VSKB Legal & Compliance Tagung 2026

Roland Stucki, Jürg Senn, Romano Ramanti

Zürcher Kantonalbank

Workshop Betrugsbekämpfung

FINMA Aufsichtsmitteilung 02/26 & Kollaborative Betrugsprävention

Agenda

1. FINMA Aufsichtsmitteilung 02/26
2. Kollaborative Betrugsprävention
3. Diskussion

FINMA Aufsichtsmitteilung 02/26

FINMA-Aufsichtsmitteilung 02/2026

Grundlagen

- Aufsichtsmitteilung basiert auf **Umfrage bei 19 Banken** verschiedener Aufsichtskategorien, die von der FINMA Ende 2025 durchgeführt wurde.

- Im Fokus steht **„digital fraud“**: Betrugsrisiken bei der digitalen Eröffnung von Kundenbeziehungen (z.B. Identitätsbetrug, gefälschte Ausweisdokumente) und bei unautorisierten Zugriffen auf Konten (z.B. Entwendung von Login-Daten).

- Banken und Personen nach Art. 1b BankG müssen ein **angemessenes Risikomanagement implementieren**, das alle **wesentlichen Risiken erfasst**, **bewertet**, **steuert** und **überwacht**.

- **Relevante regulatorische Vorgaben:**
  - Bankengesetz (BankG)
  - Bankenverordnung (BankV)
  - Geldwäschereigesetz (GwG)
  - Geldwäschereiverordnung-FINMA (GwV-FINMA)
  - FINMA-Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“
  - FINMA-Rundschreiben 2016/7 „Video- und Online-Identifizierung“

FINMA-Aufsichtsmitteilung 02/2026

Erkenntnisse aus der Umfrage „Digital Banking“

1. **Fehlende Governance-Strukturen:** Viele Banken haben keine klaren Governance-Strukturen für digitale Betrugsrisiken. Nur 12 von 19 Instituten verfügen über nachhaltige Strukturen und 42 % haben keine spezifische „Digital Fraud Policy“.

2. **Mangelnde Erkennung von Betrugstrends:** 26 % der Institute haben keine Prozesse zur proaktiven Erkennung von Betrugstrends (Horizon Scanning). Nur 12 von 19 Instituten nutzen Technologien zur Echtzeit-Betrugserkennung.

3. **Unzureichende Reaktionspläne:** 7 von 19 Instituten haben keine Standardprozesse oder Reaktionspläne für Betrugsfälle. Nur wenige aktualisieren ihre Pläne regelmässig oder bieten 24/7-Meldekanäle an.

4. **Fehlende technische Kontrollen:** 20 % der Institute setzen keine Schlüsselkontrollen wie Geoblocking, IP-Risk-Rating oder Device-Fingerprinting ein. Zudem werden bestehende Kontrollen oft nicht regelmässig überprüft.

5. **Unzureichende Schulungen:** Einige Institute schulen ihre Mitarbeitenden nicht ausreichend zu digitalen Betrugsrisiken. Sensibilisierung erfolgt oft nicht rollenbasiert, und besonders gefährdete Kundengruppen werden selten identifiziert.

6. **Betrügerische Kontoeröffnungen:** Zunehmende Betrugsfälle durch gefälschte Ausweise, Identitätsmissbrauch und Deepfake-Technologien bei digital eröffneten Konten. Kriminelle nutzen immer ausgefeiltere Methoden, um Kontrollmechanismen zu umgehen.

7. **Schwächen in der Geldwäschereiprävention:** Grosse Unterschiede in der Effektivität der Geldwäscherei-Dispositive zwischen den Instituten. KYC-Informationen werden oft nicht ausreichend erhoben oder für das Transaktionsmonitoring genutzt.

FINMA-Aufsichtsmitteilung 02/2026

Fazit / Handlungsbedarf

Die FINMA fordert von den Banken:

- Klare Governance-Strukturen und Zuständigkeiten
- Proaktive Erkennung und schnelle Reaktion auf Betrugstrends
- Regelmässige Überprüfung und Verbesserung von Kontrollen
- Bessere Schulung von Mitarbeitenden und Sensibilisierung von Kunden

Dies löst für die Banken **Handlungsbedarf** aus:

Op. Risk Management

- Nutzung von **technischen Möglichkeiten** zur Erkennung von Deepfakes und manipulierten Videos.
- Regelmässige **Weiterbildung** der Mitarbeitenden.
- Umfassende digitale **Betrugspräventionsstrategie**.

Compliance Risk Management

- **Geldwäscherei-Dispositive** (Systeme und Prozesse) zur raschmöglichsten Aufdeckung digitaler Betrugsfälle und Money Muling-Fälle.
- **Transaktionsüberwachungssysteme** zwecks umgehender Identifizierung potenzieller Verdachtsfälle.

Kollaborative Betrugsprävention

Vorstudie der Schweizerischen Bankiervereinigung

Ziel und Vorgehen

Zürcher Kantonalbank

Swiss Banking acrea

1. Project overview

SBA pre-study «Collaborative Fraud Prevention»

Objective / Mission

Translate the abstract interest of various stakeholders in Collaborative Fraud Prevention into an **engaged "Coalition of the Willing" with a concrete, prioritized, aligned plan of action.**

Participants

The following parties have actively participated in and jointly financed the pre-study:

BCV, Entris Banking, Julius Bär, Migros Bank, PostFinance, Raiffeisen, SIX, Swiss Banking, UBS, Zürcher Kantonalbank

Approach

1. **Structured analysis** of possible measures **(«longlist»)**
2. **Joint prioritization** of possible measures **(«shortlist»)**
3. **Identification of key questions & fields of action** that need to be clarified in the main project(s)
4. **Recommendation of governance** for the main project(s)

Timeline

- **Start** of pre-study: **August 2024**
- **End** of pre-study: **Q1 2025**
- **Result communication: April 2025 (tbc)**

Scope

- The focus is on **account-to-account payment fraud** via **digital channels**
- Within this scope, the **initial consideration set** of potential measures is **very broad**
- **The pre-study aims to build upon existing measures and initiatives**, e.g., from Switch CERT, EBAS, SPC, …

Out-of-scope

- Detailed solution concept(s)
- Technical implementation / PoC
- Vendor selection(s)
- L&C expert opinion(s) by law firm
- Project plan for main project(s)

Vorstudie der Schweizerischen Bankiervereinigung

Erarbeitete Longlist

Zürcher Kantonalbank

Swiss Banking acrea

3. Measure longlist and shortlist

Longlist: Framework

Longlist measures descriptions are available in separate **excel file**

(n) = number of measures on longlist

15 Technical focus

10 Centralized approaches

All technical measures to collect and analyze data *in a central place*.

3 Decentralized approaches

All technical measures that allow keeping data in a *decentralized* (federated) manner, i.e., on the participants' own premises, without sharing them directly.

2 Indifferent approaches

Technical measures that could be implemented either in a centralized or decentralized (federated) manner.

21 Non-technical focus

3 Customer Education & Engagement

Collaborate on educating customers (and potentially other stakeholders) to increase awareness for fraud topics

5 Best Practices & Training

Establish best practices and trainings across participants to educate practitioners on state-of-the-art fraud detection and prevention.

2 Intelligence & Information Exchange

Organize regular sharing of (non-R&D) intelligence and information among participants that address the participants' own current fraud situation.

4 Investigations & Responses

Share resources and establish organizational structures and processes that allow quick responses to fraud cases across participating organizations.

1 Research & Development

Increase the R&D collaboration among participants through research initiatives, innovation workshops, etc.

3 Collaboration Beyond Banks

Collaborate with other payment actors (e.g., cards, TWINT) and industries (e.g., telcos, marketplaces, social media).

3 Regulatory Collaboration

Extend the existing collaboration between banks and regulators regarding collaborative fraud prevention.

8 Foundational

2 Collaborative Framework

Define frameworks and governance(s) to foster future collaboration on fraud prevention among participants.

6 Harmonization & Standards

Harmonize standards, definitions and procedures as a foundation for technical CFP measures like reporting, data exchange, or monitoring.

Vorstudie der Schweizerischen Bankiervereinigung

Gemeinsam gewählte Shortlist

Zürcher Kantonalbank

Swiss Banking acrea

3. Measure longlist and shortlist

Shortlist: Top priority collaborative fraud prevention measures

Collaborative Fraud Prevention – Part 2

1.

Joint awareness campaigns

Enable **joint awareness campaigns** with a **recognizable brand and substantial reach** by bundling **resources of banks and other stakeholders** to **raise awareness and educate the population** on the existence and dangers of fraud.

Measure type: **Non-technical focus:** Customer education & engagement

2.

Network-level risk scoring service

A service in which a **centralized provider** offers a **risk score during payment entry** in real-time. The computation of the risk score includes **network-level** analysis through machine learning algorithms.

Measure type: **Technical focus:** Centralized approaches

3.

Cross product & industry exchange

Establish a **permanent exchange of fraud experts across payment products** (e.g. A2A payments, cards, Twint, crypto) and **across industries** (e.g. telcos, marketplaces, social media) for exchange of knowledge, best practices, threat intelligence, and nudging.

Measure type: **Non-technical focus:** Collaboration beyond banks

16.0
6.20

Massnahme 1: Gemeinsame Awareness-Kampagne

Pay Attent!ion

Zürcher Kantonalbank

Weshalb braucht es Pay Attent!on?

Druck steigt	Bevölkerung braucht Aufklärung	One Voice is Key
Zunahme von Zahlungsbetrug über Zahlungsmittel-Grenzen hinweg	**Regelmässige Berichterstattung** über Zahlungsbetrug in den Medien (Verunsicherung)	**Wiedererkennung** dank gemeinsamem Auftritt und einheitlichen Botschaften
Zunahme Druck auf Finanzbranche Regulierungen im Ausland	**Eigenverantwortung der Bevölkerung stärken** im Umgang mit Zahlungsmitteln	**Nationale Reichweite** und hochwertiges Kampagnenmaterial dank gebündelter Kräfte

Klares Signal der Finanzbranche und der Polizei für eine starke Prävention im Zahlungsverkehr!

8

pay attent!on

Massnahme 2: Network Level Risk Indicators - NLRI

Überblick

Network-Level Risk Indicators (NLRI) Service

The Solution

The NLRI service is foreseen as a set of centrally calculated risk indicators that serve as additional risk signals (e.g., IBAN age) supporting banks in their assessment on whether a specific transaction could be fraudulent.

Feasibility study initiated by SIC AG

Close collaboration with bank experts ensures that the proposed solution effectively complements the banks' fraud prevention measures, and that the associated legal challenges are accounted for (e.g., banking secrecy).

Role of SNB

BoD SIC banks would like SNB to play an active role in the provision of such as service. SNB is analyzing which role they can play over the coming months.

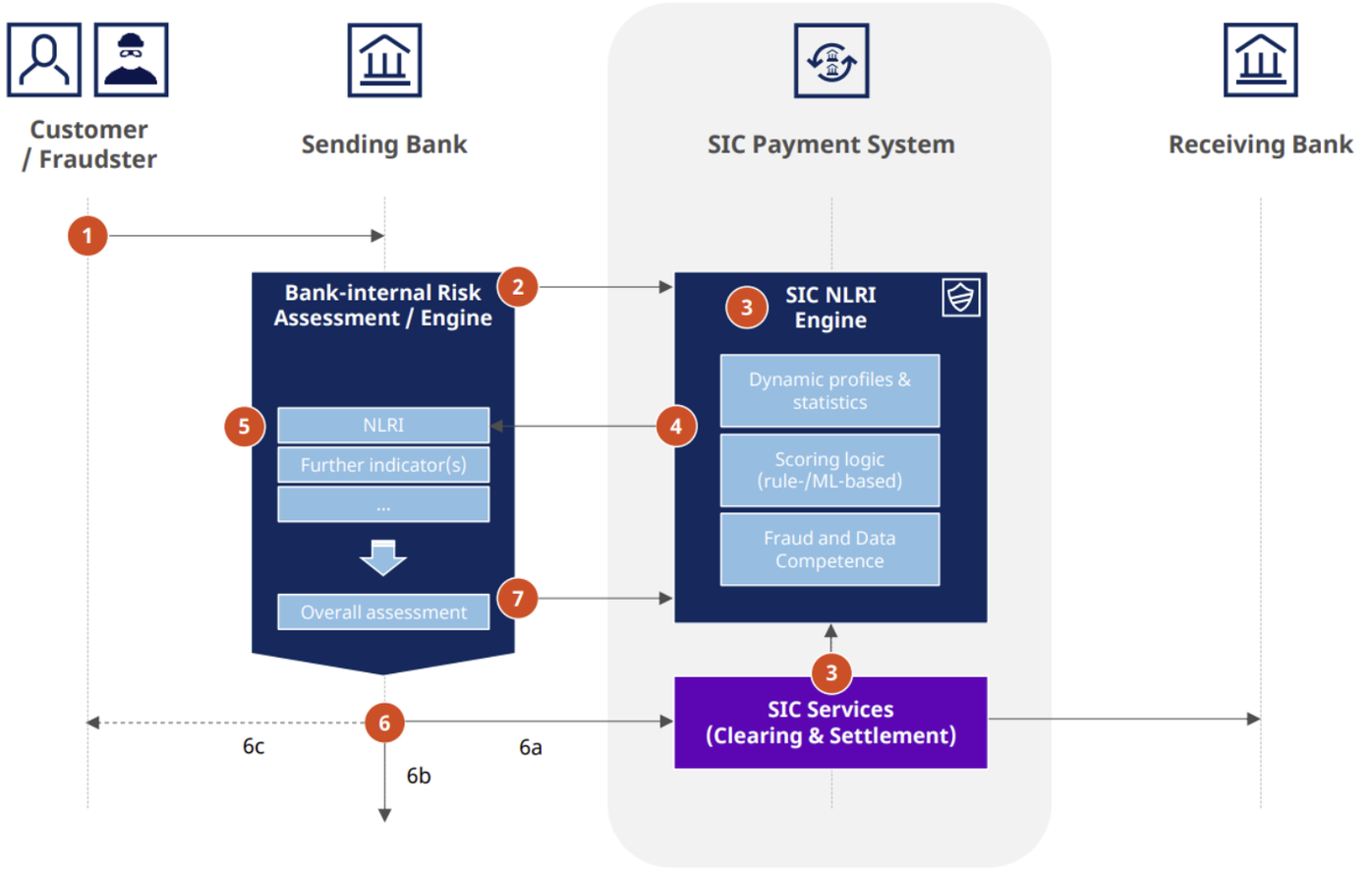
Next Steps

Conduction of a Proof of Value (to be confirmed), detailing of the NLRI solution design, business model and key legal considerations. Implementation is planned for 2027.

Massnahme 2: Network Level Risk Indicators - NLRI

Überblick

Network-Level Risk Indicator (NLRI) service overview



Description

1. Client or fraudster enters payment data in e-/m-banking and confirms payment.
2. **Indicator request:** before payment processing, the bank sends trx data to SIC (e.g., via API).
3. **NLRI Engine:** leverages rule-based logic and ML data models (based on past trx data stored by SIC and NLRI risk reporting) to compute real-time risk indicators for the queried trx.
4. **Output:** relevant risk indicators are delivered back to the sending bank
5. **Integration:** bank can integrate the risk indicators into its internal risk
6. assessment and **takes final decision**:
   a) transaction is processed inhouse or via SIC
   b) transaction is on hold for further investigation
   c) transaction is declined, and the client is informed
7. **NLRI risk reporting** on trx provided by the banks back to SIC

Massnahme 3: Working Group Fraud Prevention

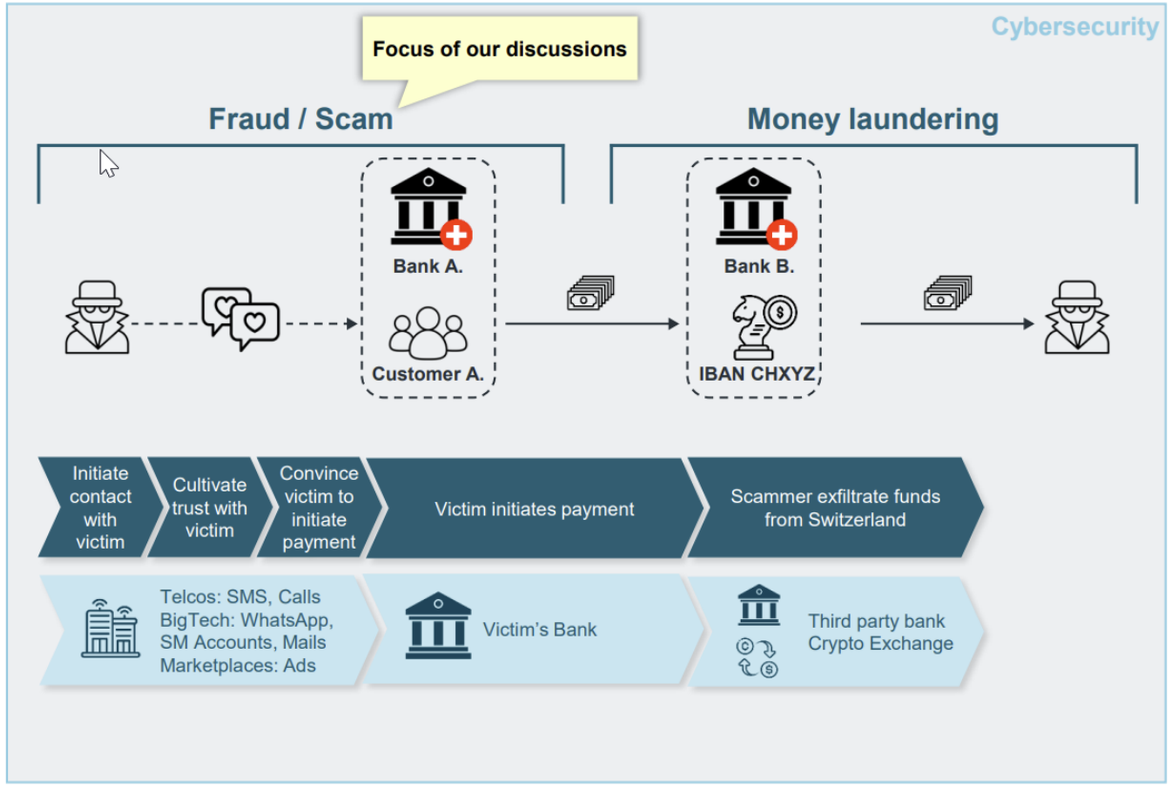
Fraud Chain

Zürcher Kantonalbank

Swiss Banking

Discusion of Pain Points along the Fraud Chain

Overview of the “Fraud Chain”



Objectives of an improved cross product & industry exchange

Shared ambition to **stop Swiss people from getting scammed.**

Stopping scams from reaching people, not just potentially refunding losses.

Tackling this problem as a whole ecosystem, each sector taking responsibility.

Diskussion

Zürcher Kantonalbank

VSKB Legal & Compliance Tagung 2026

Roland Stucki, Jürg Senn, Romano Ramanti