

TE OGH 2024/8/28 7Ob95/24g

JUSLINE Entscheidung

🕒 Veröffentlicht am 28.08.2024

Kopf

Der Oberste Gerichtshof hat als Revisionsgericht durch die Senatspräsidentin Dr. Solé als Vorsitzende und die Hofrätinnen und Hofräte Mag. Dr. Wurdinger, Mag. Malesich, Dr. Weber und Mag. Fitz als weitere Richter in der Rechtssache der klagenden Partei K*, vertreten durch Dr. Leopold Boyer, Mag. Daniela Neuhuber, Mag. Leopold Boyer, Rechtsanwälte in Gänserndorf, gegen die beklagte Partei S* Aktiengesellschaft, *, vertreten durch Hosp, Hegen & Partner Rechtsanwälte in Salzburg, wegen Löschung in eventu 27.650 EUR, über die Revision der klagenden Partei gegen das Urteil des Oberlandesgerichts Linz als Berufungsgericht vom 28. März 2024, GZ 11 R 7/24i-47, womit das Urteil des Landesgerichts Salzburg vom 29. Dezember 2023, GZ 14 Cg 54/23p-43, bestätigt wurde, den

Beschluss

gefasst:

Spruch

Die Revision wird zurückgewiesen.

Die klagende Partei ist schuldig, der beklagten Partei die mit 2.166,90 EUR (darin enthalten 361,15 EUR USt) bestimmten Kosten des Revisionsverfahrens binnen 14 Tagen zu ersetzen.

Text

Begründung:

[1] Der Kläger ist Kontoinhaber eines bei der Beklagten geführten Girokontos und verfügt über Internetbanking. Die Beklagte bietet ihren Internetbanking-Kunden ein Zwei-Faktor-Authentifizierungs-System an, das mit jeweils zwei der drei möglichen Faktoren Wissen, Besitz oder Inhärenz arbeitet, um Zahlungsvorgänge zu autorisieren. Darüber hinaus gibt es eine automatisierte Transaktionsüberwachung, die aufgrund von Algorithmen erkennt, wenn eine – auch ordnungsgemäß autorisierte Zahlungsanweisung – vom sonstigen Kundenverhalten abweicht. Der Kläger erhielt vor dem verfahrensgegenständlichen Vorfall eine Warnung der Beklagten vor betrügerischen „Phishing“-Nachrichten.

[2] Am Vorfalstag klickte der Kläger auf einen Link in einer – als Nachricht eines Paketzustellers getarnten – SMS-Nachricht und gab dort einige persönliche Daten sowie seine Verfügernummer für das Internetbanking bei der Beklagten an. In der Folge hob er insgesamt 7.500 EUR bar von seinem Konto ab und tätigte verschiedene Erledigungen. Noch währenddessen wurde der Kläger von einer ihm unbekannten Nummer angerufen. Es wurde ihm mitgeteilt, dass auf das Konto des Klägers zugegriffen werde. Der Kläger verschob das Telefonat zuerst, bis er zu Hause war. Dort rief er die aufscheinende Nummer zur Kontrolle zurück. Dabei wurde über Tonband ein Geldinstitut angegeben, bei dem der Kläger kein Konto hat. Am selben Abend wurde der Kläger von einem unbekannten Täter mit einer deutschen Telefonnummer angerufen. Der Anrufer ersuchte den Kläger, sein Internetbanking einzusehen. Zwischenzeitig hatte der unbekannte Täter über einen Desktop die Web-Anwendung des Internetbankings des Klägers

gestartet und die Verfügernummer des Klägers eingegeben. Der Kläger öffnete daraufhin die App auf seinem Smartphone und bestätigte durch die Eingabe seiner PIN neben seinem eigenen Login über die Kontroll-App auch den Login des unbekannten Täters über die Web-Version. So gelang es dem unbekannten Täter, in das Internetbanking des Klägers einzusteigen. Dieser teilte dem Kläger mit, er müsse nun seinen Anweisungen folgen und verschiedene Dinge bestätigen, damit das Geld – das nach den Angaben des unbekannten Täters vom Konto des Klägers widerrechtlich abgebucht werden sollte – zurückgeholt werden könne. Der unbekannte Täter bereitete eine Auslandsüberweisung in Höhe von 20.000 EUR vor, die der Kläger einsehen konnte und mit seinen Daten freigab. Obwohl diese Überweisung damit ordnungsgemäß autorisiert war, stoppte das „Fraud-Transaction-Monitoring“ Programm der Beklagten die Überweisung, weil Betrag und Empfängerkonto vom üblichen Buchungsverhalten des Klägers abwich. Anschließend übermittelte der unbekannte Täter dem Kläger vier weitere bereits ausgefüllte Überweisungsaufträge über zweimal 9.000 EUR, 3.950 EUR und 5.700 EUR auf dasselbe Konto. Der Kläger gab alle diese Überweisungen ordnungsgemäß mit beiden Schritten seiner App frei. Er bemerkte im Zuge der Abbuchungsvorgänge, dass das Geld auf seinem Girokonto weniger und weniger wurde und Abbuchungen stattfanden, lies sich aber von dem unbekannten Täter beschwichtigen, dass dies dazu diene, Betrugsversuche zu „bearbeiten“ und sich sein Kontostand dann regulieren werde. Diese Überweisungen von insgesamt 27.650 EUR wurden vom „Fraud-Transaction-Monitoring“ der Beklagten nicht mehr gestoppt und ließen sich auch nicht mehr zurückholen.

[3] Der Kläger fordert von der Beklagten die Löschung der Kontobuchungen; in eventu, die Zahlung von 27.650 EUR. Er brachte – soweit im Revisionsverfahren noch relevant – vor, das Kontrollsystem der Beklagten hätte auch die weiteren Überweisungen als nicht gewollt erkennen müssen.

[4] Die Beklagte wendet – soweit im Revisionsverfahren noch relevant – ein, ihre Kontrollsysteme würden sämtliche gesetzlichen Vorgaben mehr als erfüllen und sie habe überdies den Kläger ausreichend vor Pishing gewarnt. Der Kläger habe selbst grob fahrlässig gehandelt.

[5] Das Erstgericht wies das Klagebegehren ab. Eine Haftung der Beklagten aufgrund §§ 67, 68 ZaDiG 2018 für nicht autorisierte Zahlungsvorgänge scheide aus, weil der Kläger alle seine Zahlungsaufträge im ordnungsgemäß ausgestalteten Zwei-Faktor-Authentifizierungs-System der Beklagten autorisiert habe. Auch allfällige zusätzliche Vorgaben der DelVO (EU) 2018/389 hätte die Beklagte mit der starken Kundenauthentifizierung und der zusätzlichen Transaktionsüberwachung erfüllt. Aus der in den AGB der Beklagten vorgesehenen Berechtigung, bei mittels Telekommunikation erteilten Aufträgen vor Ausführung eine Auftragsbestätigung einzuholen, sei für den Kläger nichts zu gewinnen. Es handle sich dabei um keine Verpflichtung, sondern vielmehr eine Absicherung, falls in einem konkreten Fall aufgrund einer notwendigen Überprüfung die Vorgaben des § 77 ZaDiG 2018 nicht erfüllt werden können. Diese Bestimmung würde die Beklagte im Übrigen dazu verpflichten, den Betrag am nächsten Geschäftstag gutzuschreiben, was die vom Kläger eingeforderten weiteren routinemäßigen Überprüfungsmaßnahmen konterkarieren würden. Dass das Transaktionsüberprüfungssystem der Beklagten funktioniere, zeige der Stopp der ersten Überweisung. Dass der Kläger am selben Tag noch eine Barabhebung von 7.500 EUR getätigt habe, lasse die darauffolgenden Überweisungen plausibel erscheinen. [5] Das Erstgericht wies das Klagebegehren ab. Eine Haftung der Beklagten aufgrund Paragraphen 67, 68, ZaDiG 2018 für nicht autorisierte Zahlungsvorgänge scheide aus, weil der Kläger alle seine Zahlungsaufträge im ordnungsgemäß ausgestalteten Zwei-Faktor-Authentifizierungs-System der Beklagten autorisiert habe. Auch allfällige zusätzliche Vorgaben der DelVO (EU) 2018/389 hätte die Beklagte mit der starken Kundenauthentifizierung und der zusätzlichen Transaktionsüberwachung erfüllt. Aus der in den AGB der Beklagten vorgesehenen Berechtigung, bei mittels Telekommunikation erteilten Aufträgen vor Ausführung eine Auftragsbestätigung einzuholen, sei für den Kläger nichts zu gewinnen. Es handle sich dabei um keine Verpflichtung, sondern vielmehr eine Absicherung, falls in einem konkreten Fall aufgrund einer notwendigen Überprüfung die Vorgaben des Paragraph 77, ZaDiG 2018 nicht erfüllt werden können. Diese Bestimmung würde die Beklagte im Übrigen dazu verpflichten, den Betrag am nächsten Geschäftstag gutzuschreiben, was die vom Kläger eingeforderten weiteren routinemäßigen Überprüfungsmaßnahmen konterkarieren würden. Dass das Transaktionsüberprüfungssystem der Beklagten funktioniere, zeige der Stopp der ersten Überweisung. Dass der Kläger am selben Tag noch eine Barabhebung von 7.500 EUR getätigt habe, lasse die darauffolgenden Überweisungen plausibel erscheinen.

[6] Das Berufungsgericht teilte die Ansicht des Erstgerichts, wonach der Beklagten keine Sorgfaltswidrigkeit zur Last liege und ergänzte, dass das Verhalten des Klägers als grob fahrlässig einzustufen sei, was eine – ohnehin nicht vorliegende – Sorgfaltswidrigkeit der Beklagten aber jedenfalls in den Hintergrund treten ließe.

[7] Es ließ die ordentliche Revision zu, weil der Oberste Gerichtshof zur Frage, ob trotz erfolgter starker Kundenauthentifizierung und erstmaliger Blockierung einer verdächtigen Überweisung ein Zahlungsdienstleister bei sodann wiederum persönlich vom Kunden aufgrund falscher Vorstellungen freigegebener Überweisungen diese zu stoppen und eine weitere Bestätigung einzuholen hätte, noch nicht Stellung nehmen musste, dies auch aufgrund der Vielzahl der zu erwartenden vergleichbaren Fälle.

Rechtliche Beurteilung

[8] Da der Kläger in seiner Revision das Vorliegen der Voraussetzungen des § 502 Abs 1 ZPO nicht zu begründen vermag, ist die Revision entgegen dem – den Obersten Gerichtshof nicht bindenden (§ 508a Abs 1 ZPO) – Ausspruch des Berufungsgerichts nicht zulässig. Die Zurückweisung eines ordentlichen Rechtsmittels wegen Fehlens einer erheblichen Rechtsfrage kann sich auf die Ausführung der Zurückweisungsgründe beschränken (§ 510 Abs 3 ZPO): [8] Da der Kläger in seiner Revision das Vorliegen der Voraussetzungen des Paragraph 502, Absatz eins, ZPO nicht zu begründen vermag, ist die Revision entgegen dem – den Obersten Gerichtshof nicht bindenden (Paragraph 508 a, Absatz eins, ZPO) – Ausspruch des Berufungsgerichts nicht zulässig. Die Zurückweisung eines ordentlichen Rechtsmittels wegen Fehlens einer erheblichen Rechtsfrage kann sich auf die Ausführung der Zurückweisungsgründe beschränken (Paragraph 510, Absatz 3, ZPO):

[9] 1. Ein vom Berufungsgericht verneinter Mangel des erstinstanzlichen Verfahrens kann im Revisionsverfahren grundsätzlich nicht mehr geltend gemacht werden (RS0043919; RS0042963). Dieser Grundsatz kann auch nicht durch die Behauptung, das Berufungsverfahren sei – weil das Berufungsgericht der Mängelrüge nicht folgte – mangelhaft geblieben, umgangen werden (RS0042963 [T58]).

[10] 2. Der Kläger geht im Rahmen seines Rechtsmittels nunmehr selbst davon aus, dass es sich bei den Zahlungsaufträgen um von ihm autorisierte gehandelt hat. Eine Haftung gemäß §§ 67, 68 ZaDiG 2018 kommt damit keinesfalls in Betracht. [10] 2. Der Kläger geht im Rahmen seines Rechtsmittels nunmehr selbst davon aus, dass es sich bei den Zahlungsaufträgen um von ihm autorisierte gehandelt hat. Eine Haftung gemäß Paragraphen 67, 68, ZaDiG 2018 kommt damit keinesfalls in Betracht.

[11] 3. Der Kläger stützt sich auf die Verletzung – weiterer – vertraglicher Verpflichtungen der Beklagten, durch deren Erfüllung sie die von ihm in Auftrag gegebenen Zahlungen stoppen hätte können.

[12] 3.1. Der Umfang von Schutz- und Sorgfaltspflichten, wie etwa die Frage von Beratungs- und Aufklärungspflichten von Banken, ist grundsätzlich eine Frage des Einzelfalls. Gegenteiliges gilt nur dann, wenn eine grobe Fehlbeurteilung vorliegt, die im Interesse der Rechtssicherheit korrigiert werden müsste (RS0106373 [T4]). Der bloße Umstand, dass zu lösende Fragen in einer Vielzahl von Fällen auftreten mögen, bewirkt entgegen der Ansicht des Klägers noch nicht deren Erheblichkeit im Sinne des § 502 Abs 1 ZPO (RS0042816). Auch eine Vielzahl von Geschädigten ändert nichts daran, dass die Frage, wie weit Aufklärungspflichten gehen, dennoch auch dabei stets von den ganz konkreten Umständen des Einzelfalls abhängt (RS0106373 [T12]). [12] 3.1. Der Umfang von Schutz- und Sorgfaltspflichten, wie etwa die Frage von Beratungs- und Aufklärungspflichten von Banken, ist grundsätzlich eine Frage des Einzelfalls. Gegenteiliges gilt nur dann, wenn eine grobe Fehlbeurteilung vorliegt, die im Interesse der Rechtssicherheit korrigiert werden müsste (RS0106373 [T4]). Der bloße Umstand, dass zu lösende Fragen in einer Vielzahl von Fällen auftreten mögen, bewirkt entgegen der Ansicht des Klägers noch nicht deren Erheblichkeit im Sinne des Paragraph 502, Absatz eins, ZPO (RS0042816). Auch eine Vielzahl von Geschädigten ändert nichts daran, dass die Frage, wie weit Aufklärungspflichten gehen, dennoch auch dabei stets von den ganz konkreten Umständen des Einzelfalls abhängt (RS0106373 [T12]).

[13] 3.2. Wenn die Vorinstanzen im konkreten Einzelfall eine Verletzung dieser Schutz- und Sorgfaltspflichten durch die Beklagte – aufgrund der bestehenden Transaktionsüberwachung und der im Vorfeld getätigten Warnungen – verneint haben, so ist das nicht korrekturbedürftig.

[14] 3.3. Da die Feststellungen, welche Vorgehensweise im Bankwesen „üblich“ wäre und welche Buchungen das früher von der Beklagten benutzte Transaktionsüberwachungssystem gestoppt hätte, an dieser Beurteilung nichts ändern würden, liegen – entgegen der Ansicht des Klägers – auch keine sekundären Feststellungsmängel vor.

[15] 4. Im Übrigen stellt auch die – selbständig tragfähige – Hilfsbegründung des Berufungsgerichts, wonach – selbst ausgehend von einer Sorgfaltspflichtverletzung der Beklagten – das festgestellte Verhalten des Klägers diese derart in den Hintergrund drängen würde, dass es zur Gänze vernachlässigt werden könnte (vgl etwa RS0027202 [T12]), keine im Einzelfall aufzugreifende Fehlbeurteilung dar. [15] 4. Im Übrigen stellt auch die – selbständig tragfähige – Hilfsbegründung des Berufungsgerichts, wonach – selbst ausgehend von einer Sorgfaltspflichtverletzung der Beklagten – das festgestellte Verhalten des Klägers diese derart in den Hintergrund drängen würde, dass es zur Gänze vernachlässigt werden könnte vergleiche etwa RS0027202 [T12]), keine im Einzelfall aufzugreifende Fehlbeurteilung dar.

[16] 5. Dass ein betrügerischer Zahlungsvorgang gerade auch ein autorisierter Zahlungsvorgang sein kann, ist Grund für das zusätzliche Transaktionsüberwachungssystem der Beklagten, welches eine Überprüfung des bereits autorisierten Zahlungsvorgangs vornimmt. Der Anregung des Klägers auf Einleitung eines EuGH-Vorabentscheidungsverfahrens zur Frage des Zusammenspiels der Begriffe „nicht autorisierter“ und „betrügerischer“ Zahlungsvorgang in Art 2 DelVO (EU) 2018/389 ist damit nicht nahezutreten, weil keine Zweifel im Zusammenhang mit Fragen aus dem Unionsrecht aufkommen (RS0082949 [T16]). [16] 5. Dass ein betrügerischer Zahlungsvorgang gerade auch ein autorisierter Zahlungsvorgang sein kann, ist Grund für das zusätzliche Transaktionsüberwachungssystem der Beklagten, welches eine Überprüfung des bereits autorisierten Zahlungsvorgangs vornimmt. Der Anregung des Klägers auf Einleitung eines EuGH-Vorabentscheidungsverfahrens zur Frage des Zusammenspiels der Begriffe „nicht autorisierter“ und „betrügerischer“ Zahlungsvorgang in Artikel 2, DelVO (EU) 2018/389 ist damit nicht nahezutreten, weil keine Zweifel im Zusammenhang mit Fragen aus dem Unionsrecht aufkommen (RS0082949 [T16]).

[17] 6. Die Revision ist daher insgesamt mangels Vorliegens einer erheblichen Rechtsfrage zurückzuweisen.

[18] 7. Die Kostenentscheidung beruht auf §§ 50, 41 ZPO. Die Beklagte hat auf die Unzulässigkeit der Revision hingewiesen. [18] 7. Die Kostenentscheidung beruht auf Paragraphen 50, 41, ZPO. Die Beklagte hat auf die Unzulässigkeit der Revision hingewiesen.

Textnummer

E142341

European Case Law Identifier (ECLI)

ECLI:AT:OGH0002:2024:00700B00095.24G.0828.000

Im RIS seit

27.09.2024

Zuletzt aktualisiert am

28.04.2025

Quelle: Oberster Gerichtshof (und OLG, LG, BG) OGH, <http://www.ogh.gv.at>

© 2026 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at