

Im zukünftigen Recht der Zahlungsdienste werden Zahlungsinstitute in verstärktem Umfang für Social Engineering haften müssen.



AUTOR

Prof. Dr. Stefan Werner, RA/FAStR, ist Banksyndikus bei der Commerzbank AG und Honorarprofessor für Bankrecht an der Universität Göttingen. Der Schwerpunkt seiner Tätigkeit liegt im Bereich des Rechts der Zahlungsdienste.

Social Engineering im Zahlungsverkehr: mehr Kontrollpflichten zulasten der Zahlungsdienstleister

Im Zahlungsverkehr galt bisher der Grundsatz der Trennung von Valuta- und Deckungsverhältnis. Nur unter engen Voraussetzungen konnte das Zahlungsinstitut ausnahmsweise nach der Rechtsprechung verpflichtet sein, den Kontoinhaber vor der Ausführung eines Zahlungsauftrags zu warnen, wenn sich ein Missbrauch im Valutaverhältnis quasi aufdrängt. Allerdings führten die Fälle des Social Engineering, in denen außerhalb der Sphäre des kontoführenden Zahlungsdienstleisters Kunden dazu veranlasst werden, aufgrund einer Täuschung Zahlungsaufträge zugunsten unberechtigter Zahlungsempfänger zu erteilen, zu der Frage, ob die an der Zahlung beteiligten Zahlungsinstitute nicht verpflichtet sein können, aufgrund ihrer Kontrollmöglichkeiten Zahlungsvorgänge auf „Fraud“ zu überprüfen, um ihre Kunden ggf. zu warnen. Ausgangspunkt solcher Überlegungen waren die Chief-Executive-Officer-(CEO-) und Chief-Financial-Officer-(CFO-) Fälle, aber auch die Konstellationen des „Enkeltricks“. Wie aktuelle Gesetzesvorhaben zeigen, neigt der EU-Gesetzgeber dazu, den Zahlungsinstituten entsprechende Kontrollpflichten und teilweise auch die daraus resultierenden Risiken aufzuerlegen:

Einen ersten Schritt stellt der durch die Europäische Verordnung zur Echtzeitüberweisung (VO (EU) 2024/886, ABIEU vom 19.3.2024, L 2024/886) mit Wirkung zum 9.10.2025 einzuführende International-Bank-Account-Number-(IBAN-)Empfängervergleich dar, aufgrund dessen das erstbeauftragte Institute einen Vergleich zwischen der Angabe der IBAN und dem Empfänger veranlassen muss. Zwar kann dieses Institut den Vergleich nicht selbst durchführen, muss diesen aber beim Empfängerinstitut veranlassen und hat gegenüber dem Auftraggeber für die Richtigkeit des Prüfungsergebnisses einzustehen. Dem Auftraggeber muss das Ergebnis dieser Überprüfung vor der Autorisierung des Zahlungsauftrags mitgeteilt werden, damit er auch im Falle eine Diskrepanz entscheiden kann, ob der Auftrag gleichwohl ausgeführt werden soll. Auch wenn bei diesem IBAN-Empfängervergleich u. a. verhindert werden soll, dass der Zahler versehentlich an einen fal-

schen Empfänger zahlt, kann er gleichfalls der Verhinderung betrügerisch veranlasster Zahlungen dienen, denn es dürfte i. d. R. für den Auftraggeber ein Warnsignal sein, wenn die IBAN nicht zu dem angegebenen Empfänger gehört.

Einen Schritt weiter geht der Entwurf der Payment Services Regulation (PSR-E, COM(2023) 367 final), der in Art. 59 den Fall erfasst, dass ein Dritter unter missbräuchlicher Nutzung des Namens sowie einer E-Mail-Adresse oder einer Telefonnummer des Zahlungsdienstleisters einen Verbraucher als Zahlungsdienstnutzer zur Autorisierung betrügerischer Zahlungsvorgänge veranlasst. Nach dieser Regelung muss der Zahlungsdienstleister, auch wenn ihn keine Pflichtverletzung trifft, dem Zahlungsdienstnutzer den Zahlungsbetrag erstatten. Nur wenn der Zahlungsdienstleister nachweisen kann, dass der Zahlungsdienstnutzer betrügerisch oder wenigstens grob fahrlässig gehandelt hat, ist er berechtigt, die Erstattung abzulehnen. Allerdings dürfte die Haftung nicht nur auf diese Fälle begrenzt werden. Zahlungsdienstleister werden, wollen sie solche Fälle verhindern, kaum Kontrollmaßnahmen installieren können, die nur diese Fälle erfassen. Werden dann aber auch andere Fälle des Social Engineering durch die „Filter“ der Zahlungsdienstleister entdeckt, liegt es nahe, daraus eine allgemeine Warnpflicht abzuleiten. Dies dürfte auch mit der sich aus Art. 84 Abs. 1 PSR-E ergebenden Verpflichtung korrespondieren, dass Zahlungsdienstleister ihre Kunden vor neuen Formen von Zahlungsbetrug warnen sollen.

Im Zusammenhang mit den Betrugsfällen des Social Engineering ist auf der Ebene des europäischen Gesetzgebers gegenüber den tradierten Grundsätzen im Zahlungsverkehr ein Paradigmenwechsel dahingehend festzustellen, dass die Trennung von Deckungs- und Valutaverhältnis bedauerlicherweise in immer weiteren Umfang aufgegeben werden soll und die Zahlungsdienstleister auch das Valutaverhältnis bei ihrer Kontrolle mit berücksichtigen müssen.