



Association Romande des Intermédiaires Financiers

Rue de Rive 8 - Case postale 3178 - 1211 Genève 3
Tél. +41 22 310 07 35 - Fax +41 22 310 07 39 - www.arif.ch - info@arif.ch
CHE-101.192.434 TVA

Circulaire sur la prévention contre le smurfing

Date : 01.01.2026

Chers Membres,

Par la présente nous souhaitons vous communiquer les exigences et les bonnes pratiques en matière de prévention du "Smurfing" ¹ dans le cadre des opérations de change.

Rappel :

Dans l'activité de change toutes les transactions sont assujetties à la LBA, quel que soit le montant de l'opération de caisse effectuée, y compris celles portant sur des montants qui n'excèdent pas le seuil de 5'000 francs pour le change FIAT ou 1'000 francs pour les monnaies virtuelles.

Dans ces deux cas cependant (change FIAT <CHF 5'000 ou change monnaie virtuelle < CHF 1'000), la vérification de l'identité du cocontractant et l'identification de l'ayant droit économique ne sont pas obligatoires s'il n'existe pas d'indices de blanchiment ou de soupçons de smurfing.

Que ce soit par le biais d'une machine ou au guichet, votre bureau de change doit être en mesure d'empêcher qu'un même client puisse changer une somme supérieure aux deux limites mentionnées ci-dessus, lors d'une ou plusieurs opérations liées.

S'il existe plusieurs guichets ou succursales, les visites fréquentes d'un même client doivent être identifiées dans la mesure du possible. Un tel contrôle peut s'effectuer par un logiciel de reconnaissance faciale. La mémoire visuelle ne suffit pas et doit être associée avec des mesures techniques appropriées.

Nous recommandons de saisir toutes les transactions dans un système électronique de paiement, commun pour tous les guichets d'une même officine, et pour toutes les succursales de l'entreprise. Un tel monitoring doit permettre d'identifier les clients réguliers et de détecter des similarités entre plusieurs opérations financières, et ainsi de déceler le smurfing.

L'utilisation de caméras de surveillance peut s'avérer efficace dans certaines situations mais doit être couplé à un système électronique de reconnaissance faciale ou autre moyen technique visant le même but de prévention du smurfing.

Dans la pratique, certains bureaux de change réduisent le risque de smurfing en appliquant des seuils plus restrictifs, ou un intervalle de 30 jours pour les transactions FIAT liées, comme c'est déjà obligatoire en présence d'actifs virtuels.

Lors d'utilisation de machines, en particulier dans l'exploitation des distributeurs automatiques de bitcoins, il est impératif qu'un système préventif existe pour empêcher une même personne non identifiée de changer plus de CHF 5'000.- en FIAT, ou plus de

¹ Placements fractionnés ou transferts de fonds multiples (smurfing ou structuring) de montants en principe inférieurs aux seuils de surveillance.

Il s'agit probablement de la méthode la plus courante de blanchiment d'argent. Elle nécessite l'implication de plusieurs personnes (smurfs/schtroumpfs) ou d'une même personne fractionnant les montants en-dessous des limites de détection.



Association Romande des Intermédiaires Financiers

Rue de Rive 8 - Case postale 3178 - 1211 Genève 3
Tél. +41 22 310 07 35 - Fax +41 22 310 07 39 - www.arif.ch - info@arif.ch
CHE-101.192.434 TVA

l'équivalent de CHF 1'000 en crypto monnaies par mois. Cela n'est possible qu'au moyen de mesures techniques, notamment en bloquant les transactions provenant du même numéro de téléphone portable, ou en utilisant la reconnaissance faciale.

La prévention du smurfing par le biais d'un téléphone portable sur lequel s'affiche un code devant être reporté sur la machine afin de valider la transaction est acceptable. Il faut cependant que la machine puisse bloquer les transactions d'un même client dès que le seuil limite est atteint dans une période de 30 jours.

Cependant, compte tenu des progrès techniques dans les logiciels de change-machines, le système de reconnaissance faciale est un moyen, certes coûteux, mais techniquement mieux adapté que celui du téléphone portable.

Pour les cryptomonnaies, il est aussi recommandé de collecter le numéro de wallet en couplant la vérification et le monitoring des transactions avec une base de données telle Chainalysis par exemple.

Si l'un des éléments au moins est identique entre deux transactions, il faut procéder à l'agrégation des volumes et appliquer le seuil de l'équivalent de CHF 1'000 en crypto monnaies, avant qu'une nouvelle transaction ne soit effectuée.

Enfin, aucune disposition technique n'est requise pour les modèles d'entreprise qui proposent aux clients occasionnels de changer des cryptomonnaies uniquement en relation avec un compte bancaire ou une carte de crédit au nom du client, étant donné que les clients concernés ont déjà été identifiés lors de l'ouverture du compte ou de l'émission de la carte de crédit et que les fonds utilisés pour le change présentent moins de risques de provenir de sources criminelles.

Ces contrôles doivent être clairement annoncés aux clients, soit par une information écrite sur la vitre du guichet, soit directement à l'écran pour le change-machine. Les informations recueillies peuvent être détruites à intervalles réguliers, mais cette destruction doit respecter la période de contrôle de 30 jours à laquelle s'ajoute une période de latence permettant à une éventuelle enquête judiciaire de pouvoir recueillir ces informations (par exemple 90 jours supplémentaires).

Nous vous prions d'agréer, chers Membres, nos meilleures salutations.