Landgericht Köln, 22 O 43/23

Datum:	20.11.2023
Gericht:	Landgericht Köln
Spruchkörper:	22. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	22 O 43/23
ECLI:	ECLI:DE:LGK:2023:1120.22O43.23.00

Rechtskraft:	nicht rechtskräftig

Tenor:

Die Beklagte wird verurteilt, das bei ihr geführte Girokonto des Klägers (Kontonr. N01) auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge in Höhe von insgesamt EUR 9.933,38 am 23.09.2022 befunden hätte.

Die Beklagte wird weiter verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von EUR 973,66 nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 23.05.2023 zu zahlen.

Die Kosten des Rechtsstreits trägt die Beklagte.

Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages.

Tatbestand: 1

Der Kläger nimmt die Beklagte auf Wiedergutschrift nicht autorisierter Zahlungsvorgänge in Anspruch. 2

Der Kläger unterhält bei der Beklagten ein Privatgirokonto mit der Kontonummer N01, basierend auf einem zwischen ihnen bestehenden Zahlungsdiensterahmenvertrag. Er nutzt hierfür seit 2017 das Online-Banking auf der Grundlage einer Rahmenvereinbarung über die Teilnahme am Online-Banking (Anl. B1, Bl. 82 ff. d. A.) unter Einbeziehung der „Bedingungen für das Online-Banking“ der Beklagten (Anlage B2). Dort heißt es (auszugsweise): 3

*„**4 Aufträge*** 4

4.1 Auftragserteilung 5

Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Sparkasse bestätigt mittels Online-Banking den Eingang des Auftrags. 6

7 Sorgfaltspflichten des Teilnehmers 7

7.1 Schutz der Authentifizierungselemente 8

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4). 9

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten: 10

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere 11

? nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt - werden, 12

? nicht außerhalb des Online-Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden, 13

? nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und 14

? nicht auf einem Gerät notiert oder als Abschrift zusammen 15

? mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. Sparkassen-Card mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient. 16

(b) Besitzelemente, wie z. B. die Sparkassen-Card mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere 17

? sind die Sparkassen-Card mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren, 18

? ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können, - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online-Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können, 19

(…) 20

7.2 Sicherheitshinweise der Sparkasse 21

22

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Sparkasse, insbesondere die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software, beachten.

7.3 Prüfung der Auftragsdaten mit von der Sparkasse angezeigten Daten 23

Die Sparkasse zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.“ 24

Für die weiteren Inhalte und Bestimmungen der Bedingungen für das Online-Banking (im Folgenden „*AGB*“) der Beklagten wird auf Anlage B2, Bl. 87 ff. d. A. verwiesen. 25

Im Hinblick auf die Nutzung des Online-Bankings entschied sich der Kläger für die Verwendung des sog. S-pushTAN-Verfahrens als Authentifizierungsinstrument (Anl. B1, Bl. 83 d. A.). Beim S-pushTAN-Verfahren ermöglicht es die Beklagte ihren Kunden eine Überweisung oder eine sonstige Handlung ? darunter beispielsweise auch die Freischaltung von ApplePay ? webbasiert in der Banking App einzugeben. Veranlasst der Kunde einen Auftrag, benötigt er für dessen Freigabe zusätzlich eine TAN als elektronische Unterschrift. Hierzu bediente der Kläger sich des S-pushTAN-Verfahrens. Durch dieses Verfahren kann der Kläger von einem einzigen Gerät aus sowohl auf sein Online-Banking zugreifen als auch eine TAN anfordern. Hierzu logt sich der Kunde über seinen PC oder sein mobiles Endgerät über eine separate App in das Online-Banking-Programm unter Verwendung von Anmeldenamen und PIN ein. Wenn er einen Auftrag (z.B. Überweisung, PIN Änderung; Kartenfreischaltung; erweiterte Konteneinsicht, pp.) initialisiert, erhält er für die elektronische Unterschrift eine TAN unter Angabe der konkreten Verwendung übersandt. Hierzu hat der Kläger auf seinem Mobiltelefon die S-pushTAN App installiert. In diese wird die Nachricht durch das Rechenzentrum übermittelt; in ihr muss der Kläger die Freigabe/TAN-Verwendung bei Anzeige des konkret übermittelten Verwendungszwecks bestätigen (Schieberegler in der pushTAN-App). Bei jeder Freigabe erscheint folgender Text: 26

„Bitte geben Sie keinen Auftrag frei, den Sie nicht explizit beauftragt haben. Wenden Sie sich bei Unklarheiten oder Fragen bitte umgehend an Ihren Berater und geben telefonisch keine sensiblen Informationen an Dritte weiter.“ 27

Am 23.09.2022 kontaktierte ein Unbekannter den Kläger telefonisch unter Anzeige der Rufnummer der Beklagten (Nummer +N02). Der Anrufer gab vor, ein Mitarbeiter der Beklagten zu sein, war dies jedoch tatsächlich nicht. Für den Anruf unter Anzeige der Nummer der Beklagten bediente er sich des sog. Call-ID Spoofings. Der Anrufer erfragte beim Kläger, ob dieser in der vergangenen Woche von betrügerischen Anrufen oder verdächtigen Kontobewegungen betroffen gewesen sei. Der Kläger verneinte dies. Der Anrufer teilte ihm daraufhin mit, dass er aufgrund aktueller Betrugsvorfälle vorsorglich das Konto und die Karte des Klägers gesperrt habe, dieses aber nun nach dessen Auskunft wieder entsperren könne. Er bat den Kläger sodann um entsprechende Freigabe über die pushTAN App der Beklagten auf dem Mobiltelefon des Klägers gebeten. In der pushTAN App erschien daraufhin, am 23.09.2022 um 12:00 Uhr, ein Auftrag mit dem Text „*Registrierung Karte*“ und dem oben genannten Warnhinweis. Der Kläger gab den Auftrag frei. Mit dieser Freigabe bestätigte er tatsächlich einen durch die Täter initiierte Registrierung einer digitalen Version seiner Debitkarte zur Speicherung auf einem mobilen Endgerät. Diese installierten die Täter auf deren mobilen Endgerät und konnten infolgedessen Zahlungen mit der digitalen 28

Debitkarte, zum Beispiel unter Nutzung von ApplePay, vornehmen.

Zwischen dem 23.09.2022 und dem 25.09.2022 nahmen die Täter Zahlungen über zusammen EUR 14.040,90 per ApplePay zu Lasten des Kontos des Klägers vor (vgl. Umsatzübersicht des Klägers, Anl. K1, Bl. 18 f. d. A., sowie Kontoauszug, Anl. K2). Lediglich zwei Zahlungen in diesem Zeitraum, in Höhe von EUR 500 bzw. EUR 50, wurden vom Kläger autorisiert. Die Beklagte erstattete dem Kläger vorgerichtlich bereits EUR 4.107,52. 29

Der Kläger forderte die Beklagte mit zwei E-Mails vom 23.10.2022 und 30.10.2022 zur Erstattung des Restbetrages von EUR 9.933,38 auf. Diese lehnte die Beklagte unter Berufung auf Ziff. 7.3 der AGB ab. Daraufhin forderte der Kläger die Beklagte erneut mit anwaltlichen Schreiben vom 23.12.2022 zur Rückerstattung des Restbetrages unter Fristsetzung bis zum 06.01.2023 auf. Die Beklagte reagierte darauf nicht. Am 22.05.2023 erhob der Kläger daraufhin die gegenständliche Klage. 30

Der Kläger ist der Ansicht, ihm stehe gegen die Beklagte ein Erstattungsanspruch in Höhe von EUR 9.933,38 auf Grundlage von § 675u Satz 2 BGB zu. Diesem könne die Beklagte auch keinen Anspruch gegen den Kläger aus § 675v Abs. 3 Nr. 2 BGB entgegenhalten, da er jedenfalls nicht grob fahrlässig gehandelt habe. Bereits objektiv sei angesichts der Nutzung der Nummer der Beklagten kein schwerer Pflichtenverstoß anzulasten; jedenfalls sei ihm sein Verhalten subjektiv nicht unentschuldbar, da der Kläger zum einen nicht technisch versiert und zum anderen der angezeigte Freigabetext nicht präzise genug gewesen sei, um Misstrauen zu erregen. Jedenfalls sei der Anspruch auch gemäß § 675v Abs. 4 Satz 1 Nr. 11 BGB ausgeschlossen, da die Beklagte keinen Nachweis einer starken Kundenauthentifizierung erbracht habe. Im Übrigen treffe die Beklagte jedenfalls ein Mitverschulden, da die gegenständlichen Zahlungen an verschiedenen Orten in Deutschland in kurzen Zeitabständen vorgenommen worden seien, was eine Vornahme durch dieselbe Person kaum möglich mache. 31

Der Kläger beantragt, die Beklagte zu verurteilen, 32

1. das bei ihr geführte Girokonto des Klägers Nr. N01 auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge, die Zahlungen in Höhe von insgesamt EUR 9.933,38 am 23.09.2022, befunden hätte; 33

2. dem Kläger die vorgerichtlichen Rechtsanwaltskosten in Höhe von EUR 973,66 nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen. 34

Die Beklagte beantragt, 35

die Klage abzuweisen. 36

Die Beklagte meint, der Kläger habe durch sein Verhalten in grob fahrlässiger Weise insbesondere gegen seine Verpflichtung aus Ziff. 7.3 der AGB zur Überprüfung der in der pushTAN App angezeigten Auftragsdaten verstoßen. Er habe einen Auftrag freigegeben, den er selbst nicht beauftragt habe und insofern die im Auftrag selbst angezeigte Warnung, dies nicht zu tun, missachtet. Im Übrigen passe der Wortlaut „*Registrierung Karte*“ nicht zu der ihm durch den angeblichen Mitarbeiter der Beklagten mitgeteilten angeblichen Entsperrung der Karte. Ein Mitverschulden der Beklagten liege auch nicht vor, da es sich bei den von dem Kläger genannten Abrechnungsorten nicht um die Einsatzorte der Karte, sondern um den Sitz des jeweiligen Gläubigers handele. 37

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen, die Gegenstand der mündlichen Verhandlung gewesen sind, ergänzend Bezug genommen. 38

Entscheidungsgründe: 39

Die zulässige Klage ist vollumfänglich begründet. 40

- I. 41 42

Der Klageantrag zu 1.) ist begründet. Der Kläger hat einen Anspruch gegen die Beklagte, das bei ihr geführte Girokonto des Klägers Nr. N01 auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge in Höhe von insgesamt EUR 9.933,38 am 23.09.2022 befunden hätte. 43

1. 44

Nach § 675u S. 1 BGB hat der Zahlungsdienstleister (hier die Beklagte) des Zahlers (hier des Klägers) im Fall eines nicht autorisierten Zahlungsvorgangs gegen diesen keinen Anspruch auf Erstattung seiner Aufwendungen. Er ist nach § 675u S. 2 BGB verpflichtet, dem Zahler den Zahlungsbetrag unverzüglich zu erstatten und, sofern der Betrag einem Zahlungskonto belastet worden ist, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. 45

2. 46

Diese Voraussetzungen sind vorliegend erfüllt, da die streitgegenständlichen Zahlungsvorgänge nicht durch den Kläger autorisiert waren. Dies ist bereits deshalb der Fall, weil sie nicht durch den Berechtigten, nämlich den Kläger, ausgeführt worden sind; eine Stellvertretung für den Kläger ist ausgeschlossen (vgl. BGH, Urteil vom 26.01.2016 – XI ZR 91/14, BGHZ 208, 331 Rn. 58 m.w.N.). Dass der Kläger die Zahlungsvorgänge mittels ApplePay nicht selbst autorisiert hat, steht nach dem Vortrag der Parteien fest. Während die Beklagte zunächst die Autorisierung jedenfalls konkludent bestritten hat („*sofern er die Freigabe einer digitalen Debitkarte nicht wissentlich veranlasst hat*“, Bl. 73 d. A.), ging sie zuletzt von „*durch den Betrüger vorgenommenen Zahlungen*“ (Bl. 157 d. A.) aus. Jedenfalls wäre auch ein einfaches Bestreiten der Beklagten, die nach Maßgabe des § 675w BGB vorrangig im Hinblick auf den Nachweis der Authentifizierung darlegungs- und beweisbelastet ist, nicht geeignet gewesen, um den substantiierten Ausführungen des Klägers entgegenzutreten (vgl. § 138 Abs. 3 ZPO). 47

Die Beklagte kann dem klägerischen Anspruch auch keinen Schadensersatzanspruch gemäß § 675v BGB nach § 242 BGB entgegenhalten (sog. dolo-agit-Einwendung). Der Beklagten steht unter keinem erdenklichen rechtlichen Gesichtspunkt ein solcher Schadensersatzanspruch zu. Ein solcher Anspruch ergibt sich insbesondere nicht aus § 675v Abs. 3 Nr. 2 BGB. 48

Nach § 675v Abs. 3 BGB ist der Zahler seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Zahler entweder in betrügerischer Absicht gehandelt hat (§ 675v Abs. 3 Nr. 1 BGB) oder er den Schaden durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Pflichten gemäß § 675l Abs. 1 BGB (§ 675v Abs. 3 Nr. 2 a) BGB) oder 49

einer oder mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments nach § 675l Abs. 2 BGB (§ 675v Abs. 3 Nr. 2 b) BGB) herbeigeführt hat.

Im Hinblick auf den allein in Betracht kommenden Anspruch gemäß § 675v Abs. 3 Nr. 2 BGB ist die Beklagte ihrer diesbezüglichen Darlegungs- und Beweislast nicht nachgekommen. 50

Grobe Fahrlässigkeit erfordert einen in objektiver Hinsicht schweren und in subjektiver Hinsicht schlechthin unentschuldbaren Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt. Selbst ein objektiv grober Pflichtenverstoß rechtfertigt für sich noch keinen zwingenden Schluss auf ein entsprechend gesteigertes personales Verschulden (vgl. BGH, Urteil vom 26.01.2016, XI ZR 91/44, Rn. 71 m.w.N.). Dabei kommt dem Zahlungsdienstleister auch kein Anscheinsbeweis zu Gute, dass bei einem Missbrauch des Online-Bankings, wenn die Nutzung eines Zahlungsauthentifizierungsinstruments korrekt aufgezeichnet worden und die Prüfung der Authentifizierung beanstandungsfrei geblieben ist, eine konkrete grob fahrlässige Pflichtverletzung des Zahlungsdienstnutzers nach § 675v Abs. 2 BGB vorliegt (BGH, a.a.O. Rn.68). 51

Schon nach dem Vortrag der Beklagten fehlt es hier allerdings beim Kläger an einer grob fahrlässigen Verletzung der Pflichten eines Zahlungsdienstnutzers. Das Verhalten des Klägers ist danach jedenfalls nicht als subjektiv schlechthin unentschuldbar zu werten. 52

Diese Einschätzung stützt das Gericht zum einen darauf, dass sich die Täter des sog. Call-ID Spoofings bedienten. Dem Kläger wurde infolgedessen die Nummer der Beklagten angezeigt, als die Täter ihn anriefen. Für einen verständigen, langjährigen Bankkunden ist die Nutzung einer ihm bekannten Nummer mit besonderem Vertrauen verbunden. Davon, dass die Möglichkeit besteht, eine fremde Nummer zu nutzen, dürfte der Durchschnittsbürger keine Kenntnis haben. Dass dem Kläger der angebliche Mitarbeiter der Beklagten nicht bekannt war, ist für sich genommen noch kein besonders verdächtiger Umstand. In einer großen Organisation wie der der Beklagten herrscht regelmäßig eine gewisse Fluktuation bzw. es findet eine Arbeitsteilung statt, sodass die Bankkunden nicht mehr zwingend nur mit einem Mitarbeiter in Kontakt stehen. 53

Etwas anderes gilt auch nicht aufgrund der Bezeichnung des Auftrags in der pushTAN App als „*Registrierung Karte*“. Zwar gab der Anrufer vor, er wolle die Karte des Klägers *entsperren* , nicht *registrieren*. Allerdings ist die Bezeichnung „*Registrierung*“ derart weit, dass für den Kläger – vor allem in der Überrumpelungssituation, in der er sich befand und auch bei der durch die Beklagte mit einem Sicherheitshinweis angemahnten sorgfältigen Prüfung – überhaupt nicht erkennbar war, dass es um die Einrichtung eines Zahlungssystems auf einem mobilen Endgerät der Herstellers Apple Inc. und damit die Freigabe einer Möglichkeit zu Kontoverfügungen geht, die nur von der Verfügungsgewalt über dieses mobile Endgerät abhängt. Dabei wäre es der Beklagten ohne weiteres möglich gewesen, durch einen eindeutigen Text, insbesondere durch Verwendung eines Hinweises gerade auf ApplePay dem Kunden deutlich vor Augen zu führen, welcher Zahlungsdienst hier freigegeben werden soll, um so ersichtlich zu machen, dass es um Endgeräte eines bestimmten Herstellers und die Nutzung als Wallet, nicht einer Karte geht (vgl. LG Köln, Urteil vom 09.03.2023 - 15 O 267/22). Bei der hier vorliegenden Gestaltung konnte der Kläger den Text in der pushTAN App dem eigentlichen Vorgang nicht zuordnen. Im Übrigen ergibt sich aus der Formulierung des Warntextes, es sei „*kein Auftrag*“ freizugeben, der nicht „*explizit beauftragt*“ wurde, nach seinem natürlichen Wortsinn nicht, dass der Auftrag zwingend über die Online-Banking App erfolgt sein muss. Der Kläger durfte davon ausgehen, dass sein – vermeintlich ? telefonisch erteilter „*Auftrag*“ diese Voraussetzungen ebenso erfülle. Der Vorgang und auch der Pflichtenverstoß des Klägers ist daher bereits nicht allein dessen Verantwortungsbereich 54

anzulasten.

Auf die Fragen, ob eine starke Kundenauthentifizierung verlangt wurde (§ 675v Abs. 4 BGB) oder der Beklagten ein Mitverschulden anzulasten ist, kommt es insofern nicht mehr an. 55

- II. 56-57

Der Klageantrag zu 2.) ist ebenfalls begründet. Der Kläger hat gegen die Beklagte einen Anspruch auf Zahlung der vorgerichtlichen Rechtsanwaltskosten in Höhe von EUR 973,66 nebst Zinsen in Höhe von fünf Prozentpunkten seit dem 23.05.2023. 58

Der Anspruch auf Zahlung der vorgerichtlichen Rechtsanwaltskosten ergibt sich aus §§ 280 Abs. 1, 2, 286 BGB i.V.m. § 675u Satz 3 BGB. Die Beklagte befand sich mit der gemäß § 675u Sätze 2, 3 BGB „unverzüglich“ geschuldeten Erstattung in Verzug (vgl. OLG Celle Hinweisbeschluss v. 17.11.2020 – 3 U 122/20, BeckRS 2020, 33608 Rn. 44 ff.). 59

Der Zinsanspruch folgt aus §§ 291, 288 Abs. 1 BGB i.V.m. § 187 Abs. 1 BGB analog. 60

- III. 61-62

Die Nebenentscheidungen folgen aus §§ 91 Abs. 1 Satz 1, 709 Sätze 1, 2 ZPO. 63

- IV. 64-65

Der Streitwert wird auf EUR 9.933,38 festgesetzt. 66
