Hanseatisches Oberlandesgericht in Bremen

Geschäftszeichen: 1 U 47/23 = 4 O 1557/22 Landgericht Bremen

B e s c h l u s s

In dem Rechtsstreit

…,

Klägerin,

Prozessbevollmächtigter:
…

gegen

…,

Beklagte,

Prozessbevollmächtigte:
…

hat der 1. Zivilsenat des Hanseatischen Oberlandesgerichts in Bremen durch den Vorsitzenden Richter am Oberlandesgericht Kelle, den Richter am Oberlandesgericht Dr. Böger und den Richter am Amtsgericht Kokemohr

am **15.04.2024** beschlossen:

I. Der Senat beabsichtigt, die Berufung der Klägerin gegen das Urteil des Landgerichts Bremen vom 15.09.2023, Az.: 4 O 1557/22, durch einstimmigen Beschluss gemäß § 522 Abs. 2 ZPO zurückzuweisen.

II. Der Klägerin wird Gelegenheit zur Stellungnahme bis zum 08.05.2024 gegeben.

I.

Die Klägerin nimmt die Beklagte auf Erstattung aufgrund diverser Abbuchungen von ihrem Girokonto in Anspruch.

Die beklagte Bank führte aufgrund mit der Klägerin bestehender Kontoführungsverträge u.a. ein Girokonto und ein Tageskonto für die Klägerin. Mit Vereinbarungen aus dem Jahr 2004 hatten die Parteien hinsichtlich der Konten der Klägerin die Nutzung des Online-Bankings sowie im Dezember 2018 die Nutzung des mobile-TAN-Verfahrens vereinbart unter weiterer Vereinbarung eines Tageslimits von EUR 50.000,- sowie der Geltung der Sonderbedingungen für das Online-Banking der Beklagten. In der Vereinbarung vom Dezember 2018 heißt es unter anderem, dass die ausgehändigten Transaktionsnummern (TAN) zur Vermeidung von Missbrauch geheim zu halten sind. Bei dem mobile-TAN-Verfahren (auch als SMS-TAN oder mTAN-Verfahren bezeichnet) wird ein Zahlungsvorgang im Online-Banking, dessen Zugang durch die Eingabe einer PIN gesichert wird, mit einer TAN autorisiert, die mittels einer SMS-Nachricht an die vereinbarte Mobilfunknummer des Kunden gesendet wird.

Am 11.03.2022 erhielt die Klägerin einen Telefonanruf. Der Anrufer gab sich als Mitarbeiter der Beklagten aus und hatte Zugang zu dem Online-Banking der Klägerin. Das Gespräch dauerte insgesamt 41 Minuten, wobei der Inhalt des Gesprächs zwischen den Parteien im Einzelnen streitig ist. Der Klägerin wurden während der Dauer dieses Gesprächs insgesamt neun TANs per SMS übersandt, teils Änderungen des Limits auf zunächst EUR 30.000,- bzw. sodann EUR 50.000,- betreffend, teils betreffend Überweisungen von Beträgen jeweils in Höhe von über EUR 9.400,- an verschiedene durch Angabe der IBAN benannte Konten. Die Klägerin teilte dem Anrufer die in den SMS enthaltenen TANs telefonisch mit. Während der Dauer des Gesprächs veranlasste der Anrufer über den Online-Banking-Zugang der Klägerin durch zwei Umbuchungen die Übertragung eines Betrags von EUR 40.500,- vom Tagesgeldkonto der Klägerin auf deren Girokonto und er löste unter Verwendung der übersandten TANs insgesamt fünf Überweisungen über einen Gesamtbetrag von EUR 47.238,08 auf verschiedene Konten unbekannter Dritter bei anderen Banken aus.

Die Beklagte belastete das Konto der Klägerin mit dem Betrag der vorgenannten Überweisungen. Mit vorgerichtlichem Schreiben ihres Prozessbevollmächtigten vom 17.05.2022 machte die Klägerin die mangelnde Berechtigung der Abbuchungen geltend; die Beklagte lehnte mit Schreiben vom 30.05.2022 eine Haftung für den Schaden

der Klägerin ab und erklärte mit weiterem Schreiben vom 30.06.2022 die Aufrechnung mit einem eigenen Schadensersatzanspruch gegen den Anspruch der Klägerin auf Wiedergutschrift des abgebuchten Betrags.

Die Klägerin hat vor dem Landgericht behauptet, dass bei dem Telefonanruf die Rufnummer ihres damaligen Sachbearbeiters der Beklagten angezeigt worden sei und dass sich der Anrufer als Herr […] von der Sicherheitsabteilung der Beklagten ausgegeben habe. Der Anrufer habe ihr zunächst mitgeteilt, dass er Informationen über einen Zugriff Dritter auf die Konten der Klägerin habe. Die Klägerin habe zunächst keine Antworten auf die daran anschließenden Fragen des Anrufers unter anderem zur Vornahme einer Änderung des Kreditlimits gegeben und stattdessen nach der Legitimation des Anrufers gefragt, worauf ihr der Anrufer Informationen zu Kontodaten, Bewegungen auf den Konten, zu ihrem Bankberater und zu persönlichen Daten der Klägerin etc. genannt habe. Die Klägerin habe sodann geäußert, dass sie gerne zurückrufen möchte, der Anrufer habe ihr aber mitgeteilt, dass sie dann in der Warteschleife landen würde und rasches Handeln erforderlich sei. Auf Anforderung des Anrufers habe die Klägerin sich in das Online-Banking-System eingeloggt und dabei festgestellt, dass die Angaben des Anrufers zu Bewegungen auf ihrem Konto zutreffend gewesen seien. Der Anrufer habe der Klägerin mitgeteilt, dass sie eine TAN erhalten werde, damit das Limit wieder geändert werden könne und dass Geld von ihrem Konto abgebucht werden werde, dass aber die Bank bis EUR 100.000,- versichert sei und er das Geld wieder zurückbuchen werde. Es seien sodann zunächst die Abbuchungen vorgenommen worden und die Klägerin habe dann im Online-Banking-System nachvollzogen, dass das Girokonto wieder ausgeglichen worden sei, sie habe dann aber festgestellt, dass das Tagesgeldkonto plötzlich auf null gestanden habe. Die Klägerin meint, dass die telefonische Weitergabe der TANs an den Anrufer nicht den Vorwurf einer groben Fahrlässigkeit begründe, da die Klägerin die Legitimation des Anrufers anhand der angezeigten Telefonnummer, der Mitteilung der ihr Konten betreffenden Daten sowie der Umbuchungen vom Tagesgeldkonto habe nachvollziehen können. Zudem meint sie, dass sie habe davon ausgehen dürfen, dass lediglich einem Bankmitarbeiter Umbuchungen vom Tagesgeldkonto möglich seien. Dem Vorwurf auch in subjektiver Hinsicht grob fahrlässigen Verhaltens der Klägerin stehe auch entgegen, dass sie – insoweit unstreitig – den Online-Banking-Zugang lediglich zur bloßen Kontoeinsichtnahme genutzt habe, wobei sie hier lediglich sporadisch das mobile-TAN-Verfahren zur Authentifizierung verwendet habe, um weiteren Zugriff auf die Kontoübersichten zu erhalten.

Die Klägerin hat weiter behauptet, dass im Online-Banking-System der Beklagten erhebliche Sicherheitslücken bestanden hätten. Dies werde dadurch belegt, dass der Anrufer Zugriff auf die Konten der Klägerin und Kenntnis von diversen Daten betreffend diese Konten gehabt habe und die streitgegenständlichen Zahlungsvorgänge habe auslösen können, ohne dass zuvor der Computer der Klägerin gehackt worden wäre oder dass sie die Zugangsdaten im Rahmen einer Phishing-Attacke weitergegeben gegeben hätte. Zudem meint die Klägerin, dass es pflichtwidrig sei, dass die Beklagte die Vornahme von Umbuchungen vom Tagesgeldkonto auf das Girokonto ohne Verwendung einer TAN zugelassen habe. Verfügungen betreffend das Tagesgeldkonto seien überdies der Klägerin nicht im Online-Banking möglich gewesen, sondern ausschließlich im Schaltergeschäft.

Die Beklagte hat vor dem Landgericht bestritten, dass bei dem Anruf bei der Klägerin eine Telefonnummer der Beklagten angezeigt worden sei und dass der Anrufer sich als Herr […] von der Sicherheitsabteilung der Bank ausgegeben habe, welche es überdies gar nicht gebe. Die Beklagte ist der Auffassung, dass sie einen Anspruch auf Schadensersatz gemäß § 675v Abs. 3 Nr. 2 Buchst. a) und b) BGB wegen einer grob fahrlässigen Verletzung von Sicherheitspflichten seitens der Klägerin durch die Weitergabe der ihr mitgeteilten TANs an den Anrufer geltend machen könne. Die Beklagte hat vor dem Landgericht behauptet, dass die Sicherheitsvorkehrungen ihres Online-Banking-Systems aufgrund der erforderlichen Legitimation zur Vornahme einer Transaktion durch die Anmeldung mit dem individuellen Zugangsnamen des Kunden, seiner PIN und der richtigen TAN sicher und unüberwindbar seien. Zudem habe die Beklagte bereits mehrere Monate zuvor auf ihrer Homepage auf die Gefahr des Phishings hingewiesen und es habe sich unter der Anmeldemaske für das Online-Banking-System der Beklagten der Hinweis befunden, dass Bankmitarbeiter niemals nach der PIN oder einer TAN fragen.

Das Landgericht hat mit Urteil vom 15.09.2023 die auf Zahlung von EUR 47.238,08 nebst Zinsen und vorgerichtlichen Rechtsanwaltskosten gerichtete Klage abgewiesen. Zur Begründung hat das Landgericht ausgeführt, dass der Erstattungsanspruch der Klägerin aus § 675u S. 2 BGB wegen der unautorisierten Zahlungsvorgänge aufgrund der Aufrechnung der Beklagten mit ihrem in gleicher Höhe bestehenden Schadensersatzanspruch gegen die Klägerin aus § 675v Abs. 3 BGB erloschen sei.

Die unstreitig erfolgte telefonische Preisgabe der der Klägerin per SMS übermittelten TANs sei als grob fahrlässiger Verstoß der Klägerin gegen ihre Pflicht aus § 675l Abs. 1 BGB zum Schutz der personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu bewerten. Bereits nach dem von der Klägerin behaupteten Inhalt und Verlauf des Telefongesprächs habe sich für die Klägerin ein Betrugsverdacht im höchsten Maße aufdrängen müssen. Der Schadensersatzanspruch der Beklagten sei auch nicht gemäß § 254 BGB wegen eines Verstoßes gegen ihre Schadensminderungspflicht verstoßen. Soweit die Klägerin massive Sicherheitslücken im Online-Banking der Beklagten behaupte, sei dieser Vortrag lediglich pauschal und nicht hinreichend konkret genug. Hinsichtlich des Tatbestandes und des weiteren Vorbringens der Parteien in erster Instanz einschließlich der dort gestellten Anträge wird im Übrigen Bezug genommen auf die Feststellungen im angefochtenen Urteil des Landgerichts Bremen vom 15.09.2023, Az.: 4 O 1557/22 (§ 540 Abs. 1 Nr. 1 ZPO).

Gegen dieses Urteil wendet sich die Klägerin mit ihrer Berufung, mit der sie ihren erstinstanzlichen Klagantrag weiterverfolgt.

Die Klägerin macht mit ihrer Berufung geltend, dass das Landgericht zu Unrecht das Vorliegen einer grob fahrlässigen Pflichtverletzung der Klägerin bejaht habe. Es liege bereits in objektiver Hinsicht kein das gewöhnliches Maß der Fahrlässigkeit erheblich übersteigender Sorgfaltspflichtverstoß vor. Der Klägerin sei nicht bekannt gewesen, dass eine Rufnummernanzeige manipuliert werden könne, und sie habe auch wegen der Kenntnis des Anrufers von kontobezogenen Daten davon ausgehen dürfen, dass es sich bei dem Anrufer um eine berechtigte Person handele. Dies gelte zumal deswegen, weil von der Klägerin weder die PIN noch Kennwörter herausgegeben worden seien. Es hätten vom Landgericht hierzu auch die Klägerin angehört bzw. sie als Partei sowie ihr Ehemann als Zeugin vernommen werden müssen. Es streite ein Anscheinsbeweis dafür, dass das Online-Banking-System der Beklagten unsicher und überwindbar sei, und hiermit habe die Klägerin als durchschnittlicher Kunde nicht rechnen müssen. Die Beklagte habe hinsichtlich der Abwicklung von Zahlungsvorgängen Risiken für die Klägerin geschaffen, für welche die Beklagte verantwortlich sei. Die Beklagte habe erst nach dem Vorfall die Sicherheit ihres Online-Banking-Systems umgestellt, während andere Banken bereits höhere technische Standards erfüllt hätten. Hinsichtlich der Umbuchungen vom Tagesgeldkonto habe das Landgericht unzutreffend festgestellt, dass hierfür keine TANs notwendig gewesen seien. Die Vornahme einer sol-

chen internen Umbuchung ohne TAN sei ausschließlich einem Bankmitarbeiter möglich gewesen, wie der Klägerin nachträglich von einer nicht benannten Mitarbeiterin der Beklagten bestätigt worden sei. Überdies fehle es auch deswegen an den subjektiven Voraussetzungen einer groben Fahrlässigkeit, weil die Klägerin unerfahren in der Nutzung des Online-Banking-Systems gewesen sei und immer nur schriftliche Überweisungen vorgenommen habe. Wenn die Beklagte selbst ihr System als unüberwindbar angebe, dann dürfe auch für die Klägerin kein strengerer Maßstab hinsichtlich ihres Vertrauens auf die Sicherheit dieses Systems angelegt werden.

Die Klägerin beantragt,

> unter Abänderung des angefochtenen Urteils die Beklagte zu verurteilen, an die Klägerin EUR 47.238,08 zu zahlen, hilfsweise im Rahmen einer Wertstellung auf dem Konto der Klägerin mit der IBAN: … gutzuschreiben, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 31.05.2022, sowie vorgerichtliche Rechtsanwaltskosten in Höhe von EUR 2.306,82 zu zahlen.

Die Beklagte beantragt,

> die Berufung zurückzuweisen.

Die Beklagte verteidigt das erstinstanzliche Urteil. Ein Zahlungsdienstnutzer handele grob fahrlässig, wenn er einem sich als Bankmitarbeiter ausgebenden Dritten eine TAN übermittele. Die Anforderungen einer starken Kundenauthentifizierung seien auf Fälle von bankinternen Umbuchungen nicht anwendbar. Zudem meint die Beklagte, dass die Mitteilung der TANs durch die Klägerin an den Anrufer nach dem ihr erteilten Hinweis, dass es zu Verfügungen kommen werde, als Autorisierung der Zahlungsvorgänge durch die Klägerin zu bewerten sei.

Hinsichtlich des weiteren Vorbringens der Parteien in der Berufungsinstanz wird auf die gewechselten Schriftsätze verwiesen.

II.

Die Berufung der Klägerin ist form- und fristgerecht eingelegt und auch in der Frist des § 520 Abs. 2 ZPO begründet worden. In der Sache hat sie keine Aussicht auf Erfolg, da das Landgericht zu Recht das Bestehen eines Anspruchs der Klägerin gegen die

Beklagte aus § 675u S. 2 BGB auf Erstattung bzw. Wiedergutschrift der von ihrem Konto abgebuchten Beträge i.H.v. insgesamt EUR 47.238,08 verneint hat. Es handelte sich zwar bei den zugrunde liegenden Überweisungen um nicht autorisierte Zahlungsvorgänge (siehe unter 1.), das Landgericht hat aber zu Recht festgestellt, dass die Beklagte den hieraus erwachsenden Ansprüchen der Klägerin aus § 675u S. 2 BGB einen Schadensersatzanspruch gegen die Klägerin aus § 675v Abs. 3 Nr. 2 Buchst. a) und b) BGB in gleicher Höhe entgegenhalten konnte, und das hiergegen gerichtete Berufungsvorbringen der Klägerin begründet keine Aussicht auf Erfolg für die Berufung der Klägerin (siehe unter 2.).

1. Die Überweisungen i.H.v. insgesamt EUR 47.238,08 zu Lasten des Kontos der Klägerin sind vom Landgericht zutreffend als nicht autorisierte Zahlungsvorgänge bewertet werden, da sie unstreitig durch den unbekannten Anrufer ausgelöst wurden und eine Autorisierung durch die Klägerin entgegen der Auffassung der Beklagten dem beiderseitigen Parteivorbringen nicht zu entnehmen ist. Dass die Klägerin zuvor dem Anrufer die jeweiligen TANs mitgeteilt hatte, ist bereits deswegen nicht als Autorisierung der Zahlungsvorgänge durch die Klägerin anzusehen, da diese Mitteilung der TANs nicht in der zwischen Klägerin und Beklagten vereinbarten Weise (§ 675j Abs. 1 BGB) durch Eingabe im Online-Banking-System der Beklagten erfolgte (insoweit unterscheidet sich der vorliegende Fall von der Konstellation der von der Beklagten zitierten Entscheidung des OLG Schleswig, Beschluss vom 03.01.2024 – 5 W 25/23, n.v.) und ihrer Mitteilung an den Anrufer auch kein Erklärungswert gegenüber der Beklagten im Sinne einer konkludenten Bevollmächtigung des Anrufers zur Erklärung einer Autorisierung für die Klägerin zukommt und im Übrigen die Grundsätze der Bevollmächtigung aus Rechtsscheinsgesichtspunkten im Hinblick auf die Autorisierung von Zahlungsvorgängen wegen der vorrangigen Regelung durch die §§ 675j, 675u, 675v BGB keine Anwendung finden (siehe BGH, Urteil vom 17.11.2020 – XI ZR 294/19, juris Rn. 13, BGHZ 227, 343). Da unstreitig die Zahlungen nicht durch die Klägerin, sondern durch den unbekannten Anrufer im Online-Banking-System der Klägerin ausgelöst wurden, kommt es daher auf die Frage der Anwendbarkeit der Grundsätze des Anscheinsbeweises für eine Autorisierung durch den Zahler in der konkret verwendeten Form des Online-Banking-Systems der Beklagten vorliegend nicht an (siehe hierzu grundlegend BGH, Urteil vom 26.01.2016 – XI ZR 91/14, juris Rn. 34 ff., BGHZ 208, 331; aus jüngerer Zeit siehe einerseits OLG Dresden, Urteil vom 06.04.2023 – 8 U 578/22, juris Rn. 56 ff., GWR 2023, 355 (Ls.); andererseits OLG Schleswig, Beschluss vom 29.10.2018 – 5 U 290/18, juris Rn. 65 ff., WM 2019, 206).

2. Dem Anspruch des Zahlers aus § 675u S. 2 BGB auf Erstattung bzw. Wiedergutschrift der Beträge unautorisierter Zahlungen kann ein Zahlungsdienstleister eigene Ansprüche aus § 675v Abs. 3 BGB wegen einer vorsätzlichen oder grob fahrlässigen Verletzung der Pflichten des Zahlers im Wege der Aufrechnung bzw. nach § 242 BGB entgegengehalten (vgl. BGH, a.a.O., juris Rn. 24 f.). Die Klägerin wendet sich mit ihrem Berufungsvorbringen ohne Aussicht auf Erfolg gegen die Feststellung des Landgerichts, dass der Beklagten gegen die Klägerin ein Schadensersatzanspruch aus § 675v Abs. 3 Nr. 2 Buchst. a) und b) BGB in Höhe des abgebuchten Betrags zusteht.

a. Dies betrifft zunächst die Feststellung des Vorliegens einer grob fahrlässigen Pflichtverletzung der Klägerin.

aa. Unstreitig hat die Klägerin dem sich als Bankmitarbeiter ausgebenden Anrufer die ihr per SMS übermittelten TANs mitgeteilt und damit gegen ihre Pflicht aus § 675l Abs. 1 S. 1 BGB zum Schutz der personalisierten Sicherheitsmerkmale verstoßen, zu denen auch die TAN zählt (siehe BGH, Urteil vom 25.07.2017 – XI ZR 260/15, juris Rn. 29, BGHZ 215, 292; so auch die Begründung des Regierungsentwurfs zum Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 21.01.2009, BT-Drucks. 16/11643, S. 106). Die Verpflichtung aus § 675l Abs. 1 S. 1 BGB ist auf die Geheimhaltung der personalisierten Sicherheitsmerkmale gerichtet (siehe BGH, Urteil vom 26.01.2016 – XI ZR 91/14, juris Rn. 58, BGHZ 208, 331). Die Mitteilung von TANs durch die Klägerin an einen Dritten – auch wenn sich letzterer als Bankmitarbeiter ausgegeben hat – stellt sich daher als Verletzung dieser Verpflichtung dar sowie der sich aus Ziff. 7.1 (2)(a) der Sonderbedingungen für das Online-Banking der Beklagten ergebenden Verpflichtung, Wissenselemente von Authentifizierungselementen nicht mündlich und nicht außerhalb des Online-Banking in Textform weiterzugeben (siehe OLG Frankfurt, Urteil vom 06.12.2023 – 3 U 3/23, juris Rn. 86, BB 2024, 706 (Ls.); OLG Köln, Urteil vom 20.10.2021 – 13 U 18/21, juris Rn. 3; OLG München, Beschluss vom 22.09.2022 – 19 U 2204/22, juris Rn. 116 f.; Beschluss vom 04.09.2023 – 19 U 1508/23 e, juris Rn. 91, BKR 2023, 839). Die wirksame Einbeziehung dieser AGB steht zwischen den Parteien nicht im Streit.

bb. Diese Pflichtverletzung erfolgte auch grob fahrlässig. Grobe Fahrlässigkeit erfordert einen in objektiver Hinsicht schweren und in subjektiver Hinsicht schlechthin unentschuldbaren Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt

(siehe BGH, Urteil vom 26.01.2016 – XI ZR 91/14, juris Rn. 71, BGHZ 208, 331 m.w.N). In objektiver Hinsicht begründet die telefonische Weitergabe von TANs an einen Dritten einen solchen schweren Sorgfaltspflichtverstoß (so auch OLG Frankfurt, Beschluss vom 22.09.2023 – 3 U 84/23, juris Rn. 19; Urteil vom 06.12.2023 – 3 U 3/23, juris Rn. 89, BB 2024, 706 (Ls.); OLG Köln, Urteil vom 20.10.2021 – 13 U 18/21, juris Rn. 3; OLG München, Beschluss vom 04.09.2023 – 19 U 1508/23 e, juris Rn. 91). Es ist bereits als allgemein und jedermann einleuchtend anzusehen, dass dem Bankkunden persönlich zugesandte Sicherheitsmerkmale von diesem nicht abweichend von der vereinbarungsgemäß vorgesehenen Verwendung gegenüber Dritten offenbart werden dürfen, wenn nicht die Sicherheit seines durch diese Merkmale geschützten Kontozugangs gefährdet werden soll. Zudem ist generell aufgrund der in den letzten Jahren vielfach durch verschiedene Medien bekannt gewordenen Fälle die Kenntnis als allgemeines Wissen vorauszusetzen, dass Kunden durch betrügerische Briefe und Anrufe vorgeblicher Bankmitarbeiter zur Preisgabe von Zugangsdaten zum Online-Banking veranlasst werden sollen, denn spätestens seit 2006 wurde das kriminelle Phänomen des Phishings und anderer Methoden, unter Vorspiegelung falscher Tatsachen den Angerufenen zu finanziellen Transaktionen veranlassen, öffentlich breit diskutiert (siehe OLG Frankfurt, Beschluss vom 22.09.2023 – 3 U 84/23, juris Rn. 19; Urteil vom 06.12.2023 – 3 U 3/23, juris Rn. 93, BB 2024, 706 (Ls.); OLG München, Beschluss vom 22.09.2022 – 19 U 2204/22, juris Rn. 99). Insbesondere ist der Vorwurf grober Fahrlässigkeit in objektiver Hinsicht zudem dann begründet, wenn der Bankkunde ohne Prüfung eines entgegenstehenden Textes der SMS, mit der ihm die TAN zugesandt wird, diese an den Dritten weiterleitet, obwohl aus diesem Text zu erkennen gewesen wäre, dass die TAN zur Autorisierung eines nicht vom Kunden gewollten Zahlungsvorgangs bestimmt war (siehe OLG Köln, Urteil vom 20.10.2021 – 13 U 18/21, juris Rn. 3; OLG Oldenburg, Beschluss vom 21.08.2018 – 8 U 163/17, juris Rn. 4, GWR 2019, 50).

cc. Der sich hieraus ergebenden Feststellung des Vorliegens eines in objektiver Hinsicht grob fahrlässigen Sorgfaltspflichtverstoßes der Klägerin stehen auch nicht die hiergegen von der Klägerin vorgebrachten Rügen entgegen:

(a) Dass – wie die Klägerin geltend macht – bei dem Anruf eine Rufnummer der Beklagten angezeigt worden sei und ihr nicht bekannt gewesen sei, dass eine Rufnummernanzeige manipuliert werden könne, steht der Annahme einer groben Fahrlässigkeit bereits deswegen nicht entgegen, weil nach den vereinbarten Sonderbedingungen für das Online-Banking jede mündliche Mitteilung einer TAN pflichtwidrig ist und TANs

vom Bankkunden lediglich im Online-Banking-System selbst weiterzugeben sind. Dem Vorwurf grober Fahrlässigkeit ist daher nicht damit zu begegnen, dass die Klägerin glaubte, mit einem Bankmitarbeiter zu sprechen. Hinzu kommt im vorliegenden Fall, dass – wie bereits das Landgericht zutreffend ausgeführt hat – die Klägerin auch hätte hinterfragen müssen, warum ein angeblicher Mitarbeiter von der Sicherheitsabteilung der Beklagten namens […] mit der Durchwahl des normalerweise für die Klägerin zuständigen Sachbearbeiters bei ihr anrufen sollte. Es kann auch nicht als einleuchtend angesehen werden, dass – wie der Klägerin nach ihrem Vorbringen von dem Anrufer mitgeteilt worden sein soll – die Klägerin im Fall eines Rückrufs in eine Warteschleife geraten sollte, wenn sie nicht die allgemeine Telefonnummer der Bank, sondern eine Durchwahl anrufe, obwohl rasches Handeln nach den Angaben des Anrufers erforderlich sei.

(b) Der Annahme eines in objektiver Hinsicht grob fahrlässigen Sorgfaltspflichtverstoßes der Klägerin steht auch nicht das Argument der Klägerin entgegen, dass sie wegen der Kenntnis des Anrufers von kontobezogenen Daten davon habe ausgehen dürfen, dass es sich bei dem Anrufer um eine berechtigte Person handele. Diese Daten sind vielmehr für einen beliebigen Dritten bei einem unbefugten Zugriff auf das Online-Banking-System einsehbar und konnten daher kein Vertrauen in die Berechtigung des Anrufers begründen, zumal nach den vorstehenden Ausführungen auch einem tatsächlichen Mitarbeiter der Beklagten die TANs nicht mündlich mitzuteilen gewesen wären.

(c) Auch soweit sich die Beklagte allgemein darauf beruft, dass ihr Online-Banking-System sicher und unüberwindbar sei, führt dies nicht dazu, dass ein durchschnittlicher Kunde darauf vertrauen dürfte, dass kein unbefugter Zugriff eines Dritten auf den Online-Banking-Zugang möglich sein könne. Die Sicherheit der Auslösung von Transaktionen über das Online-Banking-System hängt vielmehr nach der gesetzgeberischen Konzeption von der Verwendung des Systems der starken Kundenauthentifizierung (Zwei-Faktor-Authentifizierung) nach den Vorgaben der § 1 Abs. 24, § 55 ZAG und den Regelungen der Delegierten Verordnung (EU) 2018/389 vom 27.11.2017 zur Ergänzung der Richtlinie (EU) 2015/2366 durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (Delegierte VO 2018/389) (ABl. L 69/23 vom 13.03.2018) ab; auf dieses Modell nimmt auch die Beklagte Bezug, wenn sie auf die erforderliche Legitimation des Kunden zur Vornahme einer Transaktion durch die Anmeldung mit dem individuellen Zugangsnamen des Kunden, seiner PIN und der richtigen TAN verweist. Die Sicherheit

dieses Modells hängt systembedingt davon ab, dass sämtliche personalisierten Sicherheitsmerkmale geheim gehalten werden, und durch die pflichtwidrige Weitergabe der überlassenen TANs hat die Klägerin damit selbst die Sicherheit des Online-Banking-Systems beschädigt, so dass sie kein Vertrauen in die Unmöglichkeit eines unbefugten Zugriffs geltend machen kann, wenn sie erst durch ihre Pflichtverletzung die missbräuchliche Auslösung von Zahlungen ermöglicht hat. Hieran ändert es auch nichts, wenn – wie die Klägerin geltend macht – von ihr weder die PIN noch Kennwörter herausgegeben worden seien und auch ihr Computer nicht gehackt worden sei, da auch dies nicht ausschließt, dass sich ein unbefugter Dritter auf andere Weise Zugang zum Online-Banking-System der Beklagten (ohne Kenntnis der erst von der Klägerin weitergegebenen TANs) verschaffen konnte, was auch aus Sicht der Klägerin nicht als ausgeschlossen anzusehen war. Dass der Klägerin seitens der Beklagten eine Garantie erklärt worden wäre in dem Sinne, dass die Beklagte jeglichen unbefugten Zugriff ausschließen könne und sämtliche Haftung für einen eventuellen Missbrauch übernehmen würde, ist den Erklärungen der Beklagten nicht zu entnehmen.

(d) Schließlich ist dem Vorwurf einer in objektiver Hinsicht grob fahrlässigen Pflichtverletzung seitens der Klägerin auch nicht das Argument entgegenzuhalten, dass die Beklagte hinsichtlich der Abwicklung von Zahlungsvorgängen Risiken für die Klägerin geschaffen habe, für welche die Beklagte verantwortlich sei. Wie vorstehend ausgeführt wurde, entspricht das System der Auslösung von Transaktionen über das Online-Banking-System unter Verwendung einer starken Kundenauthentifizierung vielmehr dem gesetzlichen Regelungsmodell und soll gerade im allgemeinen Interesse die Sicherheit für Gelder und personenbezogene Daten der Zahlungsdienstnutzer sowie die Sicherstellung und Aufrechterhaltung eines fairen Wettbewerbs zwischen allen Zahlungsdienstleistern gewährleisten (siehe die Begründung des Regierungsentwurfs zum Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie vom 13.03.2017, BT-Drucks. 18/11495, S. 82), so dass hier kein lediglich im Interesse der Beklagten eröffnetes Risiko vorliegt.

dd. Auch in subjektiver Hinsicht ist der Vorwurf einer grob fahrlässigen Pflichtverletzung begründet; das Verhalten der Klägerin stellt sich als in subjektiver Hinsicht schlechthin unentschuldbarer Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt dar. Die Klägerin ist durch die Vereinbarung vom Dezember 2018 ausdrücklich auf die Verpflichtung zur Geheimhaltung ihr übermittelter TANs hingewiesen werden; dasselbe ergibt sich auch aus den einbezogenen Sonderbedingungen für das Online-Banking

der Beklagten. Vor diesem Hintergrund kann auch offenbleiben, ob die Beklagte bereits vor dem Tag der unautorisierten Abbuchungen diesbezügliche Warnhinweise auf ihrer Homepage veröffentlicht hatte (ebenso in der dortigen Konstellation auch OLG München, Beschluss vom 04.09.2023 – 19 U 1508/23 e, juris Rn. 90). Aus den vorstehenden Ausführungen ergibt sich auch, dass der Grad des subjektiven Fahrlässigkeitsvorwurfs gegenüber der Klägerin nicht im Hinblick darauf zu reduzieren ist, dass die Beklagte selbst sich allgemein auf eine Sicherheit und Unüberwindbarkeit ihres Online-Banking-Systems beruft.

Der Annahme des Vorliegens einer auch in subjektiver Hinsicht grob fahrlässigen Pflichtverletzung der Klägerin kann auch nicht eine subjektive Unerfahrenheit der Klägerin in der Nutzung des Online-Banking-Systems zur Auslösung von Zahlungsvorgängen entgegengehalten werden. Abgesehen von dem bereits bei Vereinbarung der Nutzung des mobile-TAN-Verfahrens im Dezember 2018 erteilten Hinweis auf die Verpflichtung zur Geheimhaltung der Klägerin übermittelter TANs war jeweils aus dem kurzen und daher auch für einen in der Verwendung des Online-Banking-Systems unerfahrenen Nutzer zu übersehenden Text der an die Klägerin übersandten SMS ausdrücklich erkennbar, dass es um die Freigabe einer Überweisung auf ein fremdes Konto geht, so dass die Klägerin hierdurch nochmals besonders gewarnt war und es sich daher auch subjektiv als ein schlechthin unentschuldbarer Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt darstellt, wenn die Klägerin dennoch die betreffenden TANs an den Anrufer übermittelte.

ee. Entgegen der Auffassung der Klägerin war daher auch nicht ihre persönliche Anhörung bzw. eine Parteivernehmung oder die Vernehmung ihres Ehemanns als Zeugen geboten, da das unter Beweis gestellte Tatsachenvorbringen der Klägerin bereits aus den vorstehend ausgeführten Gründen keine anderweitige Beurteilung hinsichtlich der Annahme des Vorwurfs einer groben Fahrlässigkeit trägt.

b. Der Anspruch der Beklagten ist nicht nach § 675v Abs. 4 S. 1 Nr. 1 BGB ausgeschlossen, weil die Beklagte unstreitig bei der Auslösung der Umbuchungen vom Tagesgeldkonto auf das Girokonto der Klägerin keine Eingabe von TANs verlangt hat, d.h. keine starke Kundenauthentifizierung i.S.d. § 1 Abs. 24 ZAG verlangt hat. Der Schaden ist der Beklagten nicht im Sinne des § 675v Abs. 3 Nr. 2 Buchst. a) und b) BGB infolge der Umbuchungen auf das Girokonto der Klägerin entstanden, sondern aufgrund der vom Anrufer ausgelösten Überweisungen auf die bei anderen Banken

geführten Konten Dritter. Bei diesen Überweisungen hat die Beklagte die starke Kundenauthentifizierung angewandt, so dass der Anspruchsausschluss nach § 675v Abs. 4 S. 1 Nr. 1 BGB schon aus diesem Grunde vorliegend nicht eingreift (zur Frage der Berücksichtigung eines anspruchskürzenden Mitverschuldens der Beklagten nach § 254 BGB wegen der Nichtanwendung der starken Kundenauthentifizierung bei den Umbuchungen vom Tagesgeld- auf das Girokonto siehe nachstehend).

c. Der Schadensersatzanspruch der Beklagten ist auch nicht nach § 254 BGB wegen eines Mitverschuldens der Beklagten zu kürzen. Zwar kann grundsätzlich auch einem Anspruch des Zahlungsdienstleisters aus § 675v Abs. 3 BGB der Einwand eines Mitverschuldens des Zahlungsdienstleisters nach § 254 BGB entgegengehalten werden, wenn ihm ein eigenes unsorgfältiges Handeln anzulasten ist (vgl. BGH, Urteil vom 17.11.2020 – XI ZR 294/19, juris Rn. 49, BGHZ 227, 343; so auch die Rspr. des Senats, siehe Hanseatisches OLG in Bremen, Beschluss vom 19.05.2021 – 1 W 4/21, juris Rn. 25, WM 2021, 1792; siehe aus der Literatur BeckOK/Schmalenbach, Ed. 69, § 675v BGB Rn. 19; Ellenberger/Findeisen/Nobbe/Böger-Nobbe, Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 107; MüKo/Zetzsche, 9. Aufl., § 675v BGB Rn. 59). Einer solchen Berücksichtigung eines eigenen Sorgfaltsverstoßes des Zahlungsdienstleisters steht es auch nicht entgegen, wenn – wie vorliegend – die Auslösung des unautorisierten Zahlungsvorgangs erst durch die grob fahrlässige Weitergabe einer dem Kunden übermittelten TAN erfolgte, die (hier von der Klägerin geltend gemachte) Sorgfaltspflichtverletzung des Zahlungsdienstleisters dem lediglich vorausging. Dies führt nicht zur Annahme einer überholenden Kausalität der Sorgfaltspflichtverletzung des Zahlungsdienstnutzers (so aber OLG Frankfurt, Beschluss vom 22.09.2023 – 3 U 84/23, juris Rn. 22), wenn die geltend gemachte Sorgfaltspflichtverletzung des Zahlungsdienstleisters in dem Sinne als weiterhin kausal für den Schaden anzusehen ist, dass diese die Schadensentstehung durch die spätere Sorgfaltspflichtverletzung des Zahlungsdienstnutzers ermöglicht oder befördert hat. Vorliegend ist aber ein der Beklagten anzulastender Sorgfaltsverstoß nicht festzustellen:

aa. Dass die Umbuchungen vom Tagesgeldkonto der Klägerin auf deren Girokonto ohne die Eingabe einer TAN ermöglicht wurden, begründet keinen Sorgfaltsverstoß der Beklagten. Nach Art. 15 der Delegierten VO 2018/389 darf vielmehr bei Überweisungen zwischen Konten derselben Person, die beim selben Zahlungsdienstleister geführt werden, von den Vorgabe einer starken Kundenauthentifizierung abgesehen werden.

Diese aufsichtsrechtliche Regelung wirkt sich auch zivilrechtlich aus: Ist aufsichtsrechtlich eine Ausnahme von der Pflicht zur Anwendung der starken Kundenauthentifizierung bestimmt, dann begründet die Nichtanwendung dieser Anforderungen keinen Sorgfaltsverstoß des Zahlungsdienstleisters und auch der Anspruchsausschluss nach § 675v Abs. 4 S. 1 Nr. 1 BGB, wonach die Nichtanwendung der starken Kundenauthentifizierung zum Ausschluss von Ansprüchen des Zahlungsdienstleisters nach § 675v Abs. 1 und Abs. 3 BGB führt, findet keine Anwendung (wie hier: Baas/Buck-Heeb/Werner-Böger, Anlegerschutzgesetze, § 675v BGB Rn. 27; Linardatos BKR 2021, 657, 670; Omlor BKR 2019, 105, 113; Schäfer/Omlor/Mimberg-Mimberg, § 1 ZAG Rn. 451; Terlau ZBB/JBB 2016, 122, 132 f.; anders dagegen BeckOGK/Hofmann, Stand 01.09.2022, § 675v BGB Rn. 94; BeckOK/Schmalenbach, Ed. 69, § 675v BGB Rn. 17a; Hoffmann VuR 2016, 243, 248; siehe auch Grüneberg/Grüneberg, 80. Aufl., § 675v BGB Rn. 11). Grundlage dieser Annahme ist der grundsätzliche Gleichklang von Aufsichts- und Zivilrecht im Rechte der Zahlungsdienste (siehe hierzu Baas/Buck-Heeb/Werner-Böger, a.a.O.; Omlor, a.a.O.). Auch soweit diesem Grundsatz hinsichtlich der Heranziehung dieser aufsichtsrechtlichen Ausnahmeregelungen im Rahmen des § 675v Abs. 4 S. 1 BGB entgegengehalten wird, dass der Wortlaut des § 675v Abs. 4 BGB eine solche Einschränkung nicht vorsieht und eine teleologische Reduktion zu Lasten des Zahlungsdienstnutzers nicht zulässig sein soll (so BeckOGK/Hofmann, a.a.O.), gilt dieses Argument wiederum jedenfalls nicht im vorliegenden Kontext der Berücksichtigung eines Sorgfaltsverstoßes im Rahmen des Mitverschuldens nach § 254 BGB.

bb. Soweit die Klägerin weiter das Vorhandensein von Lücken im Sicherheitssystem der Beklagten geltend macht, kann eine solche mangelnde Systemsicherheit grundsätzlich ein anspruchskürzendes Mitverschulden des Zahlungsdienstleisters begründen, wenn das verwendete System nicht dem Stand der Technik entspricht (siehe Ellenberger/Findeisen/Nobbe/Böger-Nobbe, Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 107; MüKo/Zetzsche, 9. Aufl., § 675v BGB Rn. 58). Dass insoweit ein Sorgfaltsverstoß der Beklagten vorliegt kann aber entgegen der Auffassung der Klägerin nicht im Wege eines Anscheinsbeweises allein aus dem Umstand eines tatsächlich erfolgten unbefugten Zugriffes gefolgert werden, da ein solcher auch dann denkbar nicht als ausgeschlossen angesehen werden kann, wenn die Beklagte sämtlichen relevanten Sorgfaltsstandards genügt hat. Dies gilt auch dann, wenn – wie die Klägerin geltend macht – sie weder die PIN noch Zugangskennwörter herausgegeben hat und auch ihr Computer nicht gehackt worden sei. Auch aus dem Umstand der von der Klägerin behaupteten späteren Umstellung des Online-Banking-Systems der Beklagten folgt nicht,

dass das System der Beklagten im Zeitpunkt des Vorfalls nicht den damals maßgeblichen Sicherheitsstandards entsprochen hat; substantiierten Sachvortrag zum geltend gemachten Sicherheitsverstoß lässt die Klägerin im Übrigen vermissen.

cc. Ein zur Annahme eines anspruchskürzenden Mitverschuldens führender Pflichtverstoß der Beklagten könnte allerdings dann anzunehmen sein, wenn die Beklagte bei dem streitgegenständlichen Vorfall Überweisungen über das vereinbarte Tageslimit hinaus zugelassen haben sollte und damit gegen die vereinbarten Betragsobergrenzen nach § 675k Abs. 1 BGB verstoßen haben sollte (vgl. BGH, Urteil vom 29.11.2011 – XI ZR 370/10, juris Rn. 27, WM 2012, 164). Die Erhöhung eines Tageslimits setzt eine Vereinbarung zwischen Zahlungsdienstnutzer und Zahlungsdienstleister voraus, zu deren Voraussetzungen sind dem vorgetragenen Sachverhalt keine genügenden Angaben entnehmen. Da aber nach dem vorgetragenen Sachverhalt bereits vor dem Vorfall ein Tageslimit von EUR 50.000,- vereinbart worden war, welches durch die Überweisungen nicht ausgeschöpft wurde, ist ein diesbezüglicher Pflichtverstoß der Beklagten nicht festzustellen.

dd. Schließlich ergibt sich ein zivilrechtlich relevanter Sorgfaltsverstoß der Beklagten auch nicht daraus, dass bei dem streitgegenständlichen Vorfall in schneller zeitlicher Folge vom Girokonto der Klägerin mehrere Überweisungen über Beträge von jeweils mehr als EUR 9.400,- an unbekannte Dritte ausgeführt wurden und dies obwohl die Klägerin bisher keine Überweisungen über das Online-Banking-System ausgelöst hatte. Zwar konnten diese Umstände in allgemeiner Hinsicht als auffällig und als Indikatoren für einen möglichen missbräuchlichen Kontozugriff angesehen werden. Nach den maßgeblichen europarechtlichen Vorgaben ist im Bereich der elektronischen Zahlungsdiensteabwicklung der Zahlungsdienstleister zur Vorhaltung eines Systems zur Betrugsprävention aber nur zur aufsichtsrechtlichen Überwachung verpflichtet, nicht dagegen zur Überwachung und Vorabkontrolle einzelner Zahlungsvorgänge: Die nach Art. 2 der Delegierten VO 2018/389 vorzuhaltenden Transaktionsüberwachungsmechanismen sind nicht auf eine Echtzeitanalyse einzelner Zahlungsvorgänge gerichtet, durch die im Interesse der betroffenen Zahlungsdienstnutzer gegebenenfalls auffällige Transaktionen vor deren Ausführung zu stoppen wären (so die Auslegung durch die Europäische Bankenaufsichtsbehörde (EBA) in Single Rulebook Q&A, Question ID 2018_4090; ebenso Casper/Terlau-Terlau, 3. Aufl., § 1 ZAG Rn. 520; anders dagegen Linardatos BKR 2021, 665, 675). Systematisch ist dies daraus abzuleiten, dass Art. 2 der Delegierten VO 2018/389 hier von Transaktionsüberwachungsmechanismen

spricht, während in Art. 18 diesen dort in Abs. 1 genannten Mechanismen die Echtzeitanalyse in Abs. 2 Buchst. c) gegenübergestellt wird. Auch insoweit verbleibt es dabei, dass die europarechtlichen aufsichtsrechtlichen Regelungen keine hier die Klägerin schützende Sorgfaltspflicht der Beklagten vorsehen; wiederum ist diese aufsichtsrechtliche Wertung auch für den zivilrechtlichen Sorgfaltsmaßstab heranzuziehen, so dass im Ergebnis ein zur Annahme eines Mitverschuldens führender Sorgfaltsverstoß der Beklagten zu verneinen ist.

3. Der Senat beabsichtigt, gemäß § 522 Abs. 2 ZPO durch Beschluss statt durch Urteil zu entscheiden, da die Rechtssache weder grundsätzliche Bedeutung hat noch die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung durch Urteil erfordern.

Der Klägerin wird Gelegenheit zur Stellungnahme innerhalb der im Tenor genannten Frist gegeben. Es wird darauf hingewiesen, dass bei Rücknahme der Berufung Gerichtsgebühren gespart werden können (Ermäßigung der Gebühr für das Verfahren im Allgemeinen gemäß Nr. 1220, 1222 KV von 4,0 auf 2,0).

gez. Kelle gez. Dr. Böger gez. Kokemohr