Swiss Banking

Collaborative Fraud Prevention

Results report of the preliminary study coordinated by the Swiss Bankers Association

April 2025

Results report
of the preliminary study

Project overview

The Swiss Bankers Association (SBA) has conducted a preliminary study on "Collaborative Fraud Prevention" to identify and prioritise possible measures to further enhance the joint efforts against fraud in Swiss account-to-account payments.

The preliminary study was carried out in cooperation with a select group of banks and other SBA members (BCV, Entris Banking, Julius Bär, Migros Bank, PostFinance, Raiffeisen, SIX, UBS and ZKB) and supported by the management consultancy Acrea. The results are based on extensive desk research on collaborative fraud prevention, dedicated interviews and workshops with fraud as well legal and compliance experts from the participating Swiss banks, and several interviews with selected providers of fraud management solutions. These activities have been carried out between the end of August 2024 and the beginning of March 2025.

This report summarises the main findings of the preliminary study and outlines three recommendations for further action.

Current trends and challenges in fraud prevention

Ongoing Shift to Digital Payments

The shift toward digital payments has revolutionised how individuals and businesses conduct financial transactions, offering speed, convenience, and accessibility. Mobile wallets, contactless payments, and online banking have become the norm, shaping consumer behaviour and expectations. As digital transactions grow, so does the relevance of protecting these transactions against fraud.

The Rising Threat of AI-Driven Fraud

Fraudsters are taking advantage offered by the possibilities of new technologies, including generative AI, to execute sophisticated scams. The financial toll of scams is staggering, with the U.S., Denmark, and Switzerland reporting the highest losses per victim.[1] Another recent study reveals that more than 40 percent of all detected fraud attempts in the European financial and payment transactions sector are AI-driven.[2] This includes deepfakes, synthetic identities and sophisticated phishing campaigns. The growing collaboration among cybercriminals and malicious actors, facilitated by the exchange of stolen data on the dark web, further enhances the effectiveness and success of fraudulent schemes.

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)

Fraud Trends in Switzerland

In recent years, cases of internet fraud have continued to rise, both globally and in Switzerland. According to the National Cyber Security Centre (NCSC), phishing attacks, invoice fraud, identity theft, and social engineering scams top the list of cybercrimes in Switzerland, resulting in significant financial losses. With the increasing adoption of instant payments, instant fraud is also becoming a reality, challenging traditional fraud prevention mechanisms.

The Interconnection of Fraud and Money Laundering

Fraud and money laundering are often linked, forming what is known as the "FinCrime Cycle." Cybercriminals acquire illicit funds through schemes like phishing, identity theft, and romance scams. These funds are then laundered using networks of "money mules".

Strengthening Fraud Prevention through Collaborative Approaches

Swiss Banks already apply a broad range of effective fraud management measures including, among many others, advanced fraud detection systems. To further address the rising fraud threats, increased collaboration among banks, other industries and regulatory authorities is key. For example, analysing the "full picture" of account-to-account payments on a network-level may help to uncover fraud and money laundering networks that are spreading their operations across multiple institutions. The Bank for International Settlements (BIS) has also emphasized the potential of collaborative fraud detection through initiatives such as "Project Aurora" (2023), demonstrating the effectiveness of shared intelligence in preventing financial crimes.

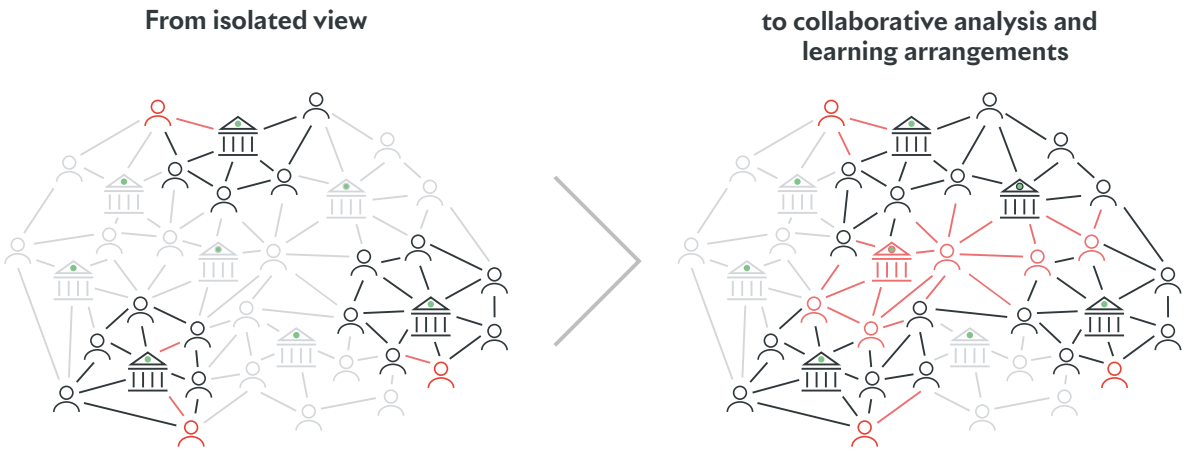

Figure 1: Visualized intention. From an isolated view to a cross-institutional view · **Source:** BIS Innovation Hub "Project Aurora"

Collaborative Fraud Prevention in Switzerland: Current Situation

Numerous collaborative fraud prevention measures already exist in Switzerland. Examples include, but are not limited to, services offered by Switch CERT, the National Cyber Security Centre (NCSC) and "eBanking aber sicher!" by Lucerne University of Applied Sciences and Arts. In addition, the Swiss Financial Intelligence Public Private Partnership (Swiss FIPPP) promotes the exchange of information between the Money Laundering Reporting Office Switzerland (MROS) and Swiss financial institutions from the private sector to share strategic insights on financial crime trends and typologies.[3] Still, the preliminary study has indicated that there is potential for increased alignment and further enhancements in collaborative fraud prevention. The "top 3" additional measures, as jointly prioritized by fraud experts of preliminary study participants, are presented in the following.

Recommendations from the preliminary study

Based on the findings from the conducted preliminary study, we recommend that the Swiss financial industry further pursues the following three measures:

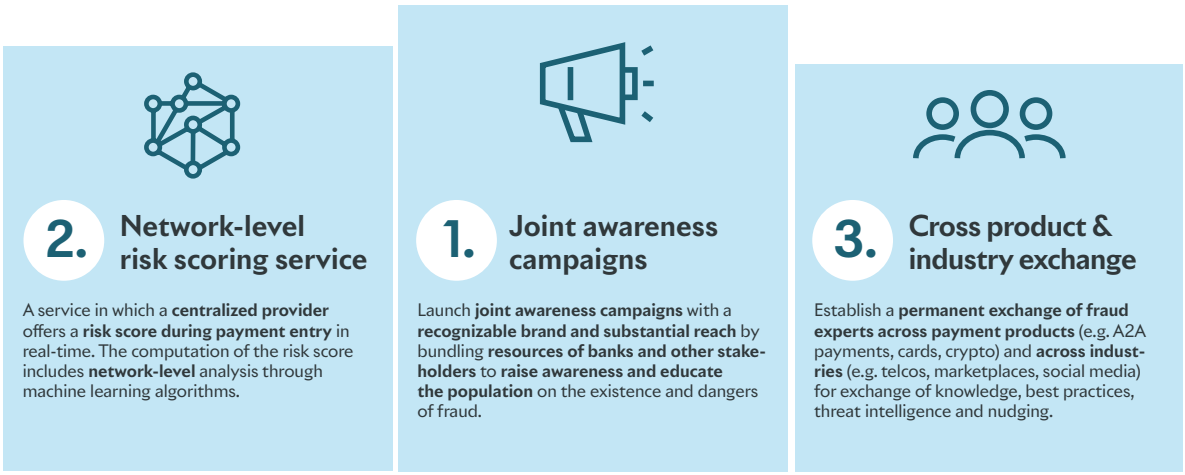

Figure 2: Recommended measures from SBA prestudy · **Source:** own contribution

3 Fedpol, Swiss Financial Intelligence Public Private Partnership (2025)

Launch Joint Awareness Campaigns

Overall idea

Bundle resources of banks and existing fraud communication formats to establish a recognizable brand with substantial reach to:

- raise awareness to protect the general Swiss public and small/medium enterprises from payment fraud
- educate the population on the existence and dangers of fraud and enable them to act appropriately not to fall for the scam/phishing attempt
- provide a central point of contact for general fraud-related media request (not related to a specific customer)

Rationale

Driven by the rapid evolution of AI technologies, scams and phishing attacks become ever more sophisticated and numerous. In this context, a wellinformed population is a key preventive measure. While numerous fraud-related communication formats already exist, both in the private and public sector, further potential lies in aligning messages and pooling budgets, thereby increasing the reach and impact of fraud awareness communication.

Implementation aspects

Joint awareness campaigns should be driven by an independent, open format (e.g. an association) with a midterm investment plan. The format should include all kinds of stakeholders, including banks and existing communication formats as well as stakeholders from outside the financial services industry (e.g. police, Schweizerische Kriminalprävention, other public authorities and digital marketplace provider such as SMG). Open questions include, but are not limited to, the detailed scope, governance, operating and funding model of the joint format. These structural questions shall be addressed in the first phase of a dedicated main project. Later phases include the development, design and launch of joint fraud awareness communication measures, including the definition of the target brand.

Project governance

Already in 2024, first constructive discussions among multiple fraud communication stakeholders were held through the initiative “Pay Attent!on” (formerly known as “Swiss Cyber Security Awareness Round-table”) initiated by EBAS.ch, card-security.ch and UBS.

The SBA preliminary study recommends to further pursue this initiative and extend it to additional stakeholders (e.g. additional banks), with the aim of specifying and institutionalising the setup during 2025 and launching joint awareness campaigns in 2026.

Further Evaluate a Network-level Risk Scoring Service

Overall idea

Develop a service in which a centralized provider offers a real-time risk score during entry of account-to-account payments data. This risk score can be used by sender banks at their own discretion, e.g., it may be included as one signal in the banks' own risk scoring models or it may be consumed by a fraud prevention solution vendor of the banks' choice. The computation of the risk score includes, but is not limited to, net-work-level analysis through machine learning algorithms. In a first step, the service will likely only be based on payment transaction data, plus participating banks' fraud flags related to these transactions.

Rationale

Network-level risk scoring services are a powerful and unique tool for banks to assess the risks related to the recipient side of a payment. How likely is it that the recipient IBAN is a money mule or another malicious actor? If sending banks have an isolated view, this is very difficult to tell; on a network level, suspicious patterns are much easier to spot. This is particularly relevant to fight the rapidly growing problem of scams, in which bank customers are tricked into entering illegitimate payments themselves. Experience from the UK, where such a service (Vocalink) already is in place, confirms substantial benefits both regarding increased fraud detection rate and less false positives.

Implementation aspects

Given the central role of Swiss Interbank Clearing (SIC) in Swiss account-to-account payments, it is predestined to develop a network-level risk scoring service. Two options for SIC's role have been identified: SIC could either offer the service itself or enable other service providers to do so. Based on an initial comparison of these options along four criteria (effectiveness, efficiency, potential for service extensions, and compliance), the fraud experts of participating banks have indicated a clear preference that SIC should offer the service itself. The feasibility of this approach needs to be further analysed through an in-depth feasibility assessment (incl. legal & compliance aspects).

Project governance

As a next step, the banks participating in the preliminary study encourage SIC to launch an in-depth feasibility assessment on that matter. The Swiss National Bank (SNB) supports this approach.

Promote Cross Product & Industry Exchange

Overall idea

Ensure a permanent exchange of fraud experts across payment products (e.g., account-to-account payments, credit and debit cards, Twint, crypto) and across industries (e.g., telcos, marketplaces, social media). The objectives of such exchanges would be to:

- efficiently share knowledge, best practices, and threat intelligence
- discuss, prioritize and initiate future collaborative fraud management measures
- nudge other industries (e.g. telcos, digital marketplaces and platforms) towards additional or improved fraud prevention measures by bundling the voice of the banks
- where required, coordinate with regulators on legal and supervisory aspects of fraud management

Rationale

In Switzerland, multiple fraud-related exchange forums and platforms already exist (e.g., Switch CERT, NCSC, SPC, PaCoS, EBAS, card-security.ch, SBA E-Alarm). However, as perceived by preliminary study participants, there is still potential to improve coordination across payment products and industries. Increased cross-industry collaboration is particularly important because a large share of scams originates on digital marketplaces and platforms and/or is facilitated by missing preventive measures by other industries (e.g., spoofing prevention).

Implementation aspects

To keep group size reasonable, the aim is not to establish a single fraud exchange forum. Rather, there should be several forums structured, e.g., along target audience such as senior product managers and technical experts.) To define the optimal set of such future fraud exchange bodies, the preliminary study recommends conducting the following in-depth analysis in a main project:

- Collect detailed information on all existing fraud exchange formats (participants, objectives, activities, communication platforms, etc.)
- Identify gaps and overlaps between the existing formats
- Propose adjustments to the existing formats and potential new forums based on identified gaps and overlaps

Project governance

The recommended in-depth analysis may best be conducted by an industry-level body that is independent of existing fraud exchange formats and holds close ties with other industries and regulators. Therefore, SBA is encouraged to lead the required in-depth analysis, in close collaboration with banks and the Swiss Financial Sector Cyber Security Centre (FS-CSC) if needed.

Conclusion

"It takes a network to beat a network". To keep pace with evolving fraud tactics and a rapidly growing number of fraud attempts, the financial sector must continuously adapt its fraud prevention approaches. We believe that additional, collaborative approaches to fraud prevention are required. Such approaches have been analysed in a structured manner through the conducted preliminary study. The three priority measures introduced in this report represent important and concrete steps to respond to these developments.

Project team

Richard Hess, Swiss Bankers Association SBA
Stephan Odermatt, Acrea AG
Stephan Wengi, Acrea AG

Experts from participating banks

David Bundi, Migros Bank AG
Angela Carpintieri, Bank Julius Bär & Co. AG
Maxime Charbonnel, Banque Cantonale Vaudoise
Nicolas Cramer, UBS Switzerland AG
Martin Dion, Banque Cantonale Vaudoise
Elisa-Sophie Eikevaag, SIX Group AG
Aline Fedier, Bank Julius Bär & Co. AG
Joëlle Gautier, UBS Switzerland AG
Roger Huber, Cantonal Bank of Zurich
Bogdan Iancu, Banque Cantonale Vaudoise
Nicky Kern, UBS Switzerland AG
Lukas Peter, Cantonal Bank of Zurich
Romano Ramanti, Cantonal Bank of Zurich
Arlind Spahija, Migros Bank AG
Seline Trachsel, Bank Julius Bär & Co. AG
Michael Wili, PostFinance AG
Stephan Zimmermann, PostFinance AG
Simon Züst, Raiffeisen Switzerland Cooperative

Swiss Bankers Association
Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch