Swiss Banking

Collaborative Fraud Prevention

Ergebnisbericht der Vorstudie koordiniert von der Schweizerischen Bankiervereinigung

April 2025

Ergebnisbericht der Vorstudie

Projektübersicht

Die Schweizerische Bankiervereinigung (SBVg) hat eine Vorstudie zum Thema «Collaborative Fraud Prevention» durchgeführt, um mögliche Massnahmen zur weiteren Verbesserung der gemeinsamen Betrugsprävention im Schweizer Konto-zu-Konto-Zahlungsverkehr zu identifizieren und zu priorisieren.

Die Vorstudie wurde in Zusammenarbeit mit einer ausgewählten Gruppe von Banken und weiteren Mitgliedern der SBVg durchgeführt (BCV, Entris Banking, Julius Bär, Migros Bank, PostFinance, Raiffeisen, SIX, UBS und ZKB) und von der Unternehmensberatung Acrea unterstützt. Die Ergebnisse basieren auf umfassender Recherche zur kollaborativen Betrugsprävention, Interviews und Workshops mit Betrugsexpertinnen und -experten sowie Fachleuten aus den Bereichen Recht und Compliance der teilnehmenden Schweizer Banken als auch mehreren Interviews mit ausgewählten Anbietern von Betrugsmanagementlösungen. Diese Aktivitäten fanden zwischen Ende August 2024 und Anfang März 2025 statt.

Dieser Bericht fasst die wichtigsten Erkenntnisse der Vorstudie zusammen und skizziert drei Handlungsempfehlungen für das weitere Vorgehen.

Aktuelle Trends und Herausforderungen in der Betrugsprävention

Kontinuierlicher Wandel hin zu digitalen Zahlungen

Digitale Zahlungen haben die Art und Weise, wie Privatpersonen und Unternehmen finanzielle Transaktionen durchführen, grundlegend verändert. Sie bieten Geschwindigkeit, Komfort und eine hohe Zugänglichkeit. Mobile Wallets, kontaktlose Zahlungen und Online-Banking sind mittlerweile zur Norm geworden und prägen das Verhalten sowie die Erwartungen der Verbraucher. Mit dem Wachstum digitaler Transaktionen steigt auch die Relevanz, diese Transaktionen vor Betrug zu schützen.

Die wachsende Bedrohung durch KI-gestützten Betrug

Betrüger machen sich die Möglichkeiten neuer Technologien, einschliesslich generativer KI, zunutze, um raffinierte Betrugsmaschen durchzuführen. Die finanziellen Schäden durch Betrug sind hoch, wobei die USA, Dänemark und die Schweiz die höchsten Verluste pro Opfer verzeichnen.[1] Eine weitere aktuelle Studie zeigt, dass mehr als 40 Prozent aller aufgedeckten Betrugsversuche im europäischen Finanz- und Zahlungsverkehrssektor mit KI unterstützt sind.[2] Dazu gehören Deepfakes, synthetische Identitäten

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)

und ausgeklügelte Phishing-Kampagnen. Die zunehmende Zusammenarbeit zwischen Cyberkriminellen und anderen böswilligen Akteuren, begünstigt durch den Austausch gestohlener Daten im Darknet, steigert zudem die Effektivität und den Erfolg betrügerischer Machenschaften.

Betrugstrends in der Schweiz

In den letzten Jahren ist die Zahl der Internetbetrugsfälle sowohl weltweit als auch in der Schweiz weiter gestiegen. Laut dem Bundesamt für Cybersicherheit (BACS) stehen Phishing-Angriffe, Rechnungs-betrug, Identitätsdiebstahl und Social-Engineering-Betrugsmaschen an der Spitze der Cyberkriminalität in der Schweiz und führen zu erheblichen finanziellen Verlusten. Mit der zunehmenden Verbreitung von Instant Payments wird auch «Instant Fraud» zur Realität, was traditionelle Betrugspräventionsmechanismen vor neue Herausforderungen stellt.

Die Verknüpfung von Betrug und Geldwäsche

Betrug und Geldwäsche sind oft miteinander verbunden und bilden den sogenannten «FinCrime Cycle». Cyberkriminelle erlangen illegale Gelder durch Betrugsmethoden wie Phishing, Identitätsdiebstahl und Romance Scams. Diese Gelder werden anschliessend über Netzwerke von «Money Mules» gewaschen.

Stärkung der Betrugsprävention durch kollaborative Ansätze

Schweizer Banken setzen bereits eine Vielzahl wirksamer Massnahmen im Betrugsmanagement ein, darunter fortschrittliche Betrugserkennungssysteme. Um den zunehmenden Betrugsbedrohungen adäquat entgegenzuwirken, ist eine verstärkte Zusammenarbeit zwischen Banken, anderen Branchen und Aufsichtsbehörden von entscheidender Relevanz. Beispielsweise könnte die Analyse des «Gesamtbildes» von Konto-zu-Konto-Zahlungen auf Netzwerkebene helfen, Betrugs- und Geldwäschenetzwerke aufzudecken, die ihre Aktivitäten über mehrere Institutionen hinweg verteilen. Auch die Bank für Internationalen Zahlungsausgleich (BIZ) hat das Potenzial kollaborativer Betrugserkennung betont, etwa durch Initiativen wie «Project Aurora» (2023), die zeigen, wie gemeinsame Datenanalysen zur Prävention von Finanzkriminalität beitragen können.

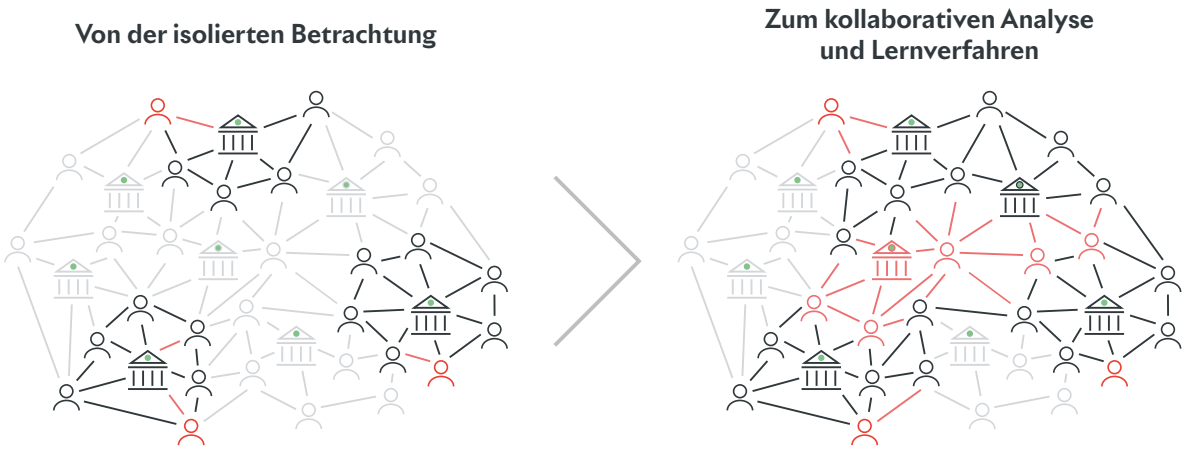

Abbildung 1: Veranschaulichte Absicht. Von einer isolierten Sicht zu einer institutsübergreifenden Sicht · **Quelle:** BIS Innovation Hub «Project Aurora»

Kollaborative Betrugsprävention in der Schweiz: Aktuelle Situation

In der Schweiz gibt es bereits zahlreiche Massnahmen zur kollaborativen Betrugsprävention. Beispiele hierfür sind unter anderem die Dienstleistungen von Switch CERT, das Bundesamt für Cybersicherheit (BACS) und die Initiative «eBanking – aber sicher!» der Hochschule Luzern. Darüber hinaus fördert die Swiss Financial Intelligence Public Private Partnership (Swiss FIPPP) den Informationsaustausch zwischen der Meldestelle für Geldwäscherei (MROS) und Schweizer Finanzinstituten aus dem Privatsektor, um strategische Erkenntnisse zu Trends und Typologien der Finanzkriminalität auszutauschen.[3] Dennoch hat die Vorstudie gezeigt, dass weiteres Potenzial für eine stärkere Abstimmung und Ergänzungen im Bereich der kollaborativen Betrugsprävention besteht. Die «Top 3» der zusätzlichen Massnahmen, die von den Betrugsexpertinnen und Betrugsexperten der Studienpartner gemeinsam priorisiert wurden, werden im Folgenden vorgestellt.

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

Empfehlungen aus der Vorstudie

Basierend auf den Erkenntnissen aus der durchgeführten Vorstudie empfehlen wir der Schweizer Finanzbranche, die folgenden drei Massnahmen weiterzuverfolgen:

Abbildung 2: Empfohlene Massnahmen aus der SBVg · **Quelle:** Eigene Darstellung

Umsetzung gemeinsamer Sensibilisierungskampagnen

Grundidee

Durch die Bündelung von Ressourcen der Banken und bestehender Kommunikationsformate zur Betrugsprävention soll eine einheitliche, gut erkennbare Marke mit hoher Reichweite geschaffen werden. Ziel ist es:

- die breite Schweizer Öffentlichkeit sowie kleine und mittlere Unternehmen (KMU) noch stärker für Betrug im Zahlungsverkehr zu sensibilisieren.
- die Bevölkerung über die Existenz und Gefahren von Betrug zu informieren und sie zu befähigen, angemessen zu handeln, um nicht Opfer von Betrugs- oder Phishing-Versuchen zu werden.
- einen zentralen Ansprechpartner für allgemeine mediale Anfragen zu Betrugsthemen (unabhängig von individuellen Kundenfällen) bereitzustellen.

Begründung

Durch die rasante Weiterentwicklung von KI-Technologien werden Betrugs- und Phishing-Angriffe immer raffinierter und zahlreicher. In diesem Zusammenhang ist eine gut informierte Bevölkerung eine zentrale

präventive Massnahme. Zwar gibt es bereits zahlreiche Kommunikationsformate zur Betrugsprävention im privaten und öffentlichen Sektor, doch besteht weiteres Potenzial in der besseren Abstimmung von Botschaften und der Bündelung von Budgets. Dies würde die Reichweite und Wirkung der Betrugsaufklärung erheblich verstärken.

Umsetzungsaspekte

Gemeinsame Awareness-Kampagnen sollten in einem unabhängigen, offenen Format (z. B. einem Verband) mit einem mittelfristigen Investitionsplan organisiert werden. Dieses Format sollte alle relevanten Akteure einbinden, darunter Banken, bestehende Kommunikationsformate sowie Stakeholder ausserhalb der Finanzdienstleistungsbranche. Dazu zählen beispielsweise die Polizei, die Schweizerische Kriminalprävention, andere öffentliche Behörden und Anbieter digitaler Marktplätze wie die SMG. Zu den offenen Fragen gehören unter anderem der genaue Umfang, die Governance sowie das Betriebs- und Finanzierungsmodell des gemeinsamen Formats. Diese strukturellen Fragen sollen in der ersten Phase eines spezifischen Hauptprojekts geklärt werden. In späteren Phasen folgen die Entwicklung, Gestaltung und Umsetzung gemeinsamer Kommunikationsmassnahmen zur Betrugsprävention, einschliesslich der Definition des gemeinsamen Marktauftritts («Brand»).

Projekt-Governance

Bereits im Jahr 2024 fanden erste konstruktive Gespräche zwischen verschiedenen Akteuren zur Kommunikation im Bereich Betrugsprävention im Rahmen der Initiative «Pay Attent!on» (ehemals bekannt als «Swiss Cyber Security Awareness Roundtable») statt. Diese Initiative wurde von EBAS.ch, card-security.ch und UBS ins Leben gerufen.

Die Vorstudie der SBVg empfiehlt, diese Initiative weiterzuführen und auf zusätzliche Stakeholder (z. B. weitere Banken) auszuweiten. Ziel ist es, im Jahr 2025 die organisatorische Struktur zu spezifizieren und zu institutionalisieren, um ab 2026 gemeinsame Awareness-Kampagnen zu starten.

Vertiefte Prüfung eines Risikobewertungsdienstes auf Netzwerkebene

Grundidee

Ein zentraler Anbieter soll einen Dienst entwickeln, der während der Eingabe von Konto-zu-Konto-Zahlungsdaten in Echtzeit einen Risikowert berechnet. Dieser Risikowert kann von den sendenden Banken nach eigenem Ermessen genutzt werden, z. B. als zusätzliches Signal in ihren eigenen Risikobewertungs-Modellen oder als Bestandteil einer Betrugspräventionslösung eines von der Bank gewählten Anbieters. Die Berechnung des Risikowerts erfolgt unter anderem durch eine Analyse auf Netzwerkebene mithilfe von Machine-Learning-Algorithmen. Im ersten Schritt wird der Dienst voraussichtlich ausschliesslich auf Zahlungsverkehrsdaten basieren, ergänzt durch Betrugsmeldungen der teilnehmenden Banken zu diesen Transaktionen.

Begründung

Risikobewertungsdienste auf Netzwerkebene sind ein leistungsstarkes und einzigartiges Instrument für Banken, um die Risiken auf der Empfängerseite einer Zahlung zu bewerten. Wie wahrscheinlich ist es, dass die Empfänger-IBAN zu einem Geldwäschenetzwerk gehört oder mit einer anderen betrügerischen Aktivität in Verbindung steht? Wenn Banken nur eine isolierte Sicht auf Transaktionen haben, ist diese Einschätzung schwierig. Auf Netzwerkebene lassen sich verdächtige Muster deutlich leichter identifizieren. Dies ist besonders relevant im Kampf gegen die stark zunehmende Betrugsform der Scams, bei denen Bankkunden dazu gebracht werden, selbst illegitime Zahlungen einzugeben. Erfahrungen aus dem Vereinigten Königreich, wo ein solcher Dienst (Vocalink) bereits implementiert ist, zeigen erhebliche Vorteile – sowohl in der Erhöhung der Betrugserkennungsrate als auch in der Reduzierung von Fehlalarmen (False Positives).

Umsetzungsaspekte

Angesichts der zentralen Rolle von Swiss Interbank Clearing (SIC) im Schweizer Konto-zu-Konto-Zahlungsverkehr ist SIC prädestiniert, einen Risikobewertungsdient auf Netzwerkebene zu entwickeln. Zwei Optionen wurden für die Rolle von SIC identifiziert: SIC könnte entweder den Dienst selbst anbieten oder andere Dienstleister dazu befähigen. Basierend auf einem ersten Vergleich dieser Optionen anhand von vier Kriterien (Effektivität, Effizienz, Potenzial für Service-Erweiterungen und Compliance) haben die Expertinnen und Experten der teilnehmenden Banken eine klare Präferenz dafür geäussert, dass SIC den Dienst selbst anbietet. Die Machbarkeit dieses Ansatzes muss durch eine eingehenden Machbarkeitsanalyse (einschliesslich rechtlicher und Compliance-Aspekte) weiter analysiert werden.

Projekt-Governance

Als nächsten Schritt regen die an der Vorstudie beteiligten Banken an, dass das SIC, eine eingehende Machbarkeitsanalyse zu diesem Thema durchführt. Die Schweizerische Nationalbank (SNB) unterstützt dieses Vorgehen.

Förderung des produkt- und branchenübergreifenden Austauschs

Grundidee

Sicherstellung eines dauerhaften Austauschs zwischen Betrugsexpertinnen und-experten über verschiedene Zahlungsprodukte (z. B. Konto-zu-Konto-Zahlungen, Kredit- und Debitkarten, Twint, Krypto) und Branchen hinweg (z. B. Telekommunikation, Marktplätze, soziale Medien). Die Ziele dieses Austauschs sind:

- effizienter Austausch von Wissen, Best Practices und Bedrohungsinformationen.
- Diskussion, Priorisierung und Initiierung zukünftiger gemeinsamer Massnahmen im Betrugsmanagement.

- Motivation anderer Branchen (z. B. Telekommunikation, digitale Marktplätze und Plattformen) zu zusätzlichen oder verbesserten Betrugspräventionsmassnahmen, indem die Stimme der Banken gebündelt wird.
- bei Bedarf Koordination mit Regulierungsbehörden zu rechtlichen und aufsichtsrechtlichen Aspekten des Betrugsmanagements.

Begründung

In der Schweiz existieren bereits mehrere betrugsbezogene Austauschforen und Plattformen (z. B. Switch CERT, BACS, SPC, PaCoS, EBAS, card-security.ch, SBVg E-Alarm). Dennoch besteht laut den Teil- nehmern der Vorstudie weiteres Potenzial, die Koordination über Zahlungsprodukte und Branchen hinweg zu verbessern. Eine verstärkte branchenübergreifende Zusammenarbeit ist besonders wichtig, da ein grosser Anteil der Scams auf digitalen Marktplätzen und Plattformen entsteht und/oder durch fehlende präventive Massnahmen in anderen Branchen begünstigt wird (z. B. Spoofing-Prävention).

Umsetzungsaspekte

Um die Gruppengrösse überschaubar zu halten, soll nicht ein einziges, zentrales Betrugsaustauschforum geschaffen werden. Stattdessen sollten mehrere Foren strukturiert werden, beispielsweise nach Zielgruppen wie Senior Product Manager und technische Experten. Zur Definition des optimalen Sets zukünftiger Betrugsaustauschgremien empfiehlt die Vorstudie die Durchführung der folgenden vertieften Analyse im Rahmen eines Hauptprojekts:

- Detaillierte Erfassung aller bestehenden Betrugsaustauschformate (Teilnehmer, Ziele, Aktivitäten, Kommunikationsplattformen, usw.).
- Identifikation von Lücken und Überschneidungen zwischen den bestehenden Formaten.
- Erarbeitung von Anpassungsvorschlägen für bestehende Formate sowie Identifikation potenzieller neuer Foren basierend auf den festgestellten Lücken und Überschneidungen.

Projekt-Governance

Die empfohlene vertiefte Analyse sollte idealerweise von einem branchenweiten Gremium durchgeführt werden, das unabhängig von bestehenden Betrugsaustauschformaten ist und enge Verbindungen zu anderen Branchen und Regulierungsbehörden hält. Daher wird die SBVg ermutigt, die erforderliche vertiefte Analyse zu leiten – in enger Zusammenarbeit mit den Banken und, falls erforderlich, dem Swiss Financial Sector Cyber Security Centre (FS-CSC).

Fazit

«Es braucht ein Netzwerk, um ein Netzwerk zu schlagen.» Um mit den sich ständig weiterentwickelnden Betrugstaktiken und der raschsteigenden Zahl an Betrugsversuchen Schritt zu halten, muss der Finanzsektor seine Betrugspräventionsansätze kontinuierlich weiterentwickeln. Wir sind überzeugt, dass zusätzliche, kollaborative Ansätze zur Betrugsprävention erforderlich sind. Diese Ansätze wurden im Rahmen der durchgeführten Vorstudie systematisch analysiert. Die drei priorisierten Massnahmen, die in diesem Bericht vorgestellt werden, stellen wichtige und konkrete Schritte dar, um diesen Entwicklungen zu begegnen.

Projekt-Team

Richard Hess, Schweizerische Bankiervereinigung SBVg
Stephan Odermatt, Acrea AG
Stephan Wengi, Acrea AG

Experten der teilnehmenden Banken

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, Zürcher Kantonalbank
Bogdan Iancu, Banque Cantonale Vaudoise
Nicky Kern, UBS Switzerland AG
Lukas Peter, Zürcher Kantonalbank
Romano Ramanti, Zürcher Kantonalbank
Arlind Spahija, Migros Bank AG
Seline Trachsel, Bank Julius Bär & Co. AG
Michael Wili, PostFinance AG
Stephan Zimmermann, PostFinance AG
Simon Züst, Raiffeisen Schweiz Genossenschaft

Schweizerische
Bankiervereinigung
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch