Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA sur la surveillance 02/2026

Risques de fraude numérique pour les banques et les personnes au sens de l'art. 1*b* LB

9 avril 2026

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

1 Introduction et définitions

Depuis fin 2022, la FINMA constate une augmentation continue des cas de fraude numérique chez les banques (ci-après : les établissements). Les dernières avancées technologiques risquent de renforcer encore cette tendance. Il s'agit notamment des progrès de l'intelligence artificielle et de la transition numérique visant à accroître l'efficacité au moyen de l'automatisation, par exemple dans l'accès en ligne aux comptes bancaires ou le traitement des paiements avec les paiements instantanés.

Compte tenu de la diversité des formes que prennent ces fraudes numériques, il n'est pas possible de formuler une définition définitive et universelle. Le terme s'entend donc généralement de manière fonctionnelle plutôt qu'en tant que définition rigide. Les fraudes numériques incluent les escroqueries utilisant des technologies numériques, des systèmes d'information ou des moyens de communication électronique à des fins de tromperie dans le but de causer un préjudice financier. On peut typiquement citer l'usurpation et le vol d'identité ou l'incitation par des tiers mal intentionnés à ouvrir en ligne des comptes bancaires servant ensuite à des fins frauduleuses. Le vol d'identifiants ainsi que l'ouverture de comptes en ligne au moyen de documents d'identité falsifiés constituent aussi des risques considérables[1].

Les risques de fraude numérique peuvent menacer les banques et les personnes au sens de l'art. 1*b* de la loi du 8 novembre 1934 sur les banques (LB ; RS *952.0*) de différentes manières. Ils peuvent d'une part toucher directement les banques et leur personnel, par exemple par le biais de l'usurpation d'identité du CEO[2] et de la fraude aux virements bancaires. D'autre part, les clients des banques peuvent aussi être victimes d'escroqueries numériques, par exemple dans le cadre de *real time phishing*[3]. Dans de telles situations, les établissements doivent immédiatement identifier les tendances en matière de fraude et remédier aux éventuelles failles de sécurité pour éviter toute nouvelle tentative d'abus ou de manipulation. Cela vaut notamment lorsque l'infrastructure numérique ou l'identité des établissements sont utilisées à des fins frauduleuses de manière ciblée et systématique. Dans ce cas, une défaillance structurelle recèle non seulement des risques juridiques considérables pour l'établissement, mais elle est aussi susceptible de causer une importante

[1] À cela s'ajoutent, par exemple, l'usurpation d'identité du client, différentes formes d'hameçonnage, le piratage de comptes et les paiements *push* autorisés ainsi que différentes formes d'ingénierie sociale, notamment la fraude au CEO et la *wire fraud*. Des études révèlent par ailleurs que de nombreuses tentatives d'escroquerie détectées dans le secteur financier et des trafic ces paiements en Europe font appel à l'IA générative.

[2] Escroquerie reposant sur des demandes de paiement prétendument urgentes émanant de cadres supérieurs.

[3] Escroquerie dans le cadre de laquelle les pirates obtiennent, par le biais d'interactions, des identifiants bancaires ou des codes d'autorisation afin de prendre le contrôle des comptes et d'effectuer des paiements frauduleux.

atteinte à la réputation qui peut affecter durablement la confiance des clients. Les risques de fraude numérique constituent donc des risques opérationnels majeurs ainsi que des risques juridiques et de réputation, auxquels l'établissement doit à tout moment accorder une attention particulière en mettant en place des mesures organisationnelles et techniques appropriées.

Fin 2025, la FINMA a mené une enquête sur les services bancaires numériques auprès de dix-neuf banques relevant de différentes catégories de surveillance. Dans la présente communication sur la surveillance, elle partage les constatations faites dans le cadre de cette enquête et de ses autres activités de surveillance. L'objectif est de sensibiliser les banques et les personnes au sens de l'art. 1*b* LB aux risques de fraude numérique afin qu'elles mettent en place un dispositif de protection efficace.

2 Bases juridiques

Les banques et les personnes au sens de l'art. 1*b* LB sont tenues de mettre en œuvre une gestion des risques adéquate dans le cadre de leurs activités. Cette gestion des risques doit couvrir l'ensemble des activités et être organisée de façon que l'ensemble des risques essentiels puissent être détectés, évalués, gérés et surveillés. Comptent particulièrement au nombre de ces risques les risques opérationnels ainsi que les risques juridiques et de réputation. Pour les banques et les personnes au sens de l'art. 1*b* LB, l'obligation d'identifier, de limiter et de surveiller leurs risques découle principalement des exigences organisationnelles selon les art. 1*a*, 1*b*, 3 al. 2 let. a et 3*c* LB en relation avec les art. 12 al. 2 et 14*e* de l'ordonnance du 30 avril 2014 sur les banques (OB ; RS *952.02*). La FINMA a précisé sa pratique de surveillance relative à cette obligation dans sa circulaire 2023/1 « Risques et résilience opérationnels – banques ». En matière de prévention du blanchiment d'argent, les obligations de diligence correspondantes découlent notamment des art. 3 à 6 de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA ; RS *955.0*) ainsi que des art. 13 ss de l'ordonnance de la FINMA du 3 juin 2015 sur le blanchiment d'argent (OBA-FINMA ; RS *955.033.*0). La circulaire de la FINMA 2016/7 « Identification par vidéo et en ligne » concrétise par ailleurs la pratique de surveillance en matière de fourniture numérique de services financiers.

3 Constatations et indications issues de l'enquête sur les services bancaires numériques

L'enquête sur les services bancaires numériques a révélé différentes lacunes dans la gestion des risques de fraude numérique chez les

établissements interrogés. Un besoin d'action concret apparaît ainsi en ce qui concerne la gestion opérationnelle des risques de fraude numérique (y c. la gouvernance et la gestion des risques, la détection et la réaction face à ces risques), le traitement des utilisations abusives de comptes ouverts en ligne ainsi que la prévention du blanchiment d'argent.

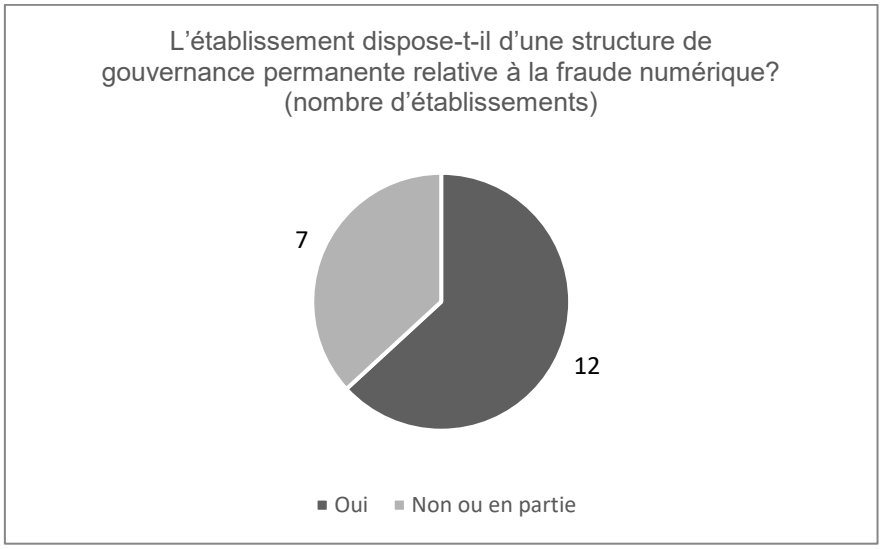
3.1 Gestion opérationnelle des risques de fraude numérique

3.1.1 Gouvernance et gestion des risques de fraude numérique

Constatations

L'enquête a révélé que de nombreux établissements ne disposaient pas de structures de gouvernance claires en lien avec les risques de fraude numérique. Or les fraudes numériques sur le marché financier suisse peuvent entraîner des pertes considérables tant pour les clients que pour les établissements financiers. Selon le rapport annuel 2024 de l'ombudsman des banques, l'escroquerie était ainsi la cause la plus fréquente des litiges soumis[4].

Douze des dix-neuf établissements interrogés ont indiqué disposer de structures de gouvernance permanentes relatives à la fraude numérique. Il s'agit, à cet égard, le plus souvent de regroupements de personnes[5], sans répartition claire des tâches et des responsabilités ni réglementation précise et documentée des compétences.

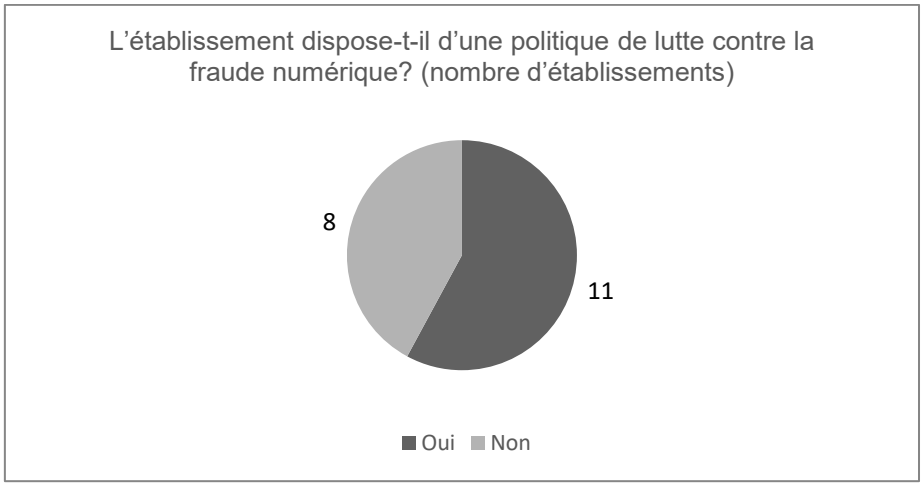


[4] Cf. Rapport annuel 2024 de l'Ombudsman des banques suisses, p. 8.

[5] Par exemple issues des entités *security operations*, *payments*, *risk management* et informatique.

Par ailleurs, trois des établissements interrogés ont indiqué ne disposer d'aucun organe de pilotage chargé des risques de fraude numérique. Il convient en revanche de souligner les résultats obtenus par la mise en place de *fraud desks* interdisciplinaires chargés de la gestion globale des exigences, des contrôles et des processus en matière de gestion des risques de fraude numérique avec une hiérarchie clairement définie.

Bon nombre des établissements interrogés ne disposent pas de directives spécifiques concernant la gestion des risques de fraude numérique. Ces questions sont plutôt traitées dans d'autres directives (notamment celles relatives aux transactions pour compte propre des collaborateurs, au blanchiment d'argent ou à la sécurité de l'information) sans que ces directives ne soient harmonisées entre elles. En conséquence, huit des dix-neuf établissements (42 %) ne disposent d'aucune politique de lutte contre la fraude numérique.



Par ailleurs, seule la moitié environ des établissements interrogés présentent régulièrement, dans leurs rapports à la direction, des indicateurs relatifs aux cas de fraude numérique.

Indications

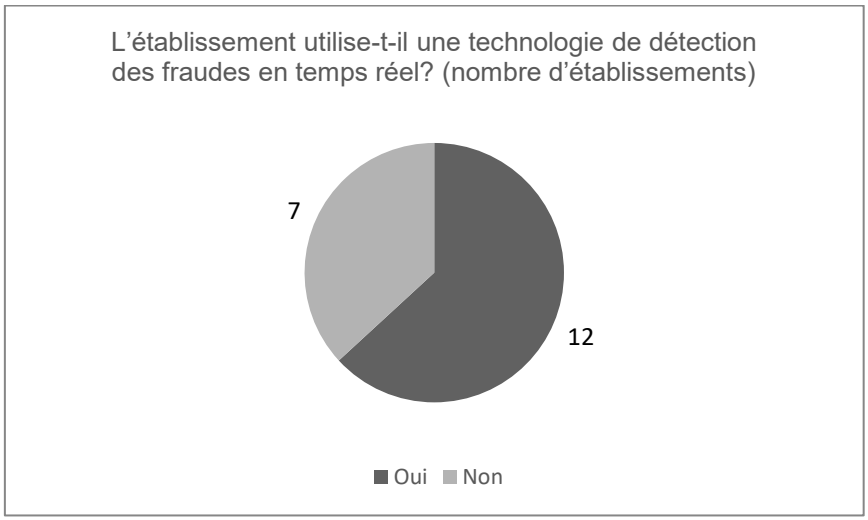
La FINMA attire l'attention sur le fait que les risques de fraude numérique peuvent être importants pour l'établissement. Ils doivent donc être identifiés, évalués, gérés et surveillés de manière globale au moyen de règles régissant les responsabilités et les procédures internes. Conformément à la pratique de surveillance de la FINMA, les établissements doivent mettre en place, dans le cadre de leur gouvernance et de leur gestion des risques, les structures, les directives, les processus et les contrôles nécessaires pour atténuer ces risques opérationnels.

3.1.2 Identification et réaction face aux tendances en matière de fraude numérique

Constatations

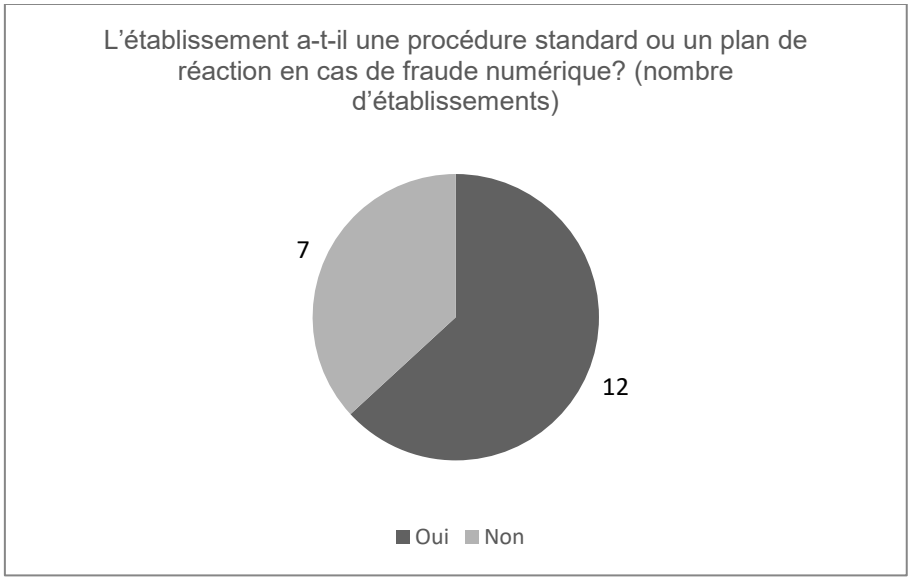
L'enquête a révélé que 26 % des établissements interrogés ne disposaient d'aucun processus permettant d'identifier et d'anticiper les tendances en matière de fraude numérique (*horizon scanning*). Ces établissements ne sont donc pas en mesure d'identifier activement les menaces et les scénarios de fraude pertinents pour leurs services numériques et ne peuvent par conséquent pas prendre les mesures de prévention qui s'imposent.

Douze des dix-neuf établissements utilisent des technologies de détection des fraudes en temps réel.



À l'inverse, sept établissements ont indiqué analyser aucun indicateur des campagnes de fraude numérique en cours, ou ne le faire que manuellement ou au cas par cas. Cela complique l'identification globale de schémas pertinents à plusieurs niveaux. En raison de leur forte dépendance vis-à-vis des prestataires de services, tous les établissements ne sont par ailleurs pas en mesure d'adapter rapidement les règles de détection pertinentes, ce qui compromet la capacité à réagir rapidement face à des séries ou des schémas de fraude identifiés.

L'enquête a aussi révélé un besoin d'harmonisation en ce qui concerne les procédures de réaction et les directives correspondantes. Sept des dix-neuf établissements interrogés n'avaient aucune procédure standard, ni aucun plan de réaction en cas de fraude numérique.



Seuls sept établissements sur les dix-neuf ont par ailleurs déclaré mettre à jour leurs plans de réaction au moins une fois par an. Les autres établissements interrogés mettent seulement leurs plans de réaction à jour en fonction des circonstances, c'est-à-dire de manière ad hoc à la suite d'un incident. De manière générale, la plupart des établissements n'ont pas fixé de délais de réaction pour signaler les cas de fraudes numériques et ils ne les mesurent ni ne les contrôlent. Seuls quelques-uns des établissements interrogés disposent de canaux de signalement disponibles 7 jours sur 7, 24 heures sur 24. De plus, ils sont rares à disposer de canaux spécifiques pour signaler les fraudes. Ils traitent plutôt ces signalements par le biais de la ligne d'assistance téléphonique générale.

Indications

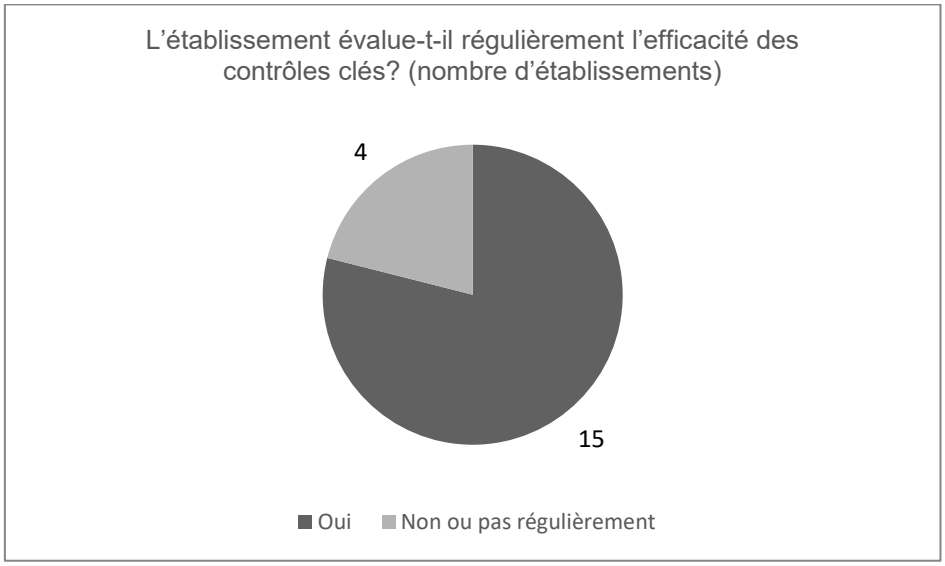
Pour lutter efficacement contre les risques de fraude numérique, il est nécessaire de mettre en place un système de détection proactif, rapide et systématique à l'échelle de l'établissement et des mesures appropriées doivent être prises immédiatement en cas de fraude. Des mécanismes de détection insuffisants et des temps de réaction trop longs peuvent entraîner une multiplication ou une aggravation des cas de fraude, une fuite irrémédiable d'actifs et l'incapacité d'empêcher à temps des transactions de blanchiment d'argent.

3.1.3 Contrôles et évaluation de l'efficacité des mesures de prévention de la fraude

Constatations

Trois des établissements interrogés n'utilisent aucun contrôle technique, tel que le géoblocage, l'évaluation des risques liés à l'adresse IP ou le

fingerprinting des appareils pour authentifier leurs clients. Quelque 20 % environ des établissements interrogés n'ont aucun contrôle clé en tant qu'outil de contrôle central face aux risques de fraude numérique ou n'en évaluent pas régulièrement l'efficacité.



Certains établissements interrogés ont indiqué qu'ils ne prévoyaient pas de former davantage leurs collaborateurs aux risques liés à la fraude numérique. Les autres établissements organisent certes des formations, mais celles-ci se limitent souvent à des informations générales sur les risques de fraude numérique, sans tenir compte des rôles spécifiques ni du domaine d'activité et de l'exposition au risque des participants (par ex. les conseillers à la clientèle). Les moyens utilisés et la fréquence des formations destinées à sensibiliser les collaborateurs et les clients varient en outre considérablement. Tous les établissements interrogés n'identifient pas non plus les segments de clientèle particulièrement vulnérables ou exposés aux risques de fraude numérique.

Indications

Étant donné que les mesures de prévention et de lutte contre la fraude numérique s'appliquent généralement à différents niveaux, leur intégration et leur efficacité doivent faire l'objet de rapports détaillés et être régulièrement vérifiées au moyen de contrôles appropriés.

Les risques de fraude numérique sont en constante évolution. La formation régulière des collaborateurs ainsi que la sensibilisation des clients constituent donc des outils de prévention essentiels pour mieux faire prendre conscience des schémas de fraude potentiels.

3.2 Utilisation frauduleuse de comptes ouverts en ligne

Constatations

Dans le cadre de son activité de surveillance, la FINMA constate que les cas de fraude impliquant des comptes clients ouverts en ligne se sont multipliés ces dernières années. Les organisations criminelles tentent, en recourant à des moyens techniques de plus en plus sophistiqués, d'ouvrir illégalement des comptes bancaires permettant de transférer des fonds d'origine illicite. Ils développent et utilisent ainsi des techniques toujours plus complexes pour contourner les mécanismes de contrôle réglementaires lors de l'ouverture d'un compte.

Dans le cadre de l'ouverture numérique de relations clients, l'ouverture frauduleuse de comptes (documents d'identité falsifiés ou usurpation d'identité) constitue notamment un risque. Ce risque augmente avec l'utilisation accrue de l'intelligence artificielle, des logiciels de manipulation vidéo et des technologies d'hypertrucage. Les organisations criminelles exploitent largement les nouvelles possibilités offertes par la technologie et il est toujours plus difficile de détecter les vidéos manipulées et les documents d'identité falsifiés. Les résultats de l'enquête ne permettent cependant pas de confirmer clairement que l'ouverture numérique de relations bancaires fait l'objet d'une recrudescence de fraudes. On note toutefois une augmentation notable du nombre de communications au MROS en lien avec des relations clients établies par voie numérique. Outre les ouvertures de comptes frauduleuses, on constate une recrudescence des cas dans lesquels des personnes sont amenées, par des moyens frauduleux et sous de faux prétextes, à ouvrir des comptes en ligne et à céder ensuite les droits d'accès à des tiers malveillants. Des malfaiteurs parviennent aussi, au moyen de méthode de cybercriminalité (par ex. des attaques d'hameçonnage), à prendre le contrôle de comptes appartenant à des tiers. Le problème est que les obligations de diligence en vigueur sont souvent respectées dans le cadre de la procédure d'ouverture dans ce sens que le compte est ouvert sur la base de documents d'identité valides. L'acte frauduleux proprement dit intervient dans une étape ultérieure, lorsque des tiers prennent le contrôle des comptes.

Indications

Les mécanismes de sécurité complémentaires revêtent une importance capitale en raison des risques accrus liés à l'ouverture de comptes en ligne. Il s'agit par exemple d'utiliser les moyens techniques pour reconnaître les hypertrucages et les vidéos manipulées. Dans le cadre d'une gestion des risques appropriée, les collaborateurs doivent aussi suivre régulièrement de formations initiales et continues sur ces évolutions (cf. Cm 8 Circ.-FINMA 16/7). Les risques généraux liés à l'ouverture numérique de relations clients et les risques d'accès non autorisé aux comptes ne doivent par ailleurs pas

être considérés isolément mais dans le cadre d'une stratégie de prévention globale de la fraude.

3.3 Prévention du blanchiment d'argent

Constatations

L'enquête révèle que le nombre relatif de communications de soupçons de blanchiment d'argent liées à des cas de fraude (sur Internet), d'usurpation d'identité, de vol d'identité, d'accès illicite à des comptes, de *money muling,* etc. varie d'un facteur dix entre les établissements interrogés. La proportion d'indices internes à la banque donnant lieu à des communications de soupçons au MROS varie quant à elle entre 12 % et 78 %. Dans l'ensemble, les réponses à l'enquête révèlent donc des différences notables entre les établissements en ce qui concerne l'efficacité des dispositifs, des systèmes et des processus de lutte contre le blanchiment d'argent pour détecter les scénarios de fraude.

Selon l'enquête, les informations recueillies dans le cadre de la procédure *know your customer* (KYC) sont généralement assez succinctes. La plupart des établissements renoncent en outre à utiliser les informations KYC collectées pour la surveillance des transactions, par exemple au moyen de scénarios ou de limites différenciés. En règle générale, les informations KYC servent seulement à des fins de vérification de la plausibilité dans le cadre de clarifications concrètes. Dans le cadre du suivi des transactions, la plupart des établissements interrogés ont fixé des seuils relativement élevés à partir desquels les opérations de passage sont identifiées comme des transactions à risque accru (TRA) pour des clients privés présentant un risque faible ou normal (100 000 ou 200 000 francs). Cela semble indiquer que les systèmes sont peu sophistiqués et identifient principalement les TRA sur la base de limites fixes plutôt qu'à partir de scénarios spécifiques. Il est donc vraisemblablement difficile pour ces établissements de détecter les cas de fraude numérique dans le cadre de la surveillance des transactions.

Indications

La FINMA rappelle aux établissements que leurs dispositifs de lutte contre le blanchiment d'argent, ainsi que les systèmes et processus qu'ils utilisent, doivent être suffisamment efficaces pour permettre de détecter le plus rapidement possible les cas de fraude numérique et de *money muling*. En particulier, les systèmes de surveillance des transactions doivent permettre de détecter immédiatement les cas potentiellement suspects.

4 Conclusion

Les banques et les personnes au sens de l'art. 1*b* LB doivent mettre en place une gouvernance appropriée et un système efficace de gestion des risques permettant d'identifier, de limiter et de contrôler les risques de fraude numérique. Ceux-ci doivent couvrir l'ensemble des activités et être organisés de façon à permettre de détecter, évaluer, gérer et surveiller l'ensemble des risques essentiels. Cela inclut aussi les risques de fraude liés à l'ouverture numérique de relations clients, notamment en lien avec l'accès non autorisé aux comptes. Afin de pouvoir surveiller de manière adéquate les risques juridiques et de réputation considérables qui y sont liés et de prendre des mesures préventives, les établissements ont besoin d'outils et de structures de gestion clairs, de processus et de responsabilités bien définis, de la capacité de détecter et de réagir de manière efficace, d'un système sophistiqué de surveillance des transactions en matière de blanchiment d'argent ainsi que d'outils ciblés permettant de vérifier l'efficacité des contrôles. En cas de multiplication des cas de fraude, l'efficacité du dispositif mis en place pour identifier et prévenir de tels incidents doit être réévaluée rapidement et, si nécessaire, complétée par des mesures supplémentaires. Cela peut aussi inclure des restrictions temporaires concernant la fourniture de certains services à l'origine de tels cas de fraude numérique.