INSTANT PAYMENTS IN DER SCHWEIZ
WO LIEGT DIE WAHRE HERAUSFORDERUNG?

Im August 2024 ist es soweit. Dann müssen die grossen Schweizer Banken Instant Payment- (IP) Zahlungseingänge verarbeiten[1] und haben die Möglichkeit, IP-Zahlungsausgänge in ihr Kundenangebot aufzunehmen. Konkret heisst das, dass bei Zahlungen aus der Schweizer Zahlungsinfrastruktur SIC bis 100 000 Schweizer Franken, der Begünstigte innerhalb von zehn Sekunden über den Betrag verfügen kann. Die Transaktion ist unwiderruflich final. Bereits jetzt wird deutlich, dass dies eine technische Herausforderung für die Zahlungsabwicklung darstellen wird. Doch wie wirken sich diese Anforderungen in Hinsicht auf Compliance und Risikomanagement aus? Können die Risiken trotz dieser Marktinitiative weiterhin bewältigt werden?

TRANSAKTIONS-SCREENING, BETRUGSERMITTLUNG & TRANSAKTIONS-MONITORING

Alle modernen Transaktions-Screening-Lösungen greifen zur Prüfung von Schlüsselelementen einer Zahlung auf gängige nationale und internationale Prüflisten zurück. So können Transaktionen identifiziert werden, deren Sender oder Empfänger möglicherweise gegen Sanktionen, Geldwäsche- oder Terrorismusfinanzierungsregeln verstossen bzw. einen Betrugsverdacht wecken. Die erste Herausforderung im IP-Bereich stellt die Prüfung von ein- und ausgehenden Zahlungen unter der zeitlichen Bedingung von wenigen Sekunden dar.

In dieser Zeitspanne muss die Begünstigten-Bank der sendenden Bank verbindlich bestätigen, dass sie die Zahlung annehmen wird. Folglich wird die Compliance-Prüfung nicht nur auf der Seite des Belastungskontos, sondern auch auf Seite des Begünstigtenkontos im kürzesten Zeitraum durchgeführt. Das Screening gegen Listen aus dem Sanktions- und Embargobereich sowie in Bezug auf die Betrugserkennung findet zweimal statt.

1. https://www.six-group.com/de/blog/2021/swiss-instant-payments.html

TRANSAKTIONS-SCREENING (SANCTIONS SCREENING / S&E SCREENING)

Wird beim Transaktions-Screening gegen Sanktions- und Embargolisten eine verdächtige Transaktion identifiziert, erfolgt gegenwärtig die erste Überprüfung dieser Transaktion durch einen Bankmitarbeitenden. Dieser Vorgang ist im vorgegebenen IP-Zeitfenster nicht möglich, weshalb die Transaktion in diesem Fall abgelehnt wird. Daher ist es umso wichtiger, dass die automatische, systemseitige Prüfung so wenig falsche Verdachtsmeldungen ("false positives") wie möglich generiert.

Ein Finanzinstitut muss somit festlegen, wie es grundsätzlich mit Warnmeldungen bei Instant Payments umgehen möchte.

Es gilt, unter Berücksichtigung des Risikomanagements, ein moderates Mass zwischen Transaktionsautomatisierung und -ablehnung zu finden, um die regulatorischen Anforderungen bestmöglich umzusetzen ohne das Kundenerlebnis zu beeinträchtigen.

BETRUGSERMITTLUNG (FRAUD DETECTION)

Eine weitere Herausforderung trifft auch den Bereich der Betrugsermittlung (Fraud Detection). Bei Instant Payments geht es nicht nur darum festzustellen, ob Zahlungsaufträge wirklich durch Kunden oder Drittanbieter erfolgt sind, die sich unberechtigt Zugang verschafft haben. Auch das Empfängerkonto kann – zum Schaden der Empfängerbank – sehr schnell"geräumt" werden. Daher wird es im Fraud-Bereich immer wichtiger, auch auf der Empfängerbankseite die eingehenden Zahlungen zu prüfen.

Betrugserkennung, die heute oft nur im Kundenkanal der Senderbank stattfindet, muss künftig unabhängig vom gewählten Kundenkanal (z.B. Mobile Banking oder Kundenberatung) erfolgen. Auch hier stellt sich die Frage, wie das positive Kundenerlebnis bestehen bleiben und gleichzeitig sichergestellt werden kann, dass Betrugsfälle zuverlässig erkannt werden. Bei der Betrugsermittlung im IP-Bereich ist es essentiell wichtig, verdächtige Vorgänge automatisiert zu erkennen – nicht nur durch zusätzliche Datenpunkte (IP-Adresse, Lokation, etc.), sondern auch durch Erkennung atypischer und unbekannter Muster, beispielsweise hinsichtlich des Kundenverhaltens und (kundenseitiger) Abläufe in den relevanten Kanälen. Verstärkt werden dafür Methoden der Künstlichen Intelligenz (AI) angewendet, die in Zukunft eine immer größere Rolle spielen werden. Das haben inzwischen auch die Aufseher erkannt[2].

2. https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.pdf

TRANSAKTIONSÜBERWACHUNG (TRANSACTION MONITORING: ANTI-MONEY LAUNDERING/ COUNTER-TERRORISM FINANCING)

Die Transaktionsüberwachung (AML) wird auch bei Instant Payments oft zusammen mit den sonstigen (non-IP) Transaktionen ex-post im Rahmen der Tagesendverarbeitung durchgeführt. Im AML-Bereich genügt es zunächst, Instant Payments als neuen Zahlungstyp im bisherigen System zu implementieren und ggf. mit spezifischen Regeln zu versehen (z.B. Ausführung 24/7). Obwohl es bisher keine besonderen regulatorischen Anforderungen gibt, sichert diese Art der Verarbeitung allerdings nicht alle möglichen Gefahren und potenziellen Bedrohungsszenarien ab, die durch die Echtzeitverarbeitung von Zahlungstransaktionen entstehen können. Des weiteren muss auch die Mustererkennung bei der Betrugsermittlung sowie bei der Transaktionsüberwachung weiterentwickelt werden. Denn mit der Einführung von Instant Payments halten auch neue/andere Verhaltens- und Transaktionsmuster Einzug, z.B. eine höhere Anzahl (Frequenz) an Zahlungen von kleineren Beträgen. Auch hier kann Künstliche Intelligenz Abhilfe schaffen.

WEITERE AUSWIRKUNGEN AUF COMPLIANCE

Neben den eher technischen Compliance-Belangen, bedarf es auch der Überprüfung von organisatorischen und rechtlichen Themen. Die operationelle Umsetzung innerhalb von Compliance basiert meist auf niedergeschriebene Regelwerke – namentlich auf Policies und Arbeitsanweisungen eines Finanzinstitutes – welche auf notwendig werdende Veränderungen geprüft und im Hinblick auf Änderungen durch Instant Payments bei Transaktions-Screening und Betrugserkennung allenfalls angepasst werden.

Abhängig von der Nutzung der Transaktionsdaten bei weiteren Compliance-Prozessen, wie etwa der Kunden-Risiko-Gewichtung, der Berechnung von Key-Risk-Indicators (KRIs) oder auch dem internen und externen Compliance Reporting, braucht es auch hier eine weitere Analyse – insbesondere hinsichtlich der unterschiedlichen Kundenarten, die das Institut betreut.

Rechtliche Themen umfasssen u.a. auch die Verwendung zusätzlicher Daten, welche besonders den automatisierten Teil der Compliance-Prüfungen entscheidend verbessern können. Die Betrachtung aus einer datenschutzrechtlichen Perspektive ist unabdinglich, um mögliche technische Optionen einsetzbar machen zu können.

FRÜHZEITIGER EINBEZUG ALLER RELEVANTEN UNTERNEHMENSBEREICHE

Die weitreichenden Auswirkungen der Einführung von Instant Payments machen deutlich, dass es ratsam ist, die jeweiligen Compliance-Abteilungen frühzeitig mit in diesen Prozess einzubeziehen. Es sollte klargestellt werden, dass im Rahmen dieser Einführung nicht nur eine technische Anpassung benötigt wird. Zudem sollten funktionsübergreifende Teams aus den Bereichen Risk, Legal, Compliance, Kundenberatung, Produktmanagement, Operations und IT zusammengestellt werden, damit eine erfolgreiche Umsetzung aller Teilaspekte einer vollständigen Compliance- und Risikoüberlegung bis zum Sommer 2024 gesichert ist.

EINE ANSPRUCHSVOLLE HERAUSFORDERUNG

Bankenseitig wird sich der Aufwand für Transaktionsprüfungen im Instant Payments-Bereich tendenziell künftig von Operations hin zu Compliance verlagern. Zudem werden andere Mitarbeiterqualifikationen in den Vordergrund treten. Es werden beispielsweise vermehrt Data Scientists zur Verbesserung der automatisierten Prüfungen und die damit verbundene Reduzierung falscher Warnmeldungen gebraucht – vor allem wenn diese unter Anwendung von künstlicher Intelligenz erfolgen. Davon werden letztendlich alle Transaktionsarten profitieren.

Obwohl die Einführung von Instant Payments besonders für den Compliance-Bereich zunächst eine grosse Herausforderung darstellt und zusätzlich – zumindest temporär – erhöhte Kapazitäten beanspruchen wird, ist eine Implementierung entsprechender Prozesse mit einem hohen Mehrwert für den Kunden verbunden und wird sich gerade im Hinblick auf ein innovatives Produktangebot auszahlen. Mit effizienten und wirksamen Compliance-Prozessen kann zudem langfristig eine erfolgreiche Positionierung der etablierten Banken gegenüber Neobanken und Fintechs erfolgen.

AUTOREN:

Wesselin Kruschev, Managing Principal

Sarah Kimmel, Principal Consultant

Gregor von Bergen, Principal Consultant

KONTAKT:

Dr. Ingo Rauser, Partner

T +41 44 434 35 15

M +41 79 203 58 85

E ingo.rauser@capco.com

WWW.CAPCO.COM

CAPCO
a wipro company