

Zahlungsdienstleister- Störung

**Der Superbooster für Zahlungsbetrug –
Wie Schwächen im System funktionierende Kontroll-
systeme bei Finanzdienstleistern herausfordern**

I. Eine Zusammenfassung über den Zahlungsbetrug

Im dritten Quartal 2025 erschütterte ein massiver Systemausfall den europäischen Finanzmarkt: Bei einem der größten Zahlungsdienstleister kam es zu einem **Ausfall der internen Kontrollsysteme**. In der Folge wurden ungeprüfte Lastschriften im Wert von mehr als 10 Milliarden Euro an deutsche Banken weitergeleitet. Betroffen waren alle großen Banken in Deutschland. Sie stoppten kurzfristig **alle Zahlungen des Zahlungsdienstleisters**, um Schaden abzuwenden. Schätzungen zufolge, waren mehrere hunderttausend Kundinnen und Kunden direkt oder indirekt betroffen: Händler erhielten ihre Gelder nicht

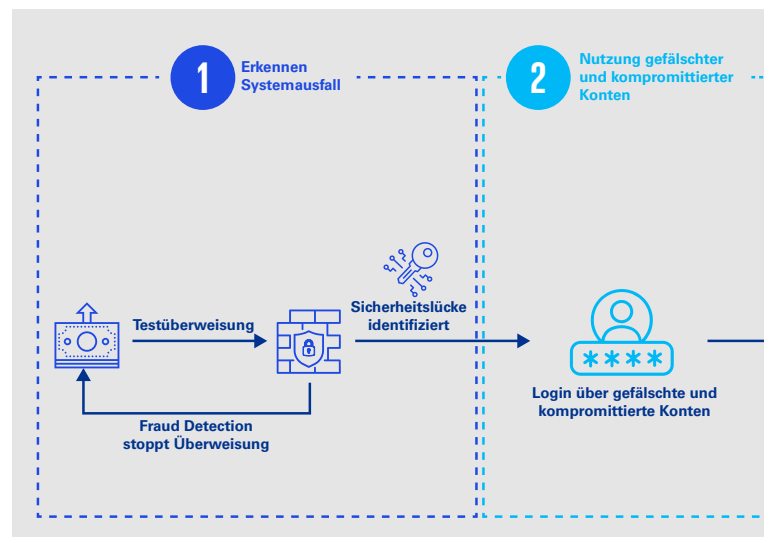
und Verbraucherinnen und Verbraucher sahen verdächtige Abbuchungen auf ihren Konten. Das grundsätzliche Problem lag darin, dass die betrugspräventiven Filter des Zahlungsdienstleisters vollständig versagten. Dadurch gelangten selbst völlig unplausible Abbuchungen – bis hin zu Einzelfällen über mehrere hundert Millionen Euro – **ungefiltert in den Bankenclearingprozess**. Erst als die Banken selbst eingriffen und vorsorglich die Transaktionen blockierten, konnte der Vorgang gestoppt werden. Der Vorfall gilt als einer der größten operationellen Zwischenfälle im europäischen Zahlungsverkehr der letzten Jahre.

1. Ausfall der ersten Kontrollinstanz

Im Zentrum des Vorfalls stand der **komplette Ausfall von internen Fraud- und Batch-Validierungssystemen**, die normalerweise jede Lastschrift vor der Weiterleitung an die Banken prüfen. Über mehrere Stunden hinweg – von Freitagabend bis Montagmorgen – blieben die Sicherheitsfilter inaktiv, sodass **sämtliche Lastschriften ungeprüft** in den Bankenclearingprozess eingespeist wurden. Betroffen war vor allem das Modul zur Erkennung unautorisierter oder fehlerhafter Mandate, das im Regelbetrieb verdächtige Abbuchungen aussortiert. Dadurch gelangten selbst extrem unplausible Buchungen in Millionenhöhe ungehindert in den Zahlungsstrom. Hinweise auf ein menschliches Versagen im Rahmen der Validierung gibt es bislang nicht. Nach aktuellem Kenntnisstand war eine technische Panne oder ein interner Systemfehler ursächlich. In der Folge mussten erst die Banken eingreifen, um die Auswirkungen des Ausfalls einzudämmen – ein Hinweis darauf, wie stark die Branche auf die vorgelagerten Filter von Zahlungsdienstleistern vertraut.

2. Vorgehensweise der Fraudster – ein mögliches Anwendungsszenario

Abbildung 1:
Denkbare Vorgehensweise der Fraudster



Quelle: KPMG in Deutschland, 2025

II. Die Rolle der Banken als zweite Kontrollinstanz

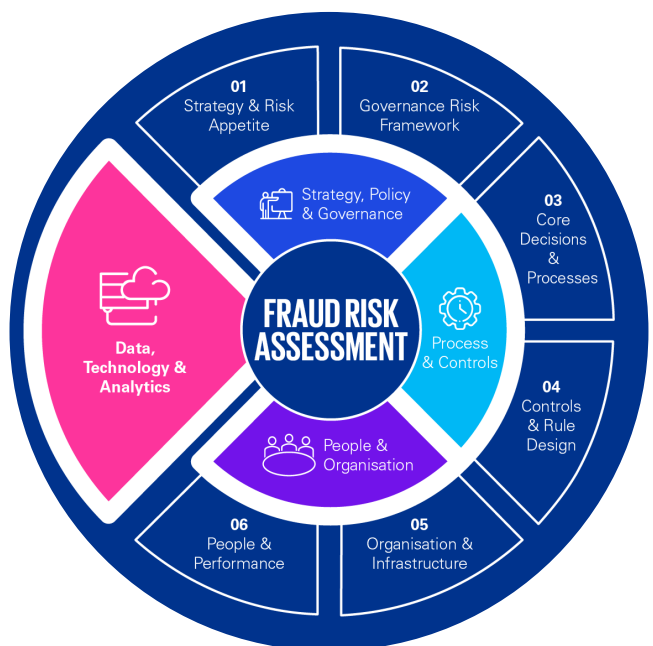
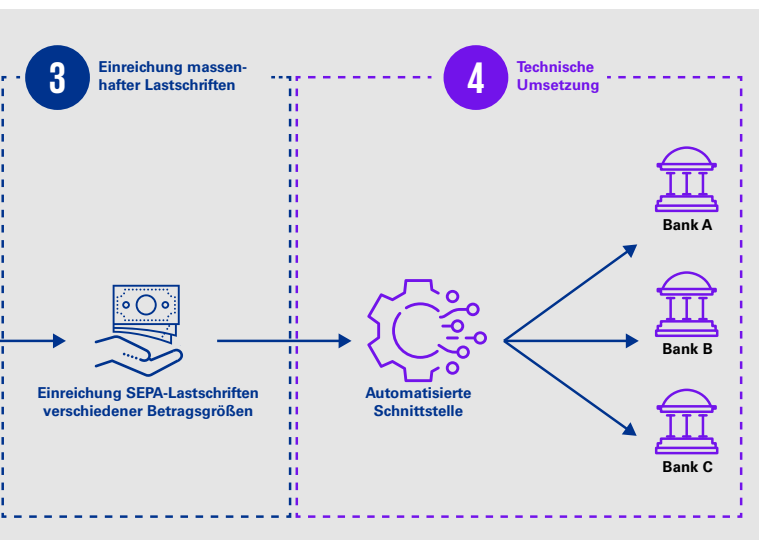
Die Banken agierten als nachgelagerte Kontrollinstanz – ihre Systeme griffen erst reaktiv. Klassische Fraud- und Anti-Money-Laundering(AML)-Algorithmen sind vor allem auf individuelle Auffälligkeiten wie untypische Beträge oder Kundenverhalten sowie bekannte Risikomuster ausgelegt. Ein systemischer Partnerausfall wird von ihnen nicht erfasst. Hinzu kommt, dass viele Monitoringsysteme im Zahlungsverkehr auf Grundlage von arbeitstäglichen Batch-Läufen aufgebaut sind und am Wochenende zumeist keine operative Überprüfung von Alerts aus den verarbeiteten Prüfläufen erfolgt. Dadurch wurde das volle Ausmaß der fehlerhaften Lastschriften erst am Montagabend sichtbar und konnte erst am Dienstagmorgen analysiert werden.

Ein wesentlicher Grund für das späte Erkennen war das Fehlen wirksamer Indizienmodelle: Die eingesetzten Transaktionsmonitoring- und Screeningssysteme waren nicht darauf kalibriert, massenhaft fehlerhafte Lastschriften von einem einzigen Großeinreicher zu erkennen. Insbesondere vor dem Hintergrund der „New Payment Methods“ zeigen sich gravierende Blind Spots. Wesentliche Szenarien wie

„ungewöhnliche Volumenspitzen pro Einreicher“, „Mandats- oder Dateninkonsistenzen in Serien von Zahlungen“ oder „unplausible Extrembeträge in Retail-Lastschriften“ waren nicht ausreichend implementiert. Somit fehlten den Banken die heuristischen Indikatoren, um einen kollektiven Kontrollverlust aufseiten des Zahlungsdienstleisters frühzeitig zu identifizieren.

Nachdem die Anomalien schließlich erkannt worden waren, reagierten die Institute mit der pauschalen Blockade sämtlicher Transaktionen des Zahlungsdienstleisters. Diese drastische Maßnahme verhinderte zwar unmittelbare Schäden, machte aber zugleich deutlich, dass die bestehenden Systeme zwar wirksam gegen Einzelfälle sind, gegenüber systemischen Ausfällen jedoch blind sind.

Abbildung 2: **Analysedimensionen im Fraud-Risk-Management**



Quelle: KPMG in Deutschland, 2025

III. Handlungsempfehlungen und Lessons Learned

Der Vorfall ist ein Lehrbuchbeispiel für operationelle Risiken durch Dritte. Der Ausfall einer einzigen Kontrollinstanz reichte aus, um Milliardenbeträge im europäischen Zahlungsverkehr zu blockieren. Er macht deutlich, wie stark Banken und Händler von der Zuverlässigkeit externer Zahlungsdienstleister abhängig sind – und welche systemischen Effekte eintreten können, wenn diese versagen.

Die Digital-Payments-Industrie und BigTechs haben einen klaren Vertrauensauftrag: Kundinnen und Kunden erwarten, dass Zahlungsinfrastrukturen selbst unter Stress sicher funktionieren. Einmal verlorenes Vertrauen in die Stabilität solcher Systeme lässt sich nur schwer zurückgewinnen.

Banken und Zahlungsdienstleister müssen ihre Resilienz gegenüber „Single Points of Failure“ stärken. Dazu gehören mehrstufige Kontrollmechanismen, wirksame Indizien, Backup-Systeme, klar definierte Notfallprozesse und eine enge Zusammenarbeit zwischen Providern und Banken. Nur durch robuste Governance, technische Redundanz und transparente Kommunikation lässt sich künftig verhindern, dass der gesamte Zahlungsverkehr durch den Ausfall eines einzelnen Akteurs ins Wanken gebracht wird.

Unser Drei-Phasen-Modell zur Überprüfung und Optimierung Ihrer Fraud-Detection-Landschaft:

Phase 1: Assessment & Ist-Analyse

- Aufnahme und Dokumentation aller Fraud-relevanten Prozesse und Kontrollen zur Prävention, Untersuchung und Eskalation
- Erfassung der bestehenden System- und Architekturkomponenten inklusive relevanter Schnittstellen, Datenquellen und Datenflüsse



Phase 2: Detektion von Blind Spots

- Exploration potenzieller Datenquellen für ungewöhnliche Transaktionsmuster
- Stress-Tests und Red Teaming – systematische Überprüfung von Fraud-Regeln und -Modellen durch Simulationen und Angriffsszenarien
- Data Mining zur Erkennung unbekannter Muster oder Anomalien
- Benchmarking – Vergleich der eigenen Fraud-Kennzahlen mit Datenpools anderer Institute

Phase 3: Optimierung & Implementierung

- Erweiterung des Indizienmodells und Anpassung der Schwellenwerte innerhalb der Monitoringsysteme: Aufnahme spezifischer Regeln, zum Beispiel Mandatsfehler, unplausible Extrembeträge oder wiederkehrende Datenfehler
- Ausbau des Kontrollspektrum, insbesondere doppelte Auslegung kritischer Kontrollen (Batch-Validierung, Mandatsprüfung), damit beim Ausfall eines Moduls ein Failover-System greift
- Aufbau zusammengesetzter Data Lakes und kontinuierliches Data Mining zur Detektion neuer Betrugsmuster
- Radarfunktionalität Darknet-Monitoring – automatisiertes Screening von Darknet-Quellen nach angebotenen Zahlungsanbieter- und Bank-Accounts zur frühzeitigen Erkennung erhöhter Betrugsrisiken

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft



Torsten Jurisch
Partner,
Financial Services
M +49 173 6523003
tjurisch@kpmg.com



Volker Smielick
Director,
Financial Services
M +49 151 55382357
vsmielick@kpmg.com



Isehdinn Semmo
Manager,
Financial Services
M +49 151 42460459
isemmo@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia



Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2025 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.