AG München, Endurteil v. 08.01.2025 – 271 C 16677/24

Titel:

Kein Erstattungsanspruch eines Bankkunden bei Preisgabe von SMS-Tans an Dritte

Normenkette:

BGB § 675j, § 675l, § 675u, § 675v

Leitsätze:

1. Ein Erstattungsanspruch gemäß § 675u BGB setzt das Vorliegen eines nicht-autorisierten Zahlungsvorgangs voraus. Die Autorisierung fehlt, wenn der Nutzer keine Zustimmung (Einwilligung oder Genehmigung) zu dem Zahlungsvorgang iSd § 675j Abs. 1 S. 1, 2 BGB erteilt hat. Als zustimmende Willenserklärung muss die Autorisierung tatsächlich vom Kunden stammen oder diesem über die Regeln der Stellvertretung zuzurechnen sein (Rn. 27) (Rn. 34) (redaktioneller Leitsatz)

2. Ermöglicht ein Bankkunde durch Preisgabe von SMS-Tans (Freigabecodes) Dritten eine Registrierung eines Geräts, liegt darin eine grob fahrlässige Verletzung der Pflichten aus § 675l Abs. 1 BGB, die eine Haftung der Bank für nicht autorisierte Zahlungsvorgänge ausschließt. (Rn. 35 – 37) (redaktioneller Leitsatz)

3. In der Umsetzung einer Zahlung trotz vorangegangener Sperrung einer Kreditkarte liegt kein Mitverschulden der Bank, wenn nach dem Inhalt der Vereinbarung mit dem Kreditkartenunternehmen eine autorisierte Transaktion nicht angehalten oder storniert werden kann und die Bank ein hinreichend sicheres Authentifizierungssystem implementiert hat. Die Übermittlung der SMS-Tan an eine individuell zugeordnete Mobilfunknummer stellt hinreichend sicher, dass lediglich der Vertragspartner diese SMS-Tan zur Freischaltung der Banking App erhält. (Rn. 38 – 40) (redaktioneller Leitsatz)

Schlagworte:

Kreditkarte, Verbraucherdarlehensvertrag, Authentifizierung, Freigabeverfahren, Banking-App, Online-Bezahlvorgängen, unberechtigte Abbuchungen, 2-Faktor-Authentifizierung, Mitverschulden, Hilfsaufrechnung, Sicherheitsmerkmale, Erstattungsanspruch, Autorisierung, Zahlungsdienstleister, Darlegungs- und Beweislast, Mobiltelefon, grobe Fahrlässigkeit, Kreditkartenunternehmen, sms-Tan

Tenor

1. Die Klage wird abgewiesen.

2. Die Klägerin hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Die Klägerin kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

Tatbestand

1
Die Klägerin begehrt von der Beklagten die Freistellung von unberechtigten Abbuchungen auf ihrer Kreditkarte wegen Internetbetruges.

2
Die Klägerin ist Kundin bei der Beklagten. Sie unterhält dort ein Girokonto mit der Kontonummer … und einer zugehörigen Mastercard mit der KD-Nr. ….

3
Weiterhin schloss die Klägerin mit der Beklagten unter dem 20.01.2020 einen Allgemein-Verbraucherdarlehensvertrag, der von der Fa. M… vermittelt wurde. Dieser Vertrag sah neben einer Erstverfügung die Einräumung eines flexibel von der Klägerin in Anspruch zu nehmenden Kreditrahmens in Höhe von 5.000 € sowie die Überlassung einer Kreditkarte vor. Als Erreichbarkeit gab die Klägerin die Mobilfunknummer … an. Hinsichtlich weiterer Einzelheiten wird auf den als Anlage B1 vorgelegten Vertrag und die als Anlage B 4 vorgelegten Bedingungen verwiesen.

4
Diese sahen insbesondere vor, dass die Authentifizierung des Karteninhabers bei Online-Bezahlvorgängen erfolgt, indem er auf Anforderung die gesondert vereinbarten Authentifizierungselemente einsetzt. Authentifizierungselemente sind Wissenselement (z.B. Online-Passwort), Besitzelemente (z.B. mobiles Endgerät zur Erzeugung und zum Empfang von einmal verwendbaren Transaktionsnummern (TAN) als Besitznachweis oder Seinselemente (z.B. Fingerabdruck) (Anlage B4, dort Buchst. A Zif. III Nr. 3).

5
Zwischen den Parteien wurde das Mastercard 3-D-Secure Verfahren vereinbart. Dieses ist als Besitzelement i.S.d. Teil A Ziff. 3 Nr. 3 der Bedingungen für Zahlungsdienste zu klassifizieren. Als Alternative zur einmal verwendeten TAN kann das Freigabeverfahren per Banking-App vom Kunden aktiviert werden.

6
Am 06.01.2024 wollte der Ehemann der Klägerin über „C…“ eine Reise für sich und seine Ehefrau buchen. Er gab dabei die Kreditkartennummer ein. Kurz darauf erschien eine Mitteilung, dass ein Betrag in Höhe von 318,99 € vorgemerkt sei. In der Folge erschienen weitere Vorankündigungen. Die Klägerin veranlasste daraufhin am Abend telefonisch die Sperrung der Kreditkarte.

7
Am 08.01.2024 erfolgten sechs unberechtigte Abbuchungen zu je 318,99 € für eine Giftcard, insgesamt 1.953,29 €.

8
Zur Autorisierung der streitgegenständlichen Online-Transaktionen fand das Mastercard 3D-Secure-Verfahren Anwendung. Das 3D-Secure Verfahren ist ein Sicherheitsverfahren, das bei Online-Zahlungen zum Einsatz kommt, um die Authentifizierung von Kreditkarten- oder Debitkarteninhabern zu verbessern. Der Begriff „3D“ steht dabei für „Three Domain Secure“ und bezieht sich auf die drei beteiligten Personen: den Karteninhaber, die ausstellende Bank und den Händler. Es ist als „Besitzelement“ i.S.d. Teil A Ziff 3 Nr. 3 der Bedingungen für Zahlungsdienste zu klassifizieren.

9
Bei dem 3D-SecureVerfahren handelt es sich um ein Freigabeverfahren mit 2-Faktor-Authentifizierung, bei dem der Kunde für die Freigabe von Kontoverfügungen eine mobile TAN per SMS oder eine Push-Benachrichtigung über die Banking App auf sein mobiles Endgerät erhält. Hinsichtlich der Einzelheiten wird auf die Ausführungen in der Klagerwiderung vom 09.08.2024 unter Ziff. 2 (Bl. 14 d.A.) verwiesen.

10
Das MasterCard 3D-Secure-Verfahren wurde per Banking-App für die Kreditkarte der Klägerin am 06.01.2024 um 13:30 Uhr aktiviert. Zur Aktivierung dieses Verfahrens auf dem neuen Gerät wurde eine SMS-Tan an die im Vertrag hinterlegte Mobilfunknummer der Klägerin (…) versandt.

11
Die an die der Klägerin zugewiesene Mobilfunknunmmer per SMS versandte SMS-Tan wurde dann auf dem mobilen Endgerät, auf dem die Banking App freigeschaltet wurde, manuell eingegeben und damit die 2-Faktor-Authentifizierung mittels Banking-App am 06.01.2024 um 13:30 Uhr freigegeben und aktiviert. Hinsichtlich der Einzelheiten wird auf die Ausführungen in der Klagerwiderung vom 09.08.2024 unter Ziff. 3 verwiesen (Bl. 14 d.A.) verwiesen.

12
8 Minuten nach der Aktivierung des 3D-Secure-Verfahrens, also am 06.01.2024 um 13:38 Uhr kam es zu der ersten streitgegenständlichen Vergütung, die online veranlasst und durch die Banking App als zweiten Faktor freigegeben wurde. Die anderen Transaktionen erfolgten in den darauffolgenden zwei Stunden. Hinsichtlich der Einzelheiten wird auf die Ausführungen in der Klagerwiderung vom 09.08.2024 unter Ziff. 4 (Bl. 15 d.A.) verwiesen.

13
Am 14.01.2024 reklamierte die Klägerin mittels Reklamationsformular die Umsätze bei der Beklagten. In diesem Formular gab sie an, die Kreditkartendaten samt Gültigkeitsdauer und Prüfziffer auf der

vermeintlichen „C…“-Seite eingegeben zu haben. Hinsichtlich der Einzelheiten wird auf die Anlage B2 verwiesen.

14
Mit anwaltlichem Schreiben vom 09.02.2024 forderte die Klägerin die Beklagte auf, den abgebuchten Betrag zurückzuerstatten. Hinsichtlich der Einzelheiten wird auf das als Anlage K1 vorgelegte Schreiben verwiesen.

15
Die Klägerin trägt vor und meint,

weder sie selbst noch ihr Ehemann hätten die Abbuchungen über insgesamt 1.953,29 € autorisiert und keine Berechtigung erteilt. Auch sei im Zuge der Buchung keine PIN und kein Passwort eingegeben worden. Insbesondere habe sie nicht am 06.01.2024 um 13:30 Uhr das smsTAN-Verfahren aktiviert und dies sei nicht über ihr Mobiltelefon gegangen. Gegen eine Weitergabe der auf SMS-Tan vom 06.01.2024 13:44 Uhr spreche die Umsatzbenachrichtigung vom 06.01.2024, wonach bereits um 13:38 Uhr, somit sechs Minuten vor Übersendung der SMS an die Klägerin ein Betrag von 0,01 € abgebucht worden sei (Anlagen K3-K5). Die smsTAN habe sie nie auf der Website eingegeben und zuvor nie auf diese Art und Weise bezahlt. Für sie hätten sich keine Zweifel an der Echtheit der Website ergeben. Eine 2-Faktor-Authentifizierung habe nicht stattgefunden. Es sei ihr nicht möglich gewesen, den Betrug zu erkennen. Von gefälschten Reiseportalen habe die Klägerin bis zu diesem Zeitpunkt nichts gewusst. Sie habe dies auch nicht durch Rundfunk/Medien mitbekommen. Sie habe die Daten nicht bewusst an Dritte weitergegeben. Die Beklagte habe spätestens nach der zweiten Zahlung im Rahmen der Betrugsprävention die Abbuchung als auffällige Zahlung erkennen können und diese möglichst umgehend einstellen müssen. Es stelle eine erhebliche Sorgfaltspflichtverletzung der Beklagtenseite dar, dass eine Beschränkung auf eine einmalige Installation und Koppelung mit dem Konto nicht erfolge. Die Beklagte müsse sicherstellen, dass die Banking App für ein Konto jeweils nur auf einem Mobilgerät installiert werden könne. Dies sei gängige Praxis bei anderen Bankinstituten. Die Authentifizierung durch mobile TAN sei nicht durch die Beantwortung der Sicherheitsabfrage erfolgt. Eine TAN könne auch nur für eine Abbuchung und nicht für sechs Abbuchungen benutzt werden. Da die Kartensperrung bereits am 06.01.2024 erfolgt sei, hätte die Auszahlung vom 08.01.2024 nicht erfolgen dürfen. Aufgrund der umgehenden Sperrung sei nicht gegen Pflichten gemäß § 675 l BGB verstoßen worden. Da die Beklagte die Stornierung der Zahlungsvorgänge unterlassen habe, sei ihr ein erhebliches Mitverschulden zuzurechnen.

16
Die Klägerin beantragt,

1.1. die Beklagte zu verurteilen, an sie 1.953,29 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz gemäß § 247 BGB seit dem 24.02.2024 zu zahlen,
Hilfsweise die Beklagte zu verurteilen, sie in Höhe von eines Betrages von 1.953,29 € nebst Zinsen hieraus in Höhe von 5 %-Punkten über dem Basiszinssatz gemäß § 247 BGB seit dem 24.02.2024 freizustellen und diesen Betrag auf das Konto der Klägerin gutzuschreiben.

2. die Beklagte zu verurteilen, an sie weitere 280,60 € an außergerichtlichen Rechtsanwaltskosten seit Rechtshängigkeit zu zahlen.

17
Die Beklagte beantragt,

die Klage abzuweisen.

18
Die Beklagte trägt vor und meint,

die streitgegenständliche Verfügung sei mittels 2-Faktor-Authentifizierung autorisiert worden. Jedenfalls sei die Klägerin der Beklagten aufgrund grob fahrlässiger Pflichtverletzung gemäß § 675v Abs. 3 Nr. 2 BGB zum Ersatz des Schadens verpflichtet. Hinsichtlich eines entsprechenden Schadensersatzanspruchs erklärte die Beklagte die Hilfsaufrechnung.

19

Aufgrund der manuellen Eingabe einer an die Mobilfunknummer der Klägerin versandten SMS-Tan sei ein Fremdzugriff technisch ausgeschlossen. Es sei daher davon auszugehen, dass die Klägerin die Banking App selbst installiert habe oder durch Preisgabe der SMS-Tan Dritten eine Registrierung eines Geräts ermöglicht habe, wobei die Preisgabe persönlicher Sicherheitsmerkmale an Dritte gemäß der vertraglichen Bestimmungen untersagt gewesen sei. Es liege nahe, dass die Klägerin einem gefälschten Reiseportal zum Opfer gefallen sei. Eine Zahlung an C… habe ausweislich der Systeme der Beklagten nicht stattgefunden. Stattdessen sei ein neues Gerät im Online-Banking der Klägerin als Freigabeinstrument im Rahmen des 2-Faktor-Authentifizierungsverfahrens hinterlegt worden. Hierzu sei – technisch zwingend – die Eingabe der SMS-Tan erforderlich gewesen. Die Klägerin habe keine Reise gebucht, sondern Giftcards von einem in den Niederlanden (Amsterdam) ansässigen Unternehmen, Co…, erworben.

20
Weiterhin sei davon auszugehen, dass die Klägerin auf der betrügerischen Website auch aufgefordert worden sei, eine SMS-Tan einzugeben. Dafür spreche, dass an die Klägerin gemäß der Aufzeichnungen der Beklagten am Tag der streitgegenständlichen Transaktionen um 13:29 Uhr eine SMS-Tan zur Aktivierung des 3D-Secure-Verfahrens gesendet worden sei. Der Zeitpunkt ergebe sich aus der Anlage B6. Diese muss die Klägerin sodann tatsächlich auf der betrügerischen Website eingegeben haben. Die Weitergabe von Authentifizierungselementen sei selbstredend und auch gemäß der Vertragsbedingungen untersagt. Die Beklagte habe hinreichende Sicherheitsmechanismen (2-Faktor-Identifizierung bzw. 3D-Secure-Verfahren) zur Verfügung gestellt, um Missbrauch zu vermeiden.

21
Es liege kein Mitverschulden der Beklagten vor. Bei einer Mastercard würde sich die Stornierung bereits getätigter Transaktionen (so genannter Chargebacks) nach dem Mastercard Chargeback Guide richten. Der Mastercard Chargeback Guide sehe vor, dass Transaktionen, die wie die vorliegenden Transaktionen per Mastercard 3D-Secure-Verfahren (bzw. auch Mastercard Identity Check genannt) freigegeben wurden, nicht mehr gestoppt bzw. zurückgeholt werden können. Hinsichtlich der Einzelheiten wird auf das als Anlage B3 vorgelegte Dokument und Bl. 36 d.A. verwiesen.

22
Hinsichtlich weiterer Einzelheiten wird auf die Schriftsätze vom 06.05.2024 (Bl. 1-4 d.A.), 03.07.2024 (Bl. 7 d.A.), 09.08.2024 (Bl. 12-19 d.A.), 26.08.2024 (Bl. 21-22 d.A.), 20.09.2024 (Bl. 34-37 d.A.) samt Anlagen und das Protokoll des Güte- und Haupttermins vom 02.10.2024 sowie die weiteren Schriftsätze vom 15.10.2024 (Bl. 52/53 d.A.), 21.11.2024 (Bl. 62/66 sowie Bl. 67/68 d.A.), 04.12.2024 (Bl. 62/66 d.A.), 05.12.2024 (Bl. 74/75 d.A.), 17.12.2024 (Bl 79/80 d.A.) samt Anlagen verwiesen.

23
Das Gericht hat Beweis erhoben durch Einvernahme des Zeugen Be… H…, des Ehemanns der Klägerin, und durch informatorische Anhörung der Klägerin.

24
Die Beteiligten haben Ihr Einverständnis mit einer Entscheidung im schriftlichen Verfahren gemäß § 128 Abs. 2 ZPO erklärt

Entscheidungsgründe

A.

25
Die zulässige Klage erweist sich als unbegründet.

26
1. Die Klägerin kann keinen Erstattungsanspruch gemäß § 675u BGB gegenüber der Beklagten geltend machen, da sie nach Überzeugung des Gerichts die verfahrensgegenständliche Transaktion maßgeblich selbst zu verantworten hat. Die Beklagte verfügt damit jedenfalls über einen Schadenersatzanspruch in nämlicher Höhe gegenüber der Klägerin, mit dem sie erfolgreich die Aufrechnung erklärt hat.

27
a) Für einen Erstattungsanspruch gemäß § 675 u BGB ist das Vorliegen eines nicht-autorisierten Zahlungsvorgangs Voraussetzung. Die Autorisierung fehlt, wenn der Nutzer keine Zustimmung (Einwilligung

oder Genehmigung) zu dem Zahlungsvorgang i.S.d. § 675j Abs. 1 Satz 1, 2 BGB erteilt hat (MüKo BGB 9. Aufl. 2023, § 675u BGB Rn. 10). Die Art und Weise der Zustimmung sind zwischen Zahler und Zahlungsdienstleister zu vereinbaren (§ 675j Abs. 1 Satz 2 und 3 BGB). Die Darlegungs- und Beweislast trifft grundsätzlich die Beklagte (BGH Urteil vom 05.03.2024, Az.: XI ZR 107/22).

28
Das Gericht geht aufgrund der Angaben beider Parteien sowie des Zeugen H… und dem in Augenschein genommenen Mobiltelefon der Klägerin von dem folgenden Geschehensablauf aus:

29
Der Zeuge H… hat am 06.01.2024 zunächst die Kreditkartendaten auf einer Fake-C…-Seite angegeben, wobei er sich nicht mit einem Benutzerkonto eingeloggt hat.

30
Der Vortrag der Beklagten, dass diese in ihren Systemen feststellen konnte, dass das Mastercard 3D-Secure Verfahren per Banking App für die Kreditkarte der Klägerin am 06.01.2024 um 13:30 Uhr aktiviert wurde, und zur Aktivierung dieses Verfahrens auf dem neuen Gerät eine SMS-TAN an die im Vertrag hinterlegte Mobilfunknummer der Klägerin (…) versandt wurde,, wurde durch Inaugenscheinnahme des Mobiltelefons der Klägerin bestätigt. Dort befindet sich, wie protokolliert, eine SMS vom 06.01.2024 13:29 Uhr mit dem Inhalt: „… ist Ihre TAN für die Aktivierung von Mastercard Identity Check vom 06.01.2024 13:44 Uhr.“ Der Eingang der SMS um 13:29 Uhr war im eingesehenen Nachrichtenverlauf wie protokolliert um 13:29 Uhr dokumentiert und wird auch durch das als Anlage B6 vorgelegte IT-Protokoll belegt. Der Vortrag der Klägerin, keine SMS-TAN erhalten zu haben und dass ihr Mobiltelefon nicht in die Freigabe involviert war, erwies sich damit als widerlegt.

31
Die Beklagte hat unbestritten vorgetragen, dass aufgrund der manuellen Eingabe einer an die Mobilfunknummer der Klägerin versandten SMS-Tan ein Fremdzugriff technisch ausgeschlossen ist. Es wurde ein neues Gerät im Online-Banking der Klägerin als Freigabeinstrument im Rahmen des 2-Faktor-Authentifizierungsverfahrens hinterlegt. Hierzu war – technisch zwingend – die Eingabe der SMS-Tan erforderlich. Die Klägerin buchte keine Reise, sondern erwarb Giftcards von einem in den Niederlanden (Amsterdam) ansässigen Unternehmen, ….

32
Das Gericht ist daher davon überzeugt, dass die Klägerin durch Preisgabe der SMS-Tan Dritten eine Registrierung eines Geräts ermöglicht hat, wobei die Preisgabe persönlicher Sicherheitsmerkmale an Dritte gemäß der vertraglichen Bestimmungen untersagt war.

33
Dabei muss der Richter persönlich subjektiv voll von der Wahrheit der behaupteten Tatsache überzeugt sein. Er darf und muss sich in tatsächlich zweifelhaften Fällen mit einem für das praktische Leben brauchbaren Grad von Gewissheit begnügen, der den Zweifeln Schweigen gebietet, ohne sie völlig auszuschließen (stRspr. BGH NJW 2018, 3513, Rn. 34). Das Gericht berücksichtigte in diesem Zusammenhang, dass die Klägerin nach eigenen Angaben auch keine smsTAN erhalten hat, was sich als widerlegt herausstellte.

34
Das Gericht ist davon überzeugt, dass es zwar keine wirksame Autorisierung für die streitgegenständliche Zahlung gegeben hat. Zwar lag bei einer technischen Betrachtung und aus der ex-ante Sicht der Beklagten eine solche Autorisierung (durch die Banking App) vor. Diese war aber nicht wirksam, da sie der Klägerin nicht zugerechnet werden kann. Die sogenannte Autorisierung als zustimmende Willenserklärung gemäß § 675j BGB muss tatsächlich vom Kunden stammen oder diesem über die Regeln der Stellvertretung zuzurechnen sein. Eine Vollmacht der Klägerin zugunsten der unbekannt gebliebenen Täter kann ausgeschlossen werden. Danach lag zwar eine technisch nicht zu beanstandende Autorisierung vor, die aber indessen nicht von der Klägerin stammte.

35
b) Die Beklagte haftet dennoch nicht für den streitgegenständlichen Zahlungsvorgang. Denn die Klägerin hat in grob fahrlässiger Weise gegen die gesetzliche Vorgabe in § 675v Abs. 3 Nr. 2 a) BGB in Verbindung mit § 675 l Abs. 1 BGB verstoßen. Bei dem sogenannten SMS-Tans (Freigabecodes) handelt es sich um

personalisierte Sicherheitsmerkmale im Sinne dieser Vorschriften. Die Klägerin hat ein solches Merkmal zur Überzeugung des Gerichts aus nicht nachvollziehbaren Gründen dritten Personen zugänglich gemacht. Freigabecodes dürfen ausschließlich dem Zahlungsdienstleister im Rahmen der vorgesehenen Prozesse offenbart werden und keinen dritten Personen.

36
Das Verhalten der Klägerin bewertet das Gericht als grob fahrlässig. Es ist eine Sache, wenn man seine Kreditkartendaten offenbart. Diese werden bei jeder Verwendung offenbart und können auch von der Karte abgelesen werden. Im Übrigen sind derartige Datensets in geradezu beliebiger Menge im sogenannten „D.“ verfügbar und werden dort gehandelt. Die Weitergabe eines im Rahmen einer Zwei-Faktor-Autorisierung erhaltenden Zugangscodes kann nicht damit gleichgesetzt werden. Mit dieser Weitergabe hilft der Nutzer (Kläger) die Sicherheitsarchitektur grundlegend auszuhebeln. Es muss jedem verständigen Nutzer solcher Kreditkarten klar sein, welches Risiko er mit der Weitergabe derartiger Daten schafft. Die Klägerin mag dies nicht bewusst getan haben und es mag ihm auch nicht erinnerlich sein. Indessen lässt sich der Vorgang plausibel nicht anders erklären. Die Weitergabe eines Verifizierungscodes an eine andere Person oder die Eingabe eines solches Codes auf einer Internetpräsenz, die nicht der Bank des Nutzers zugeordnet werden kann, verbietet sich von selbst.

37
In den letzten Jahren wurden vielfach durch verschiedene Medien Fälle von betrügerischen Vorgängen bekannt. Die Klägerin musste daher von der Möglichkeit solcher betrügerischer Vorgänge, wenn auch in unterschiedlicher Ausgestaltung, jedenfalls allgemeine Kenntnis haben. Falls nicht, wäre dies zumindest als grob fahrlässige Unkenntnis einzustufen (vgl. OLG München, Hinweisbeschluss vom 22.09.2022, 19 U 2204/22, BeckRS 2022, 36075 Rn. 68, beck-Online). Hinsichtlich der Gesamtumstände ist ferner zu berücksichtigen, dass der Zeuge H…, wie im Termin vom 02.10.2024 angegeben, sich vor Eingabe der Kreditkartendaten nicht auf der vermeintlichen … – Seite einloggte, was eine erhebliche Abweichung von einem regulären Buchungs- und Bezahlvorgang darstellt.

38
c) Ein Mitverschulden der Beklagten aufgrund Umsetzung der Zahlung trotz vorangegangener Sperrung kommt nicht in Betracht.

39
aa) Die Beklagte hat unter Vorlage der entsprechenden Unterlagen zu den vertraglichen Vereinbarungen mit dem Kreditkartenunternehmen unbestritten vortragen. Nach dem Inhalt dieser Vereinbarung kann eine autorisierte Transaktion seitens der Beklagten nicht angehalten oder storniert werden. Die streitgegenständliche Transaktion war wie vertraglich vorgesehen autorisiert. Ein Zurückholen der Transaktion war der Beklagten daher aus vertraglichen Gründen nicht möglich. Eine Verletzung des mit dem Kläger bestehenden Dienstleistungsvertrags kann der Beklagten daher insoweit nicht vorgeworfen werden. Die Einholung eines Sachverständigengutachtens war vor diesem Hintergrund nicht erforderlich.

40
bb) Soweit die Klageseite rügte, dass die Beklagte ein nicht hinreichend sicheres Authentifizierungssystem implementiert habe, war auch insoweit keine Einholung eines Sachverständigengutachtens veranlasst. Denn die Authentifizierung erfolgte gemäß der zwischen den Parteien vereinbarten Regelungen. Darüber hinaus erfolgt durch die Übermittlung der smsTAN an eine individuell zugeordnete Mobilfunknummer eine hinreichende Sicherstellung, dass lediglich der Vertragspartner diese smsTAN zur Freischaltung der Banking App erhält. Dass dann mit der Banking-App Transaktionen freigegeben werden können, ist durch den vorangegangenen Identity Check gerechtfertigt.

41
2. Die Nebenforderungen teilen das Schicksal der Hauptforderung.

B.

42
Die Kostenfolge bestimmt sich aus § 91 Abs. 1 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit aus §§ 708 Nr. 11, 711 ZPO. Der Streitwert wurde gemäß § 3 ZPO bestimmt.