

Collaborative Fraud Prevention

Rapport sur les résultats de l'étude préliminaire
coordonné par l'Association suisse des banquiers

Avril 2025

Rapport sur les résultats
de l'étude préliminaire

Aperçu du projet

L'Association suisse des banquiers (ASB) a réalisé une étude préliminaire intitulée «Collaborative Fraud Prevention». Il s'agissait d'identifier et de prioriser des mesures possibles en vue d'améliorer encore la prévention commune des fraudes dans le trafic des paiements de compte à compte en Suisse.

Cette étude préliminaire s'est faite en collaboration avec un groupe de banques et d'autres membres de l'ASB constitué à cet effet (BCV, Entris Banking, Julius Baer, Banque Migros, PostFinance, Raiffeisen, SIX, UBS et ZKB), avec l'appui du cabinet de conseil Acrea. Ses conclusions résultent de recherches extensives sur la prévention collaborative des fraudes, d'entretiens et d'ateliers avec des expertes et des experts en fraude ainsi qu'avec des spécialistes du droit et de la conformité au sein des banques suisses participantes, et de plusieurs entretiens avec des fournisseurs de solutions de gestion de la fraude. Les travaux y relatifs ont été menés entre fin août 2024 et début mars 2025.

Le présent rapport récapitule les principales conclusions de l'étude préliminaire et formule trois recommandations opérationnelles pour la suite du processus.

Tendances et problématiques actuelles en matière de prévention des fraudes

Recours accru aux paiements numériques

A la fois rapides, confortables et très accessibles, les systèmes numériques de paiement ont radicalement transformé la manière dont les particuliers et les entreprises effectuent leurs transactions financières. Les portemonnaies mobiles, les paiements sans contact et la banque en ligne sont aujourd'hui la norme et conditionnent à la fois les comportements et les attentes des consommatrices et des consommateurs. Plus les transactions numériques se développent, plus il devient important de les protéger contre la fraude.

Menace grandissante de la fraude basée sur l'IA

Les fraudeurs exploitent les possibilités qu'offrent les nouvelles technologies, y compris l'intelligence artificielle (IA) générative, pour se livrer à des arnaques sophistiquées. Les préjudices financiers causés par la fraude sont élevés et les Etats-Unis, le Danemark et la Suisse occupent le haut du classement en termes de pertes par victime.¹ Selon une autre étude récente, en Europe, plus de 40 % des tentatives de fraude détectées dans le secteur de la finance et du trafic des paiements sont basées sur l'IA.² Il s'agit

1 [GASA, Global Anti-Scam Alliance and Feedzai Unveil 2024 Global State of Scams Report as Scams Continue to Plague Consumers \(2024\)](#)

2 [Signicat, The Battle Against AI-driven Identity Fraud \(2025\)](#)

notamment d'hypertrucages (deepfakes), de fraudes à l'identité synthétique et de campagnes sophistiquées d'hameçonnage (phishing). La collaboration croissante entre les cybercriminels et d'autres acteurs malveillants, favorisée par la circulation de données volées sur le darknet, renforce en outre l'efficacité des agissements frauduleux et contribue à leur succès.

Evolution de la fraude en Suisse

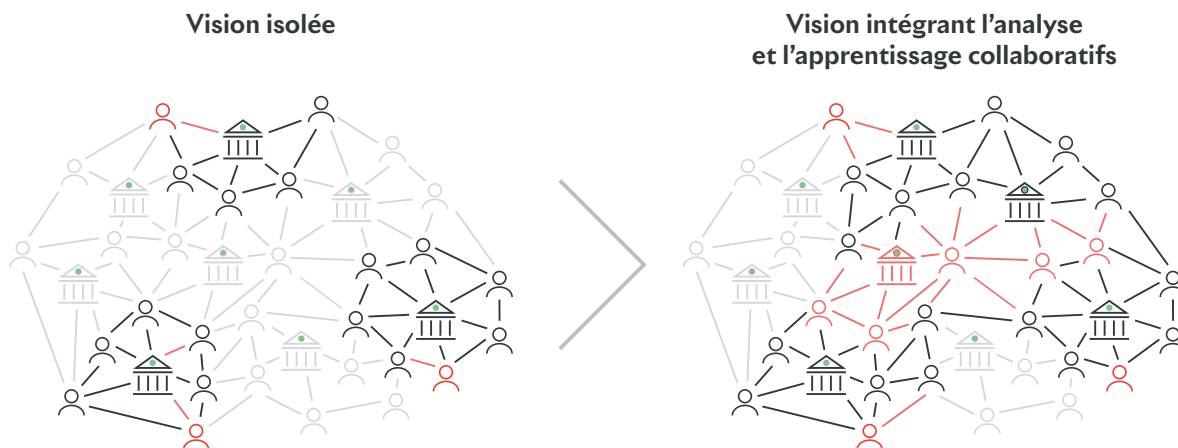
Ces dernières années, le nombre de cas de fraude en ligne a continué d'augmenter en Suisse comme dans le monde entier. Selon l'Office fédéral de la cybersécurité (OFCS), l'hameçonnage, la fraude à la facturation, l'usurpation d'identité et la fraude par ingénierie sociale sont les formes de cybercriminalité les plus répandues en Suisse et les pertes financières en résultant sont considérables. Les paiements instantanés étant de plus en plus courants, la «fraude instantanée» se répand elle aussi et place les mécanismes traditionnels de prévention des fraudes face à de nouveaux défis.

Liens entre fraude et blanchiment d'argent

La fraude et le blanchiment d'argent sont souvent liés et forment ensemble ce qu'il est convenu d'appeler le cycle de la criminalité financière (FinCrime Cycle). Les cybercriminels recourent à des méthodes frauduleuses (p. ex. hameçonnage, usurpation d'identité, arnaque aux sentiments ou romance scam) pour empocher illégalement de l'argent, qu'ils blanchissent ensuite via des réseaux de mules financières (money mules).

Renforcement de la prévention des fraudes au moyen d'approches collaboratives

Les banques suisses disposent déjà d'un arsenal performant en matière de gestion des fraudes, dont des systèmes avancés de détection. Afin de contrer efficacement les menaces grandissantes de fraude, il est essentiel de renforcer la collaboration entre les banques, les autres secteurs et les autorités de surveillance. Par exemple, analyser le «tableau complet» des paiements de compte à compte selon une approche collaborative pourrait aider à détecter les réseaux de fraude et de blanchiment d'argent qui déploient leurs activités sur plusieurs institutions. La Banque des règlements internationaux (BRI) a d'ailleurs insisté sur le potentiel que recèle la détection collaborative des fraudes – notamment dans le cadre d'initiatives comme le projet Aurora (2023), qui montrent comment des analyses communes de données peuvent contribuer à prévenir la criminalité financière.



Graphique 1: illustration du but poursuivi. De la vision isolée (à gauche) à la vision collaborative (à droite). Source: BIS Innovation Hub: Project Aurora – The power of data, technology and collaboration to combat money laundering across institutions and borders (2023)

Prévention collaborative des fraudes en Suisse: état des lieux

La prévention collaborative des fraudes fait déjà l'objet de nombreuses mesures en Suisse. Citons à titre d'exemples les services de Switch CERT, la création de l'Office fédéral de la cybersécurité (OFCS), ou encore l'initiative «e-banking en toute sécurité!» (EBAS) de la Haute école de Lucerne. Par ailleurs, le Swiss Financial Intelligence Public Private Partnership (partenariat public-privé suisse en matière de renseignement financier, Swiss FIPPP), instauré entre le Bureau de communication en matière de blanchiment d'argent (MROS) et des établissements financiers suisses issus du secteur privé, mise sur l'échange d'informations pour développer des connaissances stratégiques sur les tendances et les typologies de la criminalité financière.³

Néanmoins, l'étude préliminaire a révélé un potentiel d'amélioration de la prévention collaborative des fraudes, qui pourrait être mieux coordonnée et complétée. Le «top 3» des nouvelles mesures à prendre, défini d'un commun accord par les expertes et les experts en fraude du groupe de travail, est présenté ci-après.

3 [Fedpol, Swiss Financial Intelligence Public Private Partnership \(2025\)](#)

Préconisations issues de l'étude préliminaire

Sur la base des conclusions de notre étude préliminaire, nous préconisons que le secteur financier suisse analyse en détail les trois mesures suivantes:



Graphique 2: mesures préconisées sur la base de l'étude préliminaire de l'ASB · Source: interne



Mettre en œuvre des campagnes communes de sensibilisation

Idée directrice

Créer une marque unique, clairement reconnaissable et de grande portée, en fédérant les ressources des banques et les formats de communication existants en matière de prévention des fraudes. L'objectif est triple:

- sensibiliser encore davantage le grand public ainsi que les petites et moyennes entreprises (PME) à la fraude dans le domaine du trafic des paiements;
- informer la population sur l'existence et les dangers de la fraude ainsi que sur les bons réflexes à avoir pour ne pas être victime de tentatives de fraude ou d'hameçonnage;
- instituer un interlocuteur unique chargé de répondre aux demandes générales des médias en matière de fraude (indépendamment des cas de fraude concernant des clientes et/ou des clients spécifiques).

Arguments

Avec le développement fulgurant des technologies de l'IA, les tentatives de fraude et d'hameçonnage sont de plus en plus nombreuses et sophistiquées. Dans ce contexte, une des mesures préventives essentielles consiste à bien informer la population. Certes, il existe déjà de multiples formats de communication sur la prévention des fraudes, dans le secteur privé comme dans le secteur public, mais un potentiel d'amélioration subsiste en termes de coordination des messages et de regroupement des budgets. Des campagnes communes de sensibilisation augmenteraient considérablement la portée et l'efficacité de l'information sur la fraude.

Éléments de mise en œuvre

Les campagnes communes de sensibilisation devraient être organisées dans un format ouvert, indépendant (p. ex. une association), avec un plan d'investissement à moyen terme. Il faudrait intégrer tous les acteurs pertinents, dont les banques, les formats de communication existants ainsi que des parties prenantes extérieures au secteur des services financiers – par exemple la police, la Prévention Suisse de la Criminalité, d'autres autorités publiques et des plateformes de commerce en ligne comme SMG. Parmi les questions à résoudre figurent le périmètre exact, la gouvernance ainsi que le modèle d'exploitation et de financement du format commun. Il est prévu de clarifier ces aspects structurels dans la première phase d'un projet principal spécifique. Des phases ultérieures seront consacrées au développement, à l'organisation et à la mise en œuvre de mesures de communication communes sur la prévention des fraudes, y compris la définition de l'image de marque commune (brand).

Gouvernance du projet

Dès 2024, de premiers entretiens constructifs sur la communication en matière de prévention des fraudes ont réuni divers acteurs dans le cadre de l'initiative Pay Attent!on (anciennement Swiss Cyber Security Awareness Roundtable). Cette initiative a été lancée par EBAS.ch, card-security.ch et UBS.

L'étude préliminaire de l'ASB préconise de la poursuivre et de l'étendre à de nouveaux partenaires (p. ex. d'autres banques). L'objectif est de spécifier et d'institutionnaliser la structure organisationnelle en 2025, afin de lancer des campagnes communes de sensibilisation à partir de 2026.



Etudier l'éventuelle création d'un service d'évaluation des risques au niveau du réseau

Idée directrice

Un prestataire central développerait un service consistant à calculer un indicateur de risque pendant la saisie des données de paiement de compte à compte, en temps réel. Cet indicateur pourrait être utilisé par les banques émettrices selon leur libre appréciation, par exemple comme un signal supplémentaire intégré dans leurs propres modèles d'évaluation des risques ou comme un élément de la solution de prévention des fraudes éventuellement fournie par un prestataire de leur choix. Le calcul de l'indicateur de risque s'effectuerait notamment dans le cadre d'une analyse au niveau du réseau, à l'aide d'algorithmes d'apprentissage automatique. Dans un premier temps, le service se baserait exclusivement sur des données de trafic des paiements, complétées par les annonces de fraude des banques participantes concernant ces transactions.

Arguments

Un service d'évaluation des risques au niveau du réseau constituerait pour les banques un instrument performant et sans équivalent, qui leur permettrait d'évaluer les risques inhérents à la ou au destinataire d'un paiement. Quelle est la probabilité que l'IBAN destinataire fasse partie d'un réseau de blanchiment d'argent ou soit lié à une autre activité frauduleuse? Lorsque les banques n'ont qu'une vision isolée des transactions, il leur est difficile de répondre à cette question. Mais au niveau du réseau, les schémas suspects sont nettement plus faciles à identifier. C'est particulièrement important dans la lutte contre les arnaques par courriel (scams), une forme de fraude en forte progression où des clientes et des clients de banques sont incités à effectuer eux-mêmes des paiements en ligne illégitimes. Au Royaume-Uni, où un service d'évaluation des risques au niveau du réseau existe déjà (Vocalink), l'expérience montre que les bénéfices en résultant sont considérables – notamment un meilleur taux de détection des fraudes et une baisse des fausses alarmes (false positives).

Eléments de mise en œuvre

Compte tenu du rôle central que joue Swiss Interbank Clearing (SIC) dans le trafic des paiements de compte à compte en Suisse, il lui reviendrait logiquement de développer ce service d'évaluation des risques au niveau du réseau. Deux options ont été identifiées: soit SIC fournit ce service elle-même, soit elle mandate un autre prestataire à cet effet. Au vu d'une première analyse comparative de ces options selon quatre critères (efficacité, efficience, extensions potentielles du service et conformité), les expertes et les experts des banques participantes se sont clairement prononcés en faveur de la fourniture du service par SIC elle-même. Cette approche reste à examiner plus en détail dans le cadre d'une étude de faisabilité approfondie (incluant les aspects juridiques et ceux liés à la conformité).

Gouvernance du projet

Les banques ayant participé à l'étude préliminaire suggèrent que dans une prochaine étape, SIC réalise une étude de faisabilité approfondie sur ce thème. La Banque nationale suisse (BNS) soutient cette méthode.



Développer les échanges sur différents produits et secteurs

Idée directrice

Assurer des échanges réguliers entre expertes et experts en fraude sur différents produits de paiement (p. ex. paiements de compte à compte, cartes de crédit et de débit, Twint, cryptomonnaies) et différents secteurs (p. ex. télécommunications, commerce en ligne, médias sociaux). Les buts de ces échanges sont les suivants:

- partage efficace de connaissances, de bonnes pratiques et d'informations sur les menaces;
- discussion sur les futures mesures communes de gestion des fraudes, classement de celles-ci par ordre de priorité et mise en œuvre;
- incitation pour d'autres secteurs (p. ex. télécommunications, commerce en ligne, plateformes numériques) à prendre des mesures supplémentaires de prévention des fraudes ou à améliorer les mesures existantes, dans la mesure où les banques parlent d'une seule voix;
- au besoin, coordination avec les autorités réglementaires sur les aspects juridiques et prudentiels de la gestion des fraudes.

Arguments

La Suisse compte déjà plusieurs forums d'échange et plusieurs plateformes en lien avec la fraude (p. ex. Switch CERT, OFCS, NCSC, CPS, PaCoS, EBAS, card-security.ch, e-Alarm de l'ASB). Néanmoins, selon les personnes ayant contribué à l'étude préliminaire, il reste un potentiel d'amélioration de la coordination au niveau des produits de paiement et des secteurs. Une collaboration intersectorielle renforcée est particulièrement importante dans la mesure où, le plus souvent, les scams apparaissent sur des sites de commerce en ligne et des plateformes numériques et/ou se diffusent dans d'autres secteurs faute de mesures préventives (p. ex. prévention des fraudes par usurpation d'identité ou spoofing).

Éléments de mise en œuvre

Afin que la taille du groupe reste gérable, il ne s'agit pas de créer un forum centralisé et unique d'échange sur la fraude. Il conviendrait plutôt de structurer plusieurs forums, par exemple par groupes cibles (senior product managers, expertes et experts techniques, etc.). Afin de définir la configuration optimale de ces

futurs forums, l'étude préliminaire préconise de procéder à une analyse approfondie dans le cadre d'un projet principal, comme suit:

- inventaire détaillé de tous les formats existants en matière de partage d'informations sur la fraude (membres, objectifs, activités, plateformes de communication, etc.);
- identification des manques ainsi que des doublons entre les formats existants;
- élaboration de propositions d'adaptation concernant les formats existants et identification de nouveaux formats potentiels sur la base des manques et des doublons constatés.

Gouvernance du projet

Idéalement, l'analyse approfondie devrait être effectuée par une entité sectorielle, indépendante des formats existants et entretenant d'étroites relations avec d'autres secteurs ainsi qu'avec les autorités réglementaires. L'ASB est donc invitée à diriger cette analyse approfondie – en étroite collaboration avec les banques et, si nécessaire, avec le Swiss Financial Sector Cyber Security Centre (FS-CSC).

Conclusion

«Il faut un réseau pour battre un réseau.» Face à l'évolution rapide des tactiques de fraude et à la multiplication des tentatives de fraude, le secteur financier n'a pas d'autre choix que de faire évoluer sans répit ses approches préventives en la matière. Nous sommes convaincus que la prévention des fraudes passe aujourd'hui par de nouvelles approches collaboratives. Celles-ci ont fait l'objet d'une analyse systématique dans le cadre de l'étude préliminaire. Les trois mesures prioritaires présentées dans ce rapport constituent des initiatives importantes et concrètes pour affronter ces évolutions.

Equipe de projet

Richard Hess, Association suisse des banquiers (ASB)

Stephan Odermatt, Acrea SA

Stephan Wengi, Acrea SA

Expertes et experts des banques participantes

David Bundi, Banque Migros SA

Angela Carpintieri, Banque Julius Baer & Co. SA

Maxime Charbonnel, Banque Cantonale Vaudoise

Nicolas Cramer, UBS Switzerland AG

Martin Dion, Banque Cantonale Vaudoise

Elisa-Sophie Eikevaag, SIX Group SA

Aline Fedier, Banque Julius Baer & Co. SA

Joëlle Gautier, UBS Switzerland AG

Roger Huber, Banque Cantonale de Zurich

Bogdan Iancu, Banque Cantonale Vaudoise

Nicky Kern, UBS Switzerland AG

Lukas Peter, Banque Cantonale de Zurich

Romano Ramanti, Banque Cantonale de Zurich

Arlind Spahija, Banque Migros SA

Seline Trachsel, Banque Julius Baer & Co. SA

Michael Wili, PostFinance SA

Stephan Zimmermann, PostFinance SA

Simon Züst, Raiffeisen Suisse société coopérative

Exclusion de responsabilité

Le présent rapport est publié exclusivement à des fins d'information et de discussion. Les informations et les opinions qu'il contient ne prétendent pas formuler des conclusions globales ou définitives sur le sujet concerné et ne constituent pas des conseils juridiques. Il reflète exclusivement les opinions des autrices et des auteurs ainsi que des expertes et des experts susmentionnés, lesquelles constituent une première analyse et sont susceptibles d'évoluer. L'Association suisse des banquiers décline toute responsabilité quant à l'exactitude, à l'exhaustivité ou à l'actualité des informations figurant dans le présent rapport.

Association suisse des banquiers

Aeschenplatz 7

Case postale 4182

CH-4002 Bâle

office@sba.ch

www.swissbanking.ch