



Luzerner
Kantonalbank

Betrugsbekämpfung - eine holistische Sicht

Workshop

VSKB Legal & Compliance Tagung

Peter Felder

12.06.2026

Agenda

1 Ausgangslage

2 Problemstellung

3 Lösungsansatz LUKB

4 Diskussion

Ausgangslage

Zunahme von Fraud-Fällen

Ab 2021

- massive Zunahme von Fraud-Fällen, insb. Cyber-Betrugsfälle (Faktor 10, sowohl bei der Anzahl Fälle, als auch bei der Anzahl MROS-Meldungen !)
- alle Varianten von Betrug (**Scam/Betrug**: +52% [falscher Polizist, falscher Bankmitarbeiter, falscher Microsoft-Supporter, Vorschuss-/Auktionsbetrug (Ricardo, Tutti, Facebook Marketplace, etc.), Anlagebetrug], **Phishing**: +23%, **Spam&allg. Meldungen**:+15%, **andere Arten**: +10%)

gestiegene Herausforderungen

- ... die schiere Masse an Fällen
- ... Betrugs- oder Schadensmeldungen kommen auf unterschiedlichsten Kanälen herein
- ... rechtzeitiges Zurückfordern
- ... Installieren von Betrugsbekämpfungssystemen
- ... Schadensbearbeitung (Rechtsfälle: Verhandlungen mit Kunden, Ombudsman, Gerichte)
- ... Belastung vieler verschiedener in der Bank involvierter Stellen
- ... gestiegene finanzielle und Reputations-Risiken
- ... gesteigener Ressourcenbedarf

Betrugsarten

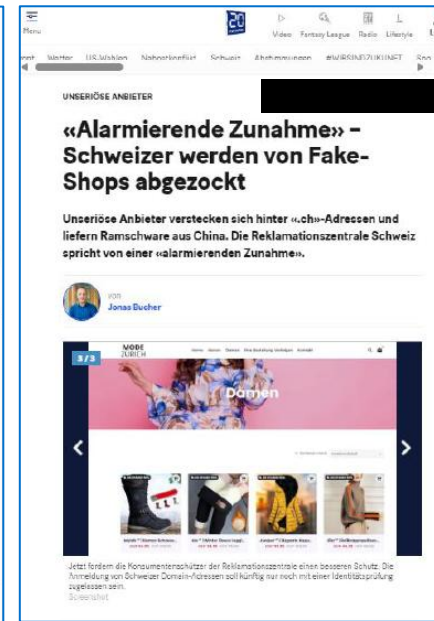
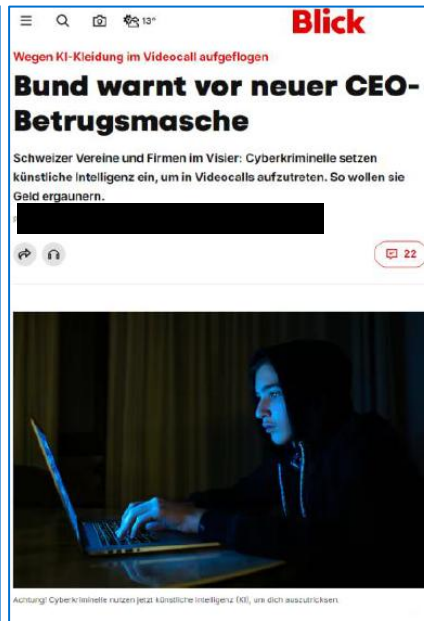
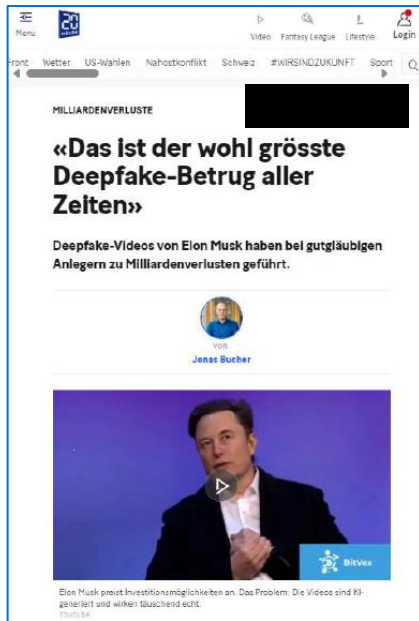
Phishing

Phishingattacken zielen darauf ab, die Credentials von Bankkunden zu stehlen, um Zugang zu digitalem Banking oder Kartendaten zu erhalten



Scam

Scams zielen darauf ab, Menschen so zu manipulieren, dass sie betrügerische Transaktionen eingeben, ausführen oder autorisieren (z.B. Anrufe von falschen Bank-, Polizei-, Regierungs-, Supportmitarbeitern, Anlageberatern, gefälschte E-Commerce-Shops, Betrug auf Online-Marktplätzen, Liebesbetrug, Anweisungen per E-Mail/Telefon von falschem CEO/CFO, etc.)



Money Mules

Money Mules (MM's) erhalten Zahlungen zur Weiterleitung (Überweisung auf weitere MM's, Kauf von Cryptowährungen, etc.)



... und es nimmt nicht ab ...

Innovation und Technologie

- Künstliche Intelligenz macht es immer einfacher zu betrügen (Fake-Briefe, Fake-Websites, Fake-Identitäten, Fake-Stimmabdruck, etc., in immer besserer "Qualität")
- Trade-off zwischen "Bequemlichkeit"/"Kundenfreundlichkeit" und Sicherheit (einfache Authorisierung, QR-Codes, SMS, etc.)
- Neue Produkte wie Instant Payment, digitales Onboarding

Betrüger werden immer "professioneller"

- Betrug "as-a-service", Hacker Bibliotheken → mit wenigen Franken "ist man dabei"
- Zunahme von gestohlenen Daten und deren Verfügbarkeit im Darknet → personalisierte Attacken werden ermöglicht
- Angriff produktübergreifend wegen Self-Service-Funktionen → Betrüger haben genaue Kenntnis von (auch internen) Abläufen und Prozessen

Problemstellung

Wie erreichen Fraud-Fälle die Bank?

Informationen von extern

- Kunde kontaktiert die Bank
- E-Banking Self Service
 - Hotline / Support
 - via Kundenberatung (Telefon, E-Mail, etc.)
 - am Schalter
 - Hinweis von Dritten
 - Editionsverfügung Stawa
 - E-Alarm, etc.

Informationen von intern

- Hinweise aus internen Systemen
- Betrugsbekämpfungssystem
 - Zahlungsverkehrssystem
 - SIX-Mitteilung
 - TWINT-Mitteilung
 - Rückruf andere Bank

Notwendige Tätigkeiten

- Sachverhalt aufnehmen, Kundenangaben erfragen
 - Vorfall, Auffälligkeiten möglichst genau beschreiben
- Sofortmassnahmen ergreifen
 - E-Banking sperren
 - Geld zurückfordern
 - intern betroffene Stellen informieren
- Sachverhalt vertiefen
 - Rückfragen/Feedback beim Kunden
 - Meldungen erstatten
 - Kundenforderungen bearbeiten

Schwierigkeiten / Herausforderungen

- (un)strukturierte Koordination der verschiedenen internen Stellen
 - Kundenberatung
 - Supporteinheiten (E-Banking, Kartenstelle, TWINT-Verantwortliche etc.)
 - Zahlungsverkehr
 - Legal und Compliance (Meldesachverhalte, Rückforderungen, rechtliche Abklärungen)
 - Technik: Sind Massnahmen in Bezug auf die Systeme notwendig?
- Zeitmanagement (insb. bei Rückforderungen)
- Einheitliche und konsistente Kundenkommunikation
 - Sachverhaltsabklärungen
 - Schadensbearbeitung

Phasen der Betrugsbekämpfung - mögliche Handlungsfelder

Betrugsprävention - Kunden schützen

- Kommunikation und Information
- Zahlungsbestätigung
- Intervention an der Quelle der Zahlung
- eingeschränktes Onboarding
(keine "unerwünschten" Kunden eröffnen)
- Authentisierung von Transaktionen
- Sicherheits- und Limitensystem

Betrug detektieren

- Anomalitäten erkennen
- Alerts / Betrugs Handling

Fälle bearbeiten

- Abwicklung von Schadensfällen

Verbesserte Koordination (Bankweit)

- Prozesse / Abläufe koordinieren
- Systeme alignieren
- Innen- und Aussenkommunikation
produktunabhängig gestalten

Ressourcen gezielt einsetzen

- Themen zusammenführen
- Kundenkommunikation verbessern

Technik anpassen

- Fraud Detection Tool anpassen
- neue Technologien prüfen (z.B. Detection analog DebiX oder OneApp erweitern auf andere Systeme)
- ...

Lösungsansatz LUKB

Ziele

Anforderungen an das Fraud Management

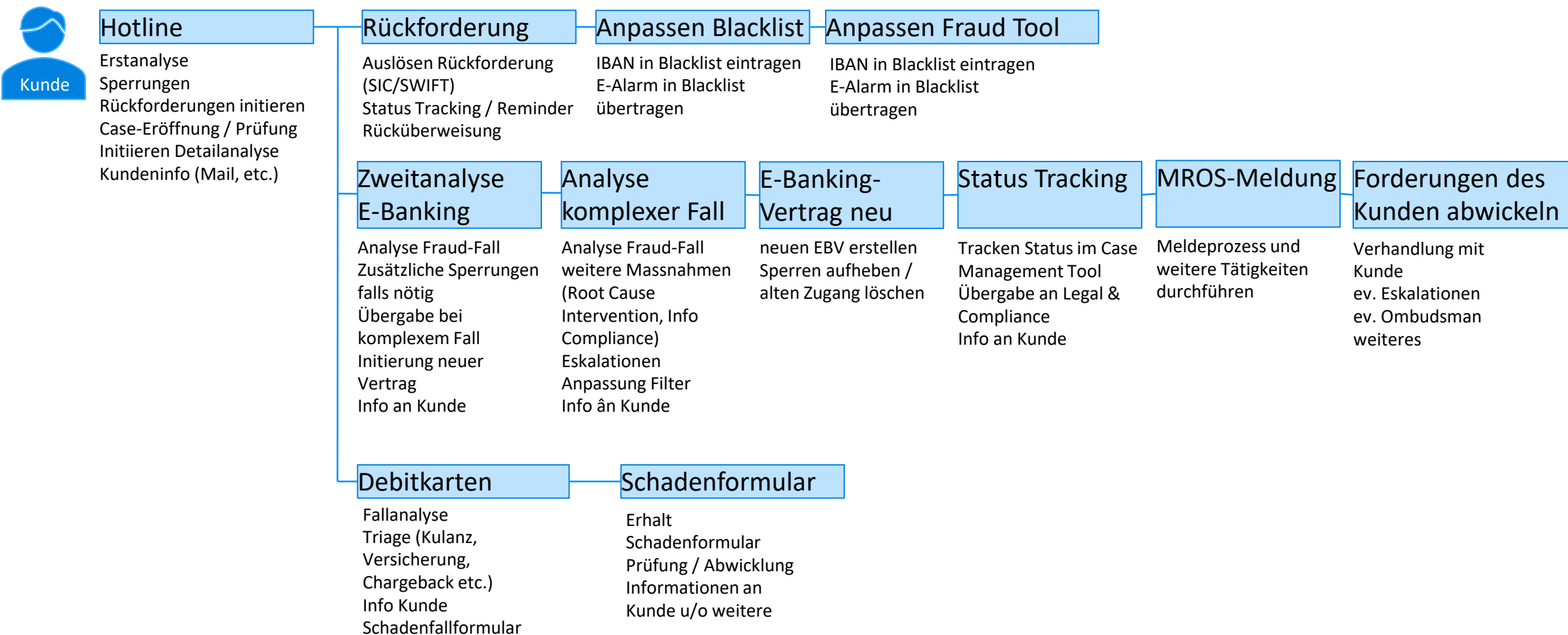
- **Customer Experience**
 - Kunden kanalunabhängig abholen
 - aktives Angehen von Fraud, schnelle Reaktion, Aufzeigen von Optionen
 - keine Convenience-Verluste
- **Prozesse**
 - intern und extern klare Anlaufstelle(n) für Beratung, Unterstützung und regelmässige Statusinformation zum Fall
 - End-to-end Prozess, zahlmittel- und kanalunabhängig
 - Priorisierung von Aufgaben (Reaktionszeit in-no-time)
- **Systeme**
 - Self-Service-Funktionalitäten und externe Partnerlösung ermöglichen 7/24-Modus
 - Anomalitäten werden über alle Kanäle und Zahlungsmittel hinweg erkannt
 - Casemanagementsystem hilft den Status des Cases und der Folgemaassnahmen zeitnah zu tracken und dem Kunden zu kommunizieren
- **Skills**
 - Alle Mitarbeitenden haben ein einheitliches und klares Verständnis zur Relevanz von Fraud Management
 - Rollen "Melder", "Analyst", Case Manager", "Abwickler" werden aktiv gelebt
 - Abwicklungsaufgaben können über externe Partner bezogen werden
- **Governance**
 - definierter konzeptioneller Lead
 - professionelles Informationsmanagement
 - zentrale Triage von Fällen
 - proaktive Kundeninformation

Ziele

kanalunabhängig / schnell und ressourceneffizient / präventiv / konsequent / kompetent / klare Rollen und Verantwortungen / möglichst convenient

Ablauf Fraud Management / Case Handling

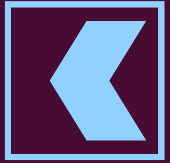
Ausgangspunkt: Kunde



Ausgangspunkt: System-Alert / Alert von dritter Partei



Fragen / Diskussion



**Luzerner
Kantonalbank**

Luzerner Kantonalbank AG

Pilatusstrasse 12

6003 Luzern

lukb.ch