1

15. Februar 2025
Fritz Knapp Verlag
36. Jahrgang
ISSN 0937-597 X
D 25079

KARTEN
cards | cartes

ZEITSCHRIFT FÜR ZAHLUNGSVERKEHR UND PAYMENTS

Digitaler Sonderdruck

Verbraucherschutz als Erfolgsfaktor für Echtzeitzahlungen

Von Jens Dauner

EUROPA IN DER ECHTZEITWELT

Foto: AdobeStock / Untamed

Verbraucherschutz als Erfolgsfaktor für Echtzeitzahlungen

Von Jens Dauner

Foto: AdobeStock/kyo

Bei der Nutzung von Echtzeit-Überweisungen hat Deutschland noch Nachholbedarf. Und dies liegt nicht zuletzt an den Sicherheitsbedenken der Verbraucher, sagt Jens Dauner. Damit Instant Payments zum Erfolg werden, gilt es deshalb, die Betrugsprävention zu verbessern, vor allem mithilfe von KI, aber auch mit einem Echtzeit-Austausch mit Kunden bei verdächtigen Transaktionen. Zudem wird die Frage nach der Haftung im Betrugsfall zu einem entscheidenden Faktor für das Vertrauen der Verbraucher. Red.

Echtzeitüberweisungen, seit dem 9. Januar verpflichtend gebührenfrei in der EU, gelten als Meilenstein im Zahlungsverkehr. Doch mit der Geschwindigkeit steigt auch das Betrugsrisiko – ein Thema, das durch die geplante PSD3-Verordnung sogar noch stärker in den Fokus rückt. Neben technologischem Fortschritt fordert die Regulierung auch eine intensivere Haftung und Betrugsprävention von Banken.

Weltweit sind Echtzeitüberweisungen (Instant Payments) auf dem Vormarsch, gelten bereits als „new normal" im Finanzsektor. Die Vorteile liegen auf der Hand: Echtzeitüberweisungen zeichnen sich im Vergleich zu herkömmlichen Zahlungsmethoden durch Schnelligkeit und Flexibilität aus. Das macht sie sowohl für Banken als auch für Verbraucher äußerst attraktiv. Die Corona-Pandemie beschleunigte den Einsatz der Technologie, die einen sekundenschnellen Zahlungsverkehr ermöglicht. Seither sind die Nutzung und Akzeptanz von Echtzeitüberweisungen weltweit gestiegen. Doch die aktuelle Debatte zeigt: Besonders in Deutschland gibt es Nachholbedarf.

Haftung im Betrugsfall als Erfolgsfaktor

Während technologische Fortschritte wie künstliche Intelligenz vielversprechende Lösungen für Betrugserkennung bieten, wird die Frage, wer im Falle von Betrug die Haftung trägt, zunehmend zu einem entscheidenden Faktor für den Erfolg der innovativen Zahlungsart und das Vertrauen der Verbraucher.

Eine Umfrage von Fico im November 2024 zeigt die aktuelle Zurückhaltung: 83 Prozent der deutschen Verbraucher haben zwar bereits Sofortzahlungen durchgeführt, doch nur 17 Prozent planen eine intensivere Nutzung im neuen Jahr. Damit hinkt Deutschland im internationalen Vergleich hinterher. Während global 22 Prozent der Nutzer mehr als zehn RTP-Transaktionen pro Monat durchführen, sind es in Deutschland lediglich 4 Prozent.

Die Politik bemüht sich, die Kluft zu schließen. Die EU-Verordnung für Echtzeitüberweisungen aus dem Jahr 2023 soll die Nutzung dieser Zahlungsart fördern. Denn deren Entwicklung ist nicht nur eine Antwort auf technologische Innovationen, sondern auch ein bedeutender Schritt, um die Wettbewerbsfähigkeit Deutschlands und Europas im globalen Finanzmarkt zu sichern. Der weltweite Anstieg der Nutzung von Echtzeitüberweisungen – im Jahr 2023 verzeichnete man eine Zunahme von 42,2 Prozent im Jahresvergleich – unterstreicht, wie wichtig es ist, den europäischen Markt auf den neuesten Stand der globalen Entwicklungen zu bringen.

Die im vergangenen Jahr verabschiedete EU-Verordnung für Echtzeitüberweisungen verpflichtet Zahlungsdienstleister, ab dem 9. Januar 2025 Echtzeitüberweisungen zu empfangen und bis Oktober 2025 auch zu versenden. Mit der Einführung der Kostenparität zwischen Sofortzahlungen und

Foto: FICO

Jens Dauner, Vice President & Managing Director Continental Europe, Fair Isaac Deutschland GmbH (FICO), Darmstadt

herkömmlichen Sepa-Überweisungen wird ein weiterer Schritt in Richtung breiterer Akzeptanz unternommen. Zudem soll die Einführung der Verifizierung des Zahlungsempfängers (Verification of Payee) Sicherheitsbedenken reduzieren.

Zu hohe Risiken für Verbraucher bei Echtzeitüberweisungen

Doch wie sicher sind Echtzeitüberweisungen wirklich? Was können Banken tun, um diese Zahlungsmethode noch attraktiver zu machen? Ein aktueller Fall aus Neustadt zeigt, wie kritisch Sicherheitsmaßnahmen bei Echtzeitüberweisungen sind: Ein Ehepaar überwies 6 000 Euro nach einer gefälschten SMS und konnte die Transaktion trotz schnellem Eingreifen nicht mehr stoppen. Das Ehepaar klagte gegen die absendende Bank, doch das Gericht entschied zugunsten des Finanzdienstleisters. Dabei wurde betont, dass alle vorgeschriebenen Sicherheitsvorkehrungen im Online-Banking, wie die Nutzung von Login- und TAN-Daten, ordnungsgemäß umgesetzt wurden. Das Urteil zeigt auf, wie hoch das Risiko für Privatpersonen weiterhin ist, und stellt eine der größten Herausforderungen bei der Entwicklung dieser Zahlungsart dar.

Für Banken bedeutet das: Sie müssen sich zunehmend mit der Frage auseinandersetzen, wie sie proaktive Maßnahmen zur Bekämpfung von Betrug entwickeln können. Verifizierungs-Apps und die Einführung von Kostenparität allein werden hier zukünftig nicht ausreichen. Es braucht neue, innovative Strategien, um den Sicherheitsstandards gerecht zu werden und das Vertrauen der Kunden zu gewinnen.

Steigende Zahl von Betrugsfällen

Im Jahr 2023 stieg die Zahl der Verbraucher, die ihre Banken über Betrugsfälle im Zusammenhang mit Echtzeitüberweisungen informierten. Gleichzeitig zeigte sich, dass viele deutsche Verbraucher immer noch Zweifel an der Sicherheit von Echtzeitüberweisungen hegen. Nur 43 Prozent sind der Ansicht, dass Banken ausreichend Aufklärungsarbeit leisten, um ihre Kunden über mögliche Betrugsmaschen zu informieren – deutlich weniger als im weltweiten Durchschnitt von 59 Prozent (aktuelle Fico-Studie). Wichtige Treiber dieser Entwicklung sind vorausgegangene Schäden, die durch Echtzeitüberweisungen entstanden sind, und ein wachsendes Bewusstsein für Internetbetrugsformen im Allgemeinen und die damit einhergehenden Konsequenzen.

Ein Beispiel, das diesen Trend bestätigt: 63 Prozent der deutschen Verbraucher gaben an, schon einmal eine SMS, eine E-Mail oder einen Anruf erhalten zu haben, von denen sie glaubten, dass es sich um einen Betrug handeln könnte. Gleichzeitig geben nur 27 Prozent an, dass Freunde oder Familienangehörige Opfer eines solchen Betrugs geworden sind. Dies deutet darauf hin, dass Verbraucher zunehmend vorsichtiger werden. 61 Prozent sehen sich selbst als verantwortlich, wenn sie auf einen Internetbetrug hereinfallen. Allerdings sind die Deutschen auch der Meinung, dass ein Teil der Schuld bei den Banken zu suchen ist: 14 Prozent sind der Meinung, dass die absendende Bank verantwortlich ist, 13 Prozent sehen die empfangende Bank in der Pflicht

Die steigende Zahl von Betrugsfällen, insbesondere solche mit hohen Schäden von über 10 000 Euro, fordert von den Banken eine verstärkte Auseinandersetzung mit Sicherheitsvorkehrungen und Schutzmechanismen. Denn auch wenn die meisten Verluste in Deutschland meist unter 500 Euro liegen, können diese für die betroffenen Verbraucher verheerend sein. Die Folge: Kunden möchten zunehmend, dass Banken im Falle eines Betrugs eine vollständige Rückerstattung oder Entschädigung leisten (65 Prozent, Fico-Studie).

Großbritannien: Geteilte Verantwortung zwischen Banken

Im Vereinigten Königreich haben Banken ihre Kunden bereits seit geraumer Zeit freiwillig im Falle von Betrügereien entschädigt. Im Jahr 2024 entschloss sich die britische Regulierungsbehörde für Zahlungssysteme jedoch, diese Entschädigung weitgehend verbindlich vorzuschreiben. Dieser Schritt unterstreicht die Überzeugung, dass Banken technisch in der Lage sind, betrügerische Transaktionen zu erkennen, wenn sie entsprechend motiviert sind. Der Politikwechsel stellt einen bedeutenden Fortschritt für die Verbraucher dar, die nun unabhängig von den Umständen umfassenden Schutz vor Finanzbetrug genießen – es sei denn, ihnen wird eine Mitschuld nachgewiesen.

Mit der Verordnung im Vereinigten Königreich wurde auch eine geteilte Verantwortung zwischen den Banken auf beiden Seiten der betrügerischen Transaktionen eingeführt. Dieser Schritt zielt darauf ab, ein zentrales Problem zu lösen: Viele Finanzinstitute waren bislang nicht ausreichend proaktiv darin, potenzielle betrügerische Geldkuriere während und nach dem Onboarding-Prozess zu identifizieren. Zuvor fehlte es den Banken, die betrügerische Überweisungen empfingen, an der Motivation, ihre Sicherheitsmaßnahmen zu verstärken, da es nicht ihre eigenen Kunden waren, die das Geld verloren.

PSD3 mit Fokus auf Betrugsprävention

Die dritte Zahlungsdiensterichtlinie der Europäischen Kommission (PSD3), die in der ersten Hälfte des Jahres 2026 veröffentlicht werden soll, geht in diesen beiden Bereichen zwar nicht so weit wie die britische Regelung, doch angesichts der Komplexität des multinationalen Rahmens schreitet die EU-Verordnung insgesamt langsamer voran. Für die Verbraucher ist jedoch positiv, dass die Betrugsprävention einen klaren Schwerpunkt der erweiterten Vorschriften bildet, insbesondere in Bezug auf die Stärkung der Verbraucherrechte.

Neben den Verbesserungen der SCA-Protokolle und der Ausweitung des Programms zur Bestätigung des Zahlungsempfängers ergeben sich aus der Perspektive der Zahlungsdienstleistungsanbieter folgende wesentliche Erkenntnisse:

1. Verlagerung der Haftung: Die neue Verordnung erweitert die Verantwortlichkeit bei Zahlungsdiensten, indem sie den Zahlungsdienstleistern die Pflicht auferlegt, bestimmte Sorgfaltspflichten zu erfüllen. Versäumt es ein Zahlungsdienstleister beispielsweise, seine Kunden über Diskrepanzen zwischen Kontokennungen und Empfängernamen bei Überweisungen zu informieren, so ist er für alle daraus resultierenden Verluste finanziell verantwortlich. Diese Verantwortung gilt auch für die empfangenden Zahlungsdienstleister, die den versendenden Dienstleister ent-

schädigen müssen, falls sie für schuldig befunden werden.

2. Robuste Betrugsüberwachung: Die PSD3-Gesetzgebung stärkt die Betrugsprävention durch einen verbesserten Datenaustausch zwischen Finanzinstituten. Sie definiert klare Anforderungen für die Haftung bei Betrug, Meldeprotokolle und Programme zur Sensibilisierung der Kunden. Zahlungsverkehrsdienstleister können verschiedene Datenpunkte austauschen, wie etwa den Kundenstandort, den Transaktionszeitpunkt, Geräteinformationen, Ausgabenmuster und Händlerinformationen, um Betrugsmuster besser zu erkennen und die Täter zu identifizieren.

Das Regelwerk legt zudem einen Fokus auf die Verbesserung der Verbraucheraufklärung über potenzielle Betrugsrisiken, unterstützt durch gemeinsame Anstrengungen der Branche. Der zweite Punkt stellt einen bedeutenden Schritt in die richtige Richtung dar – denn nun steht die britische Regulierungsbehörde vor der Frage, wie sie eine stärkere branchenübergreifende Zusammenarbeit fördern kann, insbesondere unter Einbeziehung von Bigtechs und Social-Media-Plattformen, die in vielen Betrugsfällen eine Rolle spielen.

Es gibt auch erste Anzeichen für zukünftige Entwicklungen, wie etwa eine Verpflichtung für Zahlungsdienstleister, Aufklärungsmaßnahmen durchzuführen, um sowohl Kunden als auch Mitarbeiter für Zahlungsrisiken zu sensibilisieren (das Vereinigte Königreich macht maßgeschneiderte Betrugswarnungen und Aufklärungsmaßnahmen in Echtzeit zur Bedingung). Zudem gibt es eine „Aufforderung" an Zahlungsdienstleister, ihre Bemühungen zur Überwachung des eingehenden Datenverkehrs zu verstärken.

Die neue PSD3-Verordnung ist ein wichtiger erster Schritt, von dem zu erwarten ist, dass er sich im Laufe der Zeit weiterentwickelt. Mit zunehmender Akzeptanz wird sie voraussichtlich weiter ausgebaut und angepasst, um den sich wandelnden Anforderungen des Zahlungsmarkts gerecht zu werden.

KI-basierte Verhaltensprofile

Um Betrug von vornherein zu verhindern, sollten Banken zunehmend auf Automatisierung und KI-gestützte Betrugsabwehr setzen. Machine-Learning-Algorithmen analysieren Transaktionsmuster in Echtzeit und erkennen Abweichungen, bevor Schaden entsteht. Die Algorithmen werden mit großen Mengen historischer Transaktionsdaten trainiert und lernen, was für einen einzelnen Kunden oder eine Kundengruppe „normal" ist. Anhand erstellter Verhaltensprofile lassen sich typische Zahlungsgewohnheiten wie zum Beispiel übliche Zahlungsbeträge, Frequenzen, verwendete Geräte und geografische Standorte identifizieren. So können untypische oder verdächtige Transaktionen schnell erkannt werden. Sobald eine solche Abweichung auftritt, wird die Transaktion entweder automatisch überprüft oder im Zweifelsfall blockiert.

Besonders bei Echtzeitüberweisungen, bei denen Transaktionen sofort abgeschlossen werden, kann dieses Verfahren das Risiko erheblich verringern. Zudem ermöglicht die kontinuierliche Anpassung der Modelle an neu auftretende Betrugsmuster, dass diese Technologien stets effektiv bleiben und auch auf sich ständig verändernde Betrugsstrategien reagieren können. So können Banken mithilfe von künstlicher Intelligenz den Betrügern immer einen kleinen, aber entscheidenden Schritt voraus sein.

Echtzeitaustausch mit dem Kunden

Auch die Kommunikation zwischen Banken und ihren Kunden muss deutlich verbessert werden. In Deutschland bevorzugen viele Verbraucher die Kontaktaufnahme über ihre Banking-App (37 Prozent, Fico-Studie), gefolgt von Telefon, SMS oder E-Mail. Eine zuverlässige und sichere Kommunikation innerhalb der App wird daher in Zukunft essenziell sein – Banken haben hier bereits mit einer schrittweisen Umstellung begonnen.

Dennoch müssen sie darauf vorbereitet sein, über verschiedene Kommunikationskanäle in Echtzeit und mit bidirektionalen Funktionen mit ihren Kunden zu kommunizieren. Nur so kann Erreichbarkeit gewährleistet werden, wenn ein Betrug vermutet oder erkannt wird. Dieser Echtzeitaustausch – unterstützt durch eine kontinuierliche Datenanalyse und Verhaltensprofilierung – reduziert die Wahrscheinlichkeit, dass ein Kunde eine Zahlung an einen Betrüger vornimmt. Auf diesem Weg können Banken das Risiko von Verlusten erheblich verringern und gleichzeitig das Vertrauen ihrer Kunden durch transparente und zeitnahe Kommunikation stärken.

Haftungsfrage immer wichtiger

Obwohl in Deutschland Fortschritte bei den Sicherheitsstandards für Echtzeitüberweisungen erzielt wurden, bleibt eine wichtige Frage unbeantwortet: Welche „Partei" trägt die Verantwortung? Im internationalen Vergleich wird sichtbar, dass die Verantwortung hierzulande immer noch stark auf den Verbraucher abgewälzt wird, was das Vertrauen in die neue Zahlungsmethode erschwert.

Im Vereinigten Königreich fordert die jüngste PSR-Verordnung im Rahmen des Contingent Reimbursement Model Code (CRMC), dass alle Banken ihren Kunden, die Opfer von Betrug geworden sind, eine Entschädigung gewähren. Zudem wird die Haftung zwischen dem absendenden und dem empfangenden Institut aufgeteilt, um durch eine verbesserte Überwachung von Geldkurieren die Spielräume für Betrüger zu verringern. In den USA haben die Regulierungsbehörden nach einer Anhörung im Senat erste Schritte in Richtung gesetzlicher Regelungen zur Rückerstattung von Kosten an Verbraucher unternommen, wobei zunächst Fälle im Fokus stehen, in denen es um die Nachahmung von Banken geht.

Gegenwärtig scheint der deutsche Kunde also noch immer der Hauptverlierer im Fall von Betrug zu sein, auch wenn dies durch die Schnelligkeit und Unwiderruflichkeit der Zahlungsmethode begünstigt wurde. Auch wenn technologische Fortschritte und regulatorische Maßnahmen den Weg für die sichere Nutzung von Echtzeitüberweisungen ebnen, wird die Frage der Verantwortung eine immer wichtigere Rolle spielen. Denn Echtzeitüberweisungen können nur dann als Revolution gelten, wenn Banken ihrer Verantwortung gerecht werden und die Betrugsbekämpfung aktiv gestalten. Durch innovative Technologien und klare Haftungsregeln müssen Banken und Politik gemeinsam einen sicheren Rahmen schaffen, um das Vertrauen der Verbraucher zu stärken. Sonst riskieren sie, die Chancen dieser Technologie zu verspielen. ■