autorisations de séjour de type L. À leur arrivée en Suisse, les victimes étaient attendues par des femmes jouant le rôle d'intermédiaires, chargées de les accompagner dans les maisons de prostitution qui leur étaient attribuées. Dès qu'elles arrivaient en Suisse, les victimes étaient sans cesse accompagnées, surveillées et par conséquent isolées socialement. Dans les cas où les victimes arrivaient avec de faux passeports, elles étaient aussi accompagnées lors de leurs démarches administratives (demande de visa, etc.), les auteurs d'infractions attendant parfois devant les bureaux des autorités.

Pour le « placement » et le voyage, les victimes devaient rembourser à leurs entremetteuses un montant situé entre 40 000 et 60 000 francs. Des frais de nourriture et de logement venaient s'y ajouter constamment. Il est ressorti des jugements que les chiffres d'affaires obtenus par les victimes étaient divisés en deux: 50 % étaient versés pour le remboursement des frais de « placement » et de voyage et les autres 50 % revenaient à la tenancière de la maison de prostitution à titre de participation aux frais courants. Les victimes se voyaient donc retirer la totalité de leurs gains. Les transactions étaient effectuées à chaque fois par les tenancières des maisons de prostitution ou par les femmes jouant le rôle d'intermédiaires. Les victimes ne tardaient pas à comprendre qu'elles ne pourraient envoyer qu'une très petite part de leur chiffre d'affaires dans leur pays d'origine pour soutenir leur famille, voire rien du

tout. Un élément essentiel permettant le contrôle des victimes, outre les mauvaises conditions et les intimidations, était le fait que les interlocutrices des victimes étaient souvent des femmes plus âgées. Selon les explications données lors des jugements, le respect des aînés, profondément ancré dans les mentalités en Thaïlande, entraînait une stricte obéissance des victimes. L'analyse du comportement en matière de transactions concernant les relations d'affaires auprès des intermédiaires financiers suisses se fonde entièrement sur les jugements notifiés, vu que le MROS n'a reçu aucune communication de soupçons dans les cas analysés.

Les typologies suivantes ont été identifiées dans les jugements analysés:

- Les victimes ne disposaient d'aucune relation d'affaires propre auprès des banques. Les relations d'affaires étaient établies au nom des auteurs d'infractions.
- Selon les documents KYC, les auteurs n'étaient pas actifs dans le milieu de la prostitution.
- Les auteurs des versements étaient généralement bien plus âgés que les victimes.
- Les rentrées d'argent des auteurs d'infractions sur les relations d'affaires établies à leur nom variaient entre 60 000 et 140 000 francs par an.
- Les versements effectués sur ces relations d'affaires étaient réalisés par des tiers.
- Les sommes versées étaient transférées en Thaïlande, à différents intermédiaires, à titre de remboursement de frais.
- De plus petits montants étaient aussi transférés par les relations d'affaires aux membres des familles des différentes victimes, au moyen de virements bancaires.
- D'autres transactions étaient effectuées à destination des entremetteuses et des membres des familles des victimes par un fournisseur de services de paiement en lieu et place de virements bancaires.

## 7. Devoirs de clarification (KYC)

### Etat de fait

Partenaire contractuel : A SA, sise aux îles Vierges britanniques. L'ayant droit économique est de nationalité indienne et domicilié à Singapour. Selon le système de la banque, l'ayant droit économique a trois autres relations d'affaires avec la banque (deux fondations dont il est le fondateur et le bénéficiaire, une autre société de domicile sise en France).

Actifs sous gestion : 30 millions

Fortune estimée : inconnue

KYC « Société de service –aucune activité opérationnelle. Selon l'ayant droit économique (information téléphonique), le but de ces quatre sociétés est la claire séparation de la fortune. L'ADE (de nationalité indienne) est à la retraite ; il était bijoutier. Sa fortune vient d'investissements »

Que pensez-vous de ce KYC ?

### Solution

- **Aucune** clarification portant sur les motifs de l'utilisation d'une société de domicile (claire séparation de la fortune).
- **Trop peu d'informations et aucune vérification de la plausibilité** de l'origine de la fortune (la fortune vient-elle de l'activité de bijoutier ou a-t-elle une autre origine? Investissements ?)
  - Si investissements : informations trop générales et trop succinctes.
- Moyen de clarifications : **insuffisant** (information téléphonique).

### Attentes de la FINMA

- Justification détaillée et vérification de la plausibilité de la configuration.



- Les informations concernant la source de la fortune et la source des fonds doivent toujours être formalisées et vérifiées.
- Les renseignements oraux du cocontractant seuls ne suffisent pas.

## 8. Surveillance des relations d'affaires

### Etat de fait

La **banque privée X** ouvre cinq relations d'affaires pour le client argentin C et ses sociétés D, E, F et G actives dans le domaine du marketing sportif (vente de droits télévisuels). Objectif du compte privé : investissement d'actifs, actifs attendus : 15 millions de CHF.

1. Le client procède aux transactions commerciales pour toutes les relations d'affaires C à G (environ 5000 sur 10 ans). G n'enregistre que les entrées et les sorties sous le mot-clé consulting.
2. Pour les transactions comportant des risques accrus, le client fournit à chaque fois sur demande des documents contractuels de 100-200 pages.
3. Pour le contrôle annuel des relations d'affaires, le conseiller à la clientèle copie toujours les informations venant du KYC dans le formulaire et le signe.
4. Après deux ans, le compte privé présente un solde de 70 millions de CHF.
5. Après cinq ans, l'attention de la banque est attirée sur des rapports de presse qui établissent des liens entre le client et des cas de corruption. Le client désigne cela sous le terme de « campagne mensongère venant de concurrents ».

Quelles questions posez-vous dans la perspective de la compliance sur ces points ?

### Solution

- Compte privé : **objectif** de la relation d'affaires ? **Consulting**: risque accru de versements corromptionnels.
- Savoir-faire (et capacité) du front et de la compliance pour surveiller les relations d'affaires ?
- La procédure pour vérifier la relation d'affaires/actualiser le fichier KYC est **insuffisante**.
- De forts écarts par rapport aux actifs attendus doivent être expliqués.
- Surveillance des **negative news** : nécessaire, le cas échéant avec recours à des externes.

### Attente de la FINMA

- La banque doit **comprendre** ses clients et disposer du savoir-faire nécessaire au niveau de la compliance et du front.
- Les informations KYC ne sont **pas statiques**, la banque doit surveiller en permanence les relations présentant des risques accrus.
- **Établissement** de relations entre les transactions et les informations KYC.
- **Moyen de clarifications** en fonction du risque.

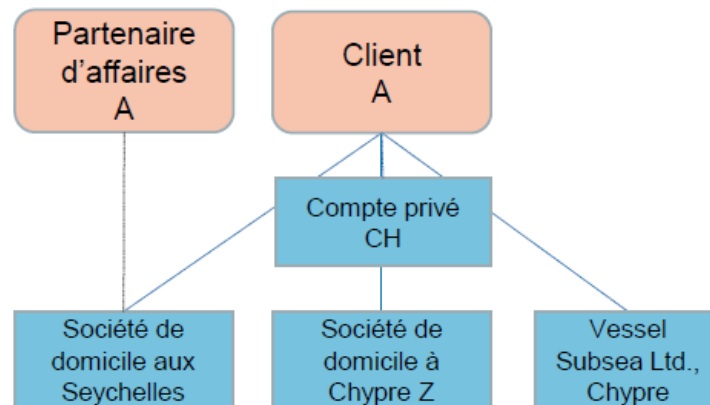
## 9. Traitement des structures complexes

### Etat de fait

La banque X entretient des relations d'affaires avec A. A est norvégien et est domicilié à Monaco. Il est entrepreneur dans le domaine de l'expédition (shipping). Il possède une société opérationnelle « Vessel Subsea Ltd » sise à Chypre. La fortune totale de A s'élève à environ 100 millions de USD. Revenus annuels : 3 millions de USD.

- La banque X entretient en tout quatre relations d'affaires avec A, lesquelles sont **toutes considérées comme « risque normal »**.
- A est impliqué dans trois autres sociétés de domicile comme ayant droit économique. Ces comptes ne sont pas gérés par la banque X.
- Dernière transaction : réception de 15 millions de USD sur le compte Z. Justification: Commission de courtage entre Vessel Subsea Ltd et la société de domicile aux Seychelles

Quelles questions la banque devrait-elle se poser concernant la relation d'affaires A et sa configuration ?



### Solution

- **Présence d'un aperçu complet** de la relation d'affaires A ?
  - La banque a entièrement clarifié et intégralement documenté le réseau de relations et l'aperçu complet de la relation d'affaires avec A.
  - Résultats reproduits dans l'organigramme (y compris parties impliquées et flux d'argent).
- Avons-nous affaire à une **structure complexe**?
  - Oui, car il y a plusieurs sociétés de domicile qui sont gérées par des actionnaires fiduciaires. La banque dispose d'indices clairs selon lesquels les deux sociétés de domicile ouvertes auprès de la banque X font partie d'une structure complexe plus importante de A. Flux de paiements entre sociétés de domicile
- **Quel est le risque de la relation d'affaires avec A ?**
  - Remettre en question l'évaluation des risques de la banque X.
  - La complexité des structures nécessite une classification en tant que relation d'affaires comportant des risques accrus (RRA).

### Attentes de la FINMA

- Éviter des **déclarations générales** comme « protection des actifs », « optimisation fiscale » pour justifier le recours à des sociétés de domicile.
- Les structures complexes doivent être classifiées comme relation(s) d'affaires comportant des risques accrus (**RRA**) (dans le cas contraire, justifier obligatoirement pourquoi il ne s'agit pas d'une RRA) -> **clarifications approfondies** nécessaires !
- La banque examine les **paramètres de risque appropriés** concernant le **recours aux sociétés de domicile**.

## 10. Devoirs de clarification (KYT)

### Etat de fait

1. La **banque régionale Z**, de taille moyenne, a l'entreprise brésilienne B comme cliente. Réception de 150 millions de USD, selon le client venant d'une transaction judiciaire avec une société pétrolière étatique.
2. Le client souhaite le transfert immédiat de 100 millions de USD à une banque privée genevoise.
3. La banque reçoit un document de 30 pages en portugais qui documente le règlement d'un différend dans le domaine de contrats d'affrètement de navires pétroliers. La banque consigne en interne une « indemnisation pour une nationalisation » comme motif juridique pour les versements.
4. En outre : afflux de 10 millions d'EUR, selon le client « Remboursement d'un prêt privé ». Contrat de prêt : signature non datée, durée de 28 jours, aucun intérêt, pas de mention du but d'utilisation.

Quelles questions posez-vous dans la perspective de la compliance sur ces points ?

### Solution

- Les **transactions judiciaires** sont souvent utilisées pour cacher un autre but du versement.
- **Opération de passage manifeste**, risque : la banque n'a pas de vision globale (par ex. versements à des fonctionnaires de la société pétrolière étatique).
- La banque a manifestement des problèmes à comprendre le contenu et la langue des documents transmis. Question: **le client convient-il à l'activité de la banque ?**
- La banque voit uniquement le remboursement du prêt –aucune possibilité de contrôler si un versement a effectivement eu lieu. En outre : le contrat contient plusieurs éléments suspects.

### Attentes de la FINMA

- La banque doit comprendre ses clients et disposer du savoir-faire nécessaire au niveau de la *compliance* et du *front*.
- **Surveillance des transactions** : examen suffisamment critique, demande de justificatifs, clarifications sérieuses voire examen du droit ou du devoir de communication.