TE OGH 2018/7/24 9Ob48/18a

JUSLINE Entscheidung

Veröffentlicht am 24.07.2018

Kopf

Der Oberste Gerichtshof hat als Revisionsgericht durch den Senatspräsidenten des Obersten Gerichtshofs Dr. Hopf als Vorsitzenden, die Hofrätinnen und Hofräte des Obersten Gerichtshofs Hon.-Prof. Dr. Dehn, Dr. Hargassner, Mag. Korn und Dr. Stefula in der Rechtssache der klagenden Parteien 1. Dr. B***** S***** und 2. Dr. V***** S*****, beide *****, beide vertreten durch Mag. Mathias Kapferer, Rechtsanwalt in Innsbruck, gegen die beklagte Partei T*****aktiengesellschaft *****, vertreten durch Dr. Erwin Markl, Rechtsanwalt in Innsbruck, wegen 12.880 EUR, über die Revision der klagenden Parteien gegen das Urteil des Landesgerichts Innsbruck als Berufungsgericht vom 26. Jänner 2018, GZ 2 R 193/17x-30, mit dem der Berufung der klagenden Parteien gegen das Urteil des Bezirksgerichts Innsbruck vom 20. Juni 2017, GZ 31 C 57/16w-26, nicht Folge gegeben wurde, in nichtöffentlicher Sitzung den

Beschluss

gefasst:

Spruch

Die Revision der klagenden Parteien wird zurückgewiesen.

Die klagenden Parteien sind schuldig, der beklagten Partei die mit 1.032,91 EUR (darin 172,15 EUR USt) bestimmten Kosten des Revisionsverfahrens binnen 14 Tagen zu ersetzen.

Begründung:

Rechtliche Beurteilung

Die ordentliche Revision wurde vom Berufungsgericht nachträglich (§ 508 Abs 3 ZPO) zugelassen, weil es für die nach § 44 Abs 2 ZaDiG erforderliche Abgrenzung zwischen leichter und grober Fahrlässigkeit beim Umgang mit Zahlungsinstrumenten keine Judikatur des Obersten Gerichtshofs gäbe. Auch wenn die Frage des Verschuldensgrads grundsätzlich nur nach den Umständen des Einzelfalls zu beurteilen sei, so mache die deutliche Zunahme elektronisch ausgelöster Zahlungsvorgänge und die damit einhergehende Zunahme von Phishing-Attacken diese Abgrenzung zu einer erheblichen Rechtsfrage im Sinne des § 502 Abs 1 ZPO. Dem schlossen sich die Revisionswerber zwecks Begründung der Zulässigkeit ihres Rechtsmittels nach § 502 Abs 1 ZPO an. Dem gegenüber bestritt die Revisionsgegnerin das Vorliegen einer erheblichen Rechtsfrage und beantragte die Zurückweisung der Revision der Kläger.

Der Oberste Gerichtshof ist bei der Prüfung der Zulässigkeit der Revision an den Ausspruch des Berufungsgerichts nach § 500 Abs 2 Z 3 ZPO nicht gebunden (§ 508a Abs 1 ZPO). Gegen das Urteil des Berufungsgerichts ist die Revision nach § 502 Abs 1 ZPO nur dann zulässig, wenn die Entscheidung von der Lösung einer erheblichen, in ihrer Bedeutung

über den Einzelfall hinausgehenden Rechtsfrage des materiellen Rechts oder des Verfahrensrechts abhängt. Dies ist hier nicht der Fall. Die Zurückweisung der ordentlichen Revision kann sich auf die Ausführung der Zurückweisungsgründe beschränken (§ 510 Abs 3 Satz 4 ZPO):

1. Mit 1. 6. 2018 ist das Zahlungsdienstegesetz 2018 (ZaDiG 2018), BGBl I 2018/17, in Kraft (§ 119 Abs 1 ZaDiG 2018) und mit Ablauf des 31. 5. 2018 das Zahlungsdienstgesetz – ZaDiG, BGBl I 2009/66, außer Kraft getreten (§ 120 ZaDiG 2018). Nach § 5 ABGB wirken Gesetze nicht zurück. Eine ausdrückliche Rückwirkungsanordnung (vgl RIS-Justiz RS0015520) sieht das ZaDiG 2018 nicht vor. Da auch der besondere Charakter der – für die Beurteilung des konkreten Falls relevanten – zwingenden Normen (vgl § 55 Abs 2 ZaDiG 2018) deren rückwirkende Anordnung auch nicht verlangt, ist der vor Inkrafttreten der neuen Bestimmungen endgültig abgeschlossene Sachverhalt nach dem ZaDiG, BGBl I 2009/66 idF BGBl I 2017/149 (in der Folge kurz ZaDiG), zu beurteilen (RIS-JustizRS0008715 [T7, T8 und T20]).

2. § 44 Abs 1 ZaDiG sieht eine grundsätzlich verschuldensunabhängige Haftung des Zahlungsdienstleisters für Zahlungsvorgänge vor, die vom Zahler nicht autorisiert waren. In diesen Fällen hat der Zahler gegenüber dem Zahlungsdienstleister einen Berichtigungs- oder Erstattungsanspruch.

Trifft den Kunden jedoch ein Verschulden am Missbrauch, wird er dem Zahlungsdienstleister nach Maßgabe des § 44 Abs 2 und 3 ZaDiG schadenersatzpflichtig. § 44 Abs 2 und 3 ZaDiG regeln die Haftung des Kunden zwingend und abschließend (RIS-Justiz RS0128542). Beruhen nicht autorisierte Zahlungsvorgänge auf der missbräuchlichen Verwendung eines Zahlungsinstruments, so ist der Zahler seinem Zahlungsdienstleister dann zum Ersatz des gesamten Schadens (begrenzt durch die Limits, die für das Konto und das Zahlungsinstrument vereinbart sind) verpflichtet, der diesem infolge des nicht autorisierten Zahlungsvorgangs entstanden ist, wenn er ihn in betrügerischer Absicht ermöglicht hat oder durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Pflichten gemäß § 36 ZaDiG (§ 44 Abs 2 Z 1 ZaDiG) oder einer oder mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments (§ 44 Abs 2 Z 2 ZaDiG) herbeigeführt hat. Im Fall einer bloß leicht fahrlässigen Verletzung dieser Sorgfaltspflichten ist die Haftung des Kunden – abweichend vom allgemeinen Schadenersatzrecht – auf einen Betrag von 150 EUR beschränkt (§ 44 Abs 2 ZaDiG).

Gemäß § 36 Abs 1 ZaDiG hat der Zahlungsdienstnutzer ua unmittelbar nach Erhalt des Zahlungsinstruments alle ihm zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale und das Zahlungsinstrument vor einem unbefugten Zugriff zu schützen. Außerdem muss der Kunde den Verlust, den Diebstahl oder die nicht autorisierte Nutzung eines Zahlungsinstruments unverzüglich anzeigen, sobald er davon Kenntnis hat (§ 36 Abs 2 ZaDiG). Zudem trifft den Zahlungsdienstnutzer eine entsprechende Rügeobliegenheit (§ 36 Abs 3 ZaDiG).

Im Fall des Mitverschuldens des Zahlungsdienstleisters kommt es zu einer Teilung des Schadens, für die insbesondere die in § 44 Abs 2 Satz 3 ZaDiG aufgezählten Zurechnungsgründe maßgeblich sind (10 Ob 102/15w Pkt 1.4.).

Somit kann der Zahler im Fall der schuldhaften Verletzung der ihn nach § 36 ZaDiG treffenden Sorgfaltspflichten im Ergebnis den nach § 44 Abs 1 ZaDiG bestehenden Berichtigungs- und Erstattungsanspruch (allenfalls ganz) verlieren. Der Zahlungsdienstleister kann dann die Belastung des Kontos des Zahlers ganz oder teilweise auf den ihm nach § 44 Abs 2 ZaDiG zustehenden Schadenersatzanspruch stützen, der insofern den bei nicht autorisierten Zahlungsvorgängen fehlenden Aufwandersatzanspruch nach § 1014 ABGB ganz oder teilweise ersetzt (10 Ob 102/15w Pkt 1.5.).

3. Zutreffend gehen die Vorinstanzen und die Parteien davon aus, dass die Fragen, ob und in welchem Ausmaß der Zahler fahrlässig gehandelt hat, nach den allgemeinen Regeln des Schadenersatzrechts zu beurteilen sind (Haghofer in Weilinger, ZaDiG § 44 Rz 27; Leixner, ZaDiG² § 44 Rz 2; Harrich, ZaDiG 300; ErläutRV 207 BlgNR 24. GP 47 f; Erwägungsgrund 33 der Zahlungsdienste-Richtlinie RL 2007/64/EG; 10 Ob 102/15w Pkt 4.1.). Es sind daher auch für die Prüfung, ob das sorgfaltswidrige Handeln des Zahlers, das den nicht autorisierten Zahlungsvorgang ausgelöst hat, als leicht oder grob fahrlässig anzusehen ist, die von der Rechtsprechung für diese Abgrenzung entwickelten Kriterien des allgemeinen Schadenersatzrechts heranzuziehen. Die Beurteilung des Verschuldensgrades kann aber regelmäßig nur aufgrund der konkreten Umstände des Einzelfalls beurteilt werden (RIS-Justiz RS0087606 [T19]; RS0105331 [T6]). Eine gravierende Fehlbeurteilung der Vorinstanzen, die im Interesse der Rechtssicherheit zu korrigieren wäre, liegt nicht vor. Auch schließen die unterschiedlich denkbaren Sorgfaltspflichtverletzungen eines Zahlers allgemeine, über den Anlassfall hinausgehende Aussagen des Obersten Gerichtshofs aus.

4.1. Nach der Rechtsprechung handelt grob fahrlässig, wer im täglichen Leben die erforderliche Sorgfalt gröblich, in hohem Grad, aus Unbekümmertheit oder Leichtfertigkeit außer Acht lässt, wer nicht beachtet, was unter den

gegebenen Umständen jedem einleuchten musste. Grobe Fahrlässigkeit ist somit bei schlechthin unentschuldbaren Pflichtverletzungen gegeben, die das gewöhnliche Maß an alltäglich vorkommenden, nie ganz vermeidbaren Fahrlässigkeitshandlungen des täglichen Lebens ganz erheblich übersteigen. Grobe Fahrlässigkeit erfordert das Vorliegen eines objektiv besonders schweren Sorgfaltsverstoßes, der bei Würdigung aller Umstände des konkreten Falles auch subjektiv schwerstens vorzuwerfen ist. Dabei muss der Schaden als wahrscheinlich vorhersehbar gewesen sein (RIS-Justiz RS0030303; RS0031127; RS0030644; RS0030272 ua). Diese Voraussetzungen sind im Einzelfall mit Bedachtnahme auf die persönlichen Verhältnisse des betreffenden Kunden und die allgemeinen Lebensgewohnheiten der Zahlungsdienstnutzer zu beurteilen (Haghofer in Weilinger, ZaDiG § 44 Rz 27).

Ausgehend vom folgenden, für den Obersten Gerichtshof bindend festgestellten Sachverhalt, ist die übereinstimmende Beurteilung der Vorinstanzen, die das sorgfaltswidrige Verhalten des Erstklägers als grob fahrlässig qualifiziert haben, jedenfalls vertretbar.

4.2. Die Kläger sind Verbraucher und gemeinsame Inhaber (mit jeweiliger Einzelverfügungsbefugnis) des beim beklagten Kreditinstitut eingerichteten Kontos. Seit 2005 nehmen sie am Electronic Banking der Beklagten teil, und zwar seit November 2013 in Form von der Beklagten zur Verfügung gestellten TAC-SMS-Codes. Die TAC-Codes der Beklagten sind vierstellig und werden durch Übermittlung einer TAC-SMS zur Zeichnung der vom Kunden gewünschten Überweisung im Zuge des Überweisungsvorgangs per netbanking auf das Handy des Kunden versendet. Diese TAC-SMS, die vom Server der Beklagten versendet werden, haben üblicherweise folgenden Inhalt: „Prüfen Sie die letzten 11 Stellen der IBAN und Betragssumme“. Diesem Hinweis folgen dann die letzten 11 Stellen der IBAN, der Überweisungsbetrag in Euro sowie der vierstellige TAC-Code, welcher ausdrücklich als „TAC“ bezeichnet wird.

Die Beklagte übermittelt immer wieder Warnungen an ihre Kunden über aktuell im Internet im Umlauf befindliche Trojaner und Phishing-Mails. Unter anderem enthielten diese Warnungen der Beklagten ausdrücklich folgenden Inhalt: „Prüfen Sie IMMER die Inhalte ihrer TAC-SMS, bevor sie mit der TAC zeichnen – also bei einer Überweisung die Empfänger-IBAN und vor allem den Betrag !!!!“ Auch der Erstkläger hat derartige Warnungen der Beklagten erhalten und auch gelesen.

Am 12. 10. 2015 wurde der Erstkläger auf seinem Handy, dessen Telefonnummer im netbanking der Beklagten hinterlegt ist, von einer ihm unbekannten Telefonnummer von einer akzentfrei Deutsch sprechenden Frau angerufen. Diese gab sich als Angestellte der Beklagten aus und forderte ihn auf, ihr aufgrund einer notwendigen Datenaktualisierung den ihm soeben per SMS übermittelten Code bekannt zu geben. Während des laufenden Anrufs öffnete der Erstkläger das ihm soeben übermittelte TAC-SMS und gab der Anruferin den darin enthaltenen TAC-Code bekannt. Das an den Erstkläger im Zuge dieses Telefonats übermittelte TAC-SMS hatte den gleichen Inhalt, wie auch die sonst üblichen TAC-SMS der Beklagten. Insbesondere enthielt es die letzten 11 Stellen der IBAN jenes Kontos, auf das die Überweisung letztlich erfolgte, einen Überweisungsbetrag von 12.880 EUR und den vierstelligen TAC-Code. Noch am selben Tag wurde vom Konto der Kläger bei der Beklagten der Betrag von 12.880 EUR auf ein österreichisches Girokonto einer anderen Kreditanstalt der unbekannten Betrüger überwiesen.

Die Betrüger hatten sich zuvor entweder durch Installieren eines Schadprogramms auf eines der IT-Systeme des Erstklägers oder durch einen Phishing-Angriff Zugriff auf das System des Erstklägers geschaffen und damit dessen Zugangsdaten erhalten. Die Betrüger konnten sich somit in der Folge im netbanking-Portal des Erstklägers mit dessen Zugangsdaten anmelden und eine Überweisung erstellen. Auf das interne Rechen- und Informationssystem der Beklagten hatten die Betrüger keinen Zugriff erlangt.

Am 14. 10. 2015 gab der Kläger über einen Anruf von derselben Telefonnummer wiederum einen TAC-Code, der ihm auf sein Handy geschickt worden war, bekannt. Zu einer entsprechenden Überweisung von 4.800 EUR auf ein spanisches Konto kam es aber nicht, weil ein Mitarbeiter der Beklagten Verdacht schöpfte und mit dem Erstkläger telefonisch in Kontakt trat.

Ausgehend von einem maßgerechten Durchschnitts-Onlinebanker, der einem unbekannten Dritten die Sicherheitsmerkmale nicht mitteilen werde, weil er sich bewusst sei, dass die Weitergabe von personalisierten Sicherheitsmerkmalen an unbekannte Dritte mit der Gefahr einer missbräuchlichen Verwendung des damit verknüpften Bankkontos durch Betrüger verbunden sei, ist die rechtliche Beurteilung des Berufungsgerichts, der Erstkläger habe durch sein Handeln grob fahrlässig seine Sorgfaltspflichten verletzt, nicht weiter korrekturbedürftig. Dass die telefonische Weitergabe eines TAC-Codes an eine unbekannte Person einen durch Betrug hervorgerufenen

Schadenseintritt nicht bloß möglich, sondern geradezu wahrscheinlich macht, muss jeder mit dem Electronic Banking vertrauten Person alleine schon aus der medialen Berichterstattung und den zahlreichen, insbesondere im Bankenbereich üblichen Warnungen bewusst sein. Schon bei einem bloß kurzen Überfliegen des SMS hätte der Erstkläger leicht erkennen können, dass es sich nicht um eine – wie telefonisch angekündigt – Datenaktualisierung handelte, sondern um eine Überweisung (Zahlungsfreigabe) eines Betrags von 12.880 EUR von seinem Konto. Auch die Auffassung des Berufungsgerichts, einem maßgerechten Durchschnitts-Onlinebanker müsse es höchst verdächtig erscheinen, wenn eine „Bankmitarbeiterin" Informationen von ihm erfahren möchte, die sie ihm laut eigener Aussage gerade selbst übermittelt habe und daher selbst darüber verfügen müsse, ist nach Lage des Falls nicht zu beanstanden. Von einer „bloßen Verkettung unglücklicher Umstände" – so die Kläger – kann nach Lage des Falls nicht gesprochen werden.

Aus der Entscheidung 10 Ob 102/15w (EvBl 2016/111 [Hoch/Kellner] = jusIT 2016/51 [Janisch] = JBl 2017, 316 [Dullinger]) ist für die Kläger nichts zu gewinnen. Darin wurde die Weitergabe von iTANs durch den Benutzer (Kunden) nach einer gelungenen Phishing-Attacke durch den Betrüger als – jedenfalls – leicht fahrlässig beurteilt. Der Beurteilung, ob das Verhalten des Kunden (sogar) grob fahrlässig war, bedurfte es nicht. In der Lehre wird die Mitteilung der Geheimzahlen durch den Kunden an eine dritte Person regelmäßig als grob fahrlässig angesehen (Harrich, ZaDiG 311; jusIT 2016/51 [Janisch], 109 [110]; EvBl 2016/111 [Hoch/Kellner], 779 [784]; Dullinger, Schadenersatzpflicht wegen Sorgfaltspflichtverletzung bei Phishing-Attacke, JBl 2017, 316 [321]).

Insgesamt gelingt es den Klägern nicht, eine erhebliche Rechtsfrage im Sinn des§ 502 Abs 1 ZPO, die die Revision zulässig machen würde, aufzuzeigen. Die Revision war daher als unzulässig zurückzuweisen.

Die Kostenentscheidung beruht auf den §§ 41, 50 ZPO. Die Beklagte hat auf die Unzulässigkeit der Revision der Kläger in ihrer Revisionsbeantwortung hingewiesen (RIS-Justiz RS0035979 [T16]).

Textnummer

E122389

European Case Law Identifier (ECLI)

ECLI:AT:OGH0002:2018:0090OB00048.18A.0724.000

Im RIS seit

14.08.2018

Zuletzt aktualisiert am

18.02.2020