Landgericht Mönchengladbach, 3 O 35/23

Datum:	23.04.2024
Gericht:	Landgericht Mönchengladbach
Spruchkörper:	3. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	3 O 35/23
ECLI:	ECLI:DE:LGMG:2024:0423.3O35.23.00

Rechtskraft: rechtskräftig

Tenor:

1. Die Klage wird abgewiesen.

2. Die Kosten des Rechtsstreits werden dem Kläger auferlegt.

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

Tatbestand: 1

Die Parteien streiten um die Rückbuchung von Belastungen betreffend mehrere bei der Beklagten geführte Konten des Klägers. 2

Der Kläger unterhält bei der Beklagten ein privat geführtes Girokonto mit der Kontonummer und ein Tagesgeldkonto unter der Kontonummer, jeweils unter Nutzung des Online-Bankings. Für diese Konten war ein Tages-Verfügungslimit von EUR vereinbart. Zudem gab die Beklagte für den Kläger eine Kreditkarte mit der Nummer aus. 3

Jeweils am und mit Wertstellung vom wurden Echtzeit-Überweisungen vom genannten Girokonto im Umfang EUR auf das Konto einer von dem genannten Tagesgeldkonto im Umfang von EUR auf dasselbe Konto und im Umfang von EUR auf das Konto vorgenommen. Zudem wurde am die angegebene Kreditkarte des Klägers mit Zahlungen von EUR belastet. Eine weitere Überweisung an das Konto eines vom Girokonto des Klägers im Umfang von EUR erfolgte ebenfalls am, wurde aber von der Bank des Zahlungsempfängers nicht akzeptiert und zurückgebucht. 4

5

Die genannten Überweisungen beruhten auf Aufträgen, die im Wege des Online-Bankings mittels der App unter Nutzung des Zugriffs des Klägers vorgenommen wurden.

Die Beklagte hat für die Nutzung des Online-Bankings unter anderem folgende AGB eingeführt: 6

„7. Sorgfaltspflichten des Teilnehmers 7.1 Schutz der Authentifizierungselemente 7

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. 8

[…] 9

(b) Besitzelemente, wie z.B. ein mobiles Endgerät sind vor Missbrauch zu schützen, insbesondere, 10

[…] dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon für die Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.“ 11

In diesem Punkt wortlautgleiche AGB hat die Beklagte auch für die Nutzung der von ihr ausgegebenen Kreditkarten eingeführt. 12

Zur Durchführung einer Überweisung mittels Online-Bankings muss sich der Kunde der Beklagten zunächst mit seinen Online-Banking-Zugangsdaten, d. h. dem Nutzernamen und der dazugehörigen Online-Banking-PIN, die nur ihm bekannt sind, im Online-Banking anmelden. Dort gibt er eine Überweisung in Auftrag. Hierzu ist auf dem mobilen Endgerät des Online-Banking-Teilnehmers eine App, die so genannte App, installiert und freigeschaltet. 13

Auf der Website der Beklagten warnt diese vor so genannten Phishing-Attacken. 14

Am Uhr wurde der Zugangsname für das Online-Banking des Klägers auf die E-Mail-Adresse "…“ geändert und mit einer SMS bestätigt. In der Folge wurde eine Rücksetzung des Passworts für den Zugang des Klägers angefordert und zu dieser E-Mail-Adresse ein entsprechender Link automatisiert gesendet, mit dem das Passwort geändert wurde. 15

Im Anschluss wurde am um Uhr die App auf einem anderen Mobiltelefon als dem bisher vom Kläger genutzten installiert und unter Nutzung des von der Beklagten an die genannte E-Mail-Adresse übersandten Passworts sowie der App die genannten Überweisungen und Belastungen der Kreditkarte autorisiert (vgl. insoweit die Activitylogs, vorgelegt von der Beklagten als Anl... 16

Der Kläger bemerkte die durchgeführten Überweisungen am Nachmittag des. Der Kläger stellte am selben Tag Strafanzeige gegen Unbekannt. 17

Die späteren Prozessbevollmächtigten des Klägers forderte daraufhin mit Schreiben vom unter Fristsetzung bis zum die Beklagte zur valutagerechten Wiedergutschrift der streitgegenständlichen Beträge auf dem Konto des Klägers sowie zur Erstattung der 18

vorgerichtlichen Rechtsanwaltskosten auf, was erfolglos blieb.

Der Kläger behauptet folgenden Hintergrund der Abbuchungen: 19

Die Angabe der E-Mail-Adresse und Anforderung des Passworts sei aufgrund eines Anrufs erfolgt, den der Kläger am Uhr erhalten habe und zu welchem auf dem Display eine der Beklagten zugeordnete Telefonnummer angezeigt worden sei. Der Anrufer habe sich wahrheitswidrig als Mitarbeiter der Beklagten ausgegeben. Aufgrund der angezeigten Telefonnummer, die der Kläger zur Bestätigung zurückgerufen habe und dabei in einer Warteschleife der Beklagten gelandet sei, habe der Kläger dem Anrufer geglaubt, als er daraufhin ein zweites Mal angerufen habe. Der vermeintliche Mitarbeiter der Beklagten habe berichtet, dass eine unautorisierte Überweisung vom Konto des Klägers erfolgt sei. Der Kläger habe dann im Online-Banking die Überweisung an ..gesehen. Der vermeintliche Mitarbeiter der Beklagten habe daraufhin den Kläger aufgefordert, ihm E-Mails und SMS von der Beklagten zu übersenden; der Kläger sei dem nachgekommen, wobei er keine Angaben dazu macht, an welche Adresse diese Übersendungen erfolgten. 20

Der Kläger behauptet weiter, dass die Überweisungsaufträge zu den genannten Überweisungen, die am wertgestellt wurden, unautorisiert erfolgt seien. 21

Der Kläger ist der Ansicht, dass die Beklagte zur Zurückbuchung der genannten Überweisungen und damit zur Wertstellung als wären diese nie vorgenommen verpflichtet sei. 22

Er behauptet, dass die Beklagte ein unzureichendes und lückenhaftes Sicherungssystem für das Online-Banking unterhalte, was jedenfalls dadurch deutlich sei, dass Beauftragungen und deren Bestätigungen von ein und demselben Mobilgerät erfolgen könnten. Im Übrigen werde die Unsicherheit noch dadurch vergrößert, dass die Beklagte anders als banküblich unmittelbare Überweisungen von einem Tagesgeldkonto auf Fremdkonten zulasse. 23

Eine Haftung des Klägers, der weder Zugangsdaten noch eine PIN unerlaubt weitergegeben habe, scheide nach seiner Ansicht aus. 24

Der Kläger beantragt, 25

1. die Beklagte zu verurteilen, das bei ihr geführte Girokonto mit der Nr. auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch den nicht autorisierten Zahlungsvorgang vom in Höhe von EUR befunden hätte; 26

2. die Beklagte zu verurteilen, das bei ihr geführte Tagesgeldkonto mit der Nr. auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge vom in Höhe von EUR und EUR befunden hätte. 27

3. die Beklagte zu verurteilen, das bei ihr geführte Kreditkartenkonto mit der Nr. auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge vom in Höhe von EUR und EUR befunden hätte. 28

4. die Beklagte zu verurteilen, an ihn vorgerichtliche Rechtsanwaltsgebühren in Höhe von EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem Zeitpunkt der Rechtshängigkeit zu zahlen. 29

Die Beklagte beantragt, 30

31

die Klage abzuweisen.

Die Beklagte bestreitet die Behauptungen des Klägers zu den Hintergründen der Überweisungen und Belastungen mit Nichtwissen. Ein Anspruch aus § 675u BGB des Klägers bestehe nicht. Insoweit bestehe ein Anscheinsbeweis, dass die Überweisungen ordnungsgemäß autorisiert seien. 32

Die Beklagte ist der Ansicht, dass der Kläger grob fahrlässig gegen seine Sorgfaltspflichten hinsichtlich der personalisierten Sicherheitsmerkmale, insbesondere solche aus Ziff. 7 der genannten AGB, verstoßen habe. 33

Hilfsweise erklärt die Beklagte mit einem Schadensersatzanspruch gegen den Kläger aus § 675v Abs. 3 Nr. 2 BGB in Höhe der Klagesumme die Aufrechnung. 34

Die Klageschrift ist der Beklagten am zugestellt worden. 35

Entscheidungsgründe: 36

Die Klage ist zulässig, aber unbegründet. 37

Dem Kläger steht gegen die Beklagte kein Anspruch auf Wiedergutschrift von insgesamt EUR entsprechend den gestellten Klageanträgen auf sein bei der Beklagten geführtes Girokonto und Tagesgeldkonto bzw. das Kreditkartenkonto gemäß § 675u S. 2 BGB zu. 38

Nach der genannten Vorschrift ist der Zahlungsdienstleister im Falle eines nicht autorisierten Zahlungsvorgangs, durch welchen ein Betrag einem Zahlungskonto belastet worden ist, verpflichtet, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. 39

Ein Zahlungsvorgang ist dabei gemäß § 675f Abs. 4 BGB jede Bereitstellung, Übermittlung oder Abhebung eines Geldbetrags, unabhängig von der zugrundeliegenden Rechtsbeziehung zwischen Zahler und Zahlungsempfänger. Zahlungsauftrag ist jeder Auftrag, den ein Zahler seinem Zahlungsdienstleister zur Ausführung eines Zahlungsvorgangs entweder unmittelbar oder mittelbar über einen Zahlungsauslösedienstleister oder den Zahlungsempfänger erteilt. Im vorliegenden Fall handelte es sich um die Übermittlung diverser Geldbeträge vom Girokonto und Tagesgeldkonto des Klägers sowie Belastungen seines Kreditkartenkontos in einem Umfang von insgesamt EUR, die am und erfolgten. 40

Dabei scheitert eine Autorisierung im vorliegenden Fall nicht schon daran, dass ein mit dem Kläger vereinbarten Tages-Verfügungslimit überschritten worden wäre. Denn dieses Limit wurde durch die Überweisungen nicht überschritten, da von keinem Konto des Klägers an einem Tag über mehr als die vereinbarten 10.000,00 EUR verfügt wurde. Vielmehr wurde am der Betrag von EUR vom Tagesgeldkonto überwiesen, am darüber hinaus die Beträge von EUR vom Girokonto und von weitere EUR vom Tagesgeldkonto. Die Belastungen des Kreditkartenkontos wiederum werden erst mit dem Ende des Abrechnungszeitraums der Kreditkarte zur Ausgleichung fällig, sodass auf sie die Tagesverfügungsgrenzen keine Anwendung finden. 41

Im Ergebnis kann allerdings die zwischen den Parteien streitige Frage, ob die genannten Belastungen im Sinne von § 675j Abs. 1 BGB autorisiert sind, dahinstehen. Denn einem möglichen Anspruch des Klägers steht der Einwand unzulässiger Rechtsausübung gemäß § 242 BGB („dolo agit“) entgegen, worauf sich die Beklagte im Hinblick auf die Geltendmachung eines Gegenanspruchs aus § 675v Abs. 3 BGB im Wege der 42

Hilfsaufrechnung zumindest konkludent beruft, da der Beklagten gegen den Kläger bei Bestehen eines Erstattungsanspruchs aus § 675u S. 2 BGB ein Schadensersatzspruch in gleicher Höhe jedenfalls gemäß § 675v Abs. 3 Nr. 2 a) u. b) BGB zustehen würde (vgl. BGH, Urt. v. 17.11.2020, XI ZR 294/19, zit. n. BeckRS 2020, 38721, Tz. 44).

Der Kläger hat nämlich den ihm entstandenen Schaden durch grob fahrlässige Verletzung von mehreren Pflichten gemäß § 675l Abs. 1 BGB und der vereinbarten Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments herbeigeführt . 43

Grob fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt in ungewöhnlich krassem Maße verletzt und unter Berücksichtigung der subjektiven Erfahrung des jeweils Handelnden auch ganz naheliegende Überlegungen nicht anstellt oder das nicht beachtet, was im konkreten Fall jedem hätte ohne Weiteres einleuchten müssen. 44

Bei der missbräuchlichen Nutzung von Online-Banking, gleich ob mit PIN und TAN gesichert oder wie hier durch Nutzung einer App, durch einen Dritten ist zu beachten, dass im Rahmen des Online-Bankings nicht per se ein Anscheinsbeweis für eine grobe Fahrlässigkeit des Kontoinhabers besteht. Insbesondere genügt ohne Hinzutreten weiterer Umstände hierfür nicht die Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die Prüfung der Authentifizierung nach § 675w S. 3 Nr. 4 BGB (vgl. BGH, Urt. v. 26.01.2016, XI ZR 91/14, zit. n. juris). Es müssen in einem solchen Fall vielmehr konkrete Umstände hinzutreten, die einen objektiv groben Pflichtverstoß begründen. 45

Nach § 675l Abs. 1 S. 1 BGB ist der Zahler verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugten Zugriffen zu schützen. Gegen die Pflicht verstieß der Kläger, da er Zugriffsmöglichkeiten zum Online-Banking, das mit den streitgegenständlichen Konten verbunden war, weitergab. 46

Von einem derartigen Verstoß gegen die Pflichten des Klägers geht die Kammer nach dem Inhalt der mündlichen Verhandlung, namentlich nach der persönlichen Anhörung des Klägers im Termin vom, aus. Auch nach dieser blieb der Vortrag des Klägers in wesentlichen Punkten lückenhaft. Insoweit besteht für den Kläger, der sich auf besondere Umstände beruft, nämlich einen betrügerischen Anruf von einem vermeintlichen Mitarbeiter der Beklagten, eine sekundäre Darlegungslast dahingehend, den Inhalt des Gesprächs, bei dem der Gesprächspartner nachvollziehbar es auf persönliche Daten und Zugänge des Klägers abgesehen hat und bei dem daher ein besonderes Risiko des Bekanntwerdens von Sicherheitsmerkmalen des Klägers bestand, in sich schlüssig darzulegen. Dem ist der Kläger – worauf die Kammer bereits im Termin hingewiesen hat – nicht nachgekommen. Sein Vortrag zum Gesprächsablauf ist lückenhaft und nicht nachvollziehbar und lässt sich im Übrigen nicht mit den technischen Vorgängen des Online-Bankings, wie sie sich aus dem von der Beklagten vorgelegten automatisierten Aufzeichnungen im Activitylog ergeben, überein bringen. 47

Denn der Kläger hat nach seinem eigenen Vortrag keine Zurücksetzung des Passworts für das Online-Banking angefordert. Allerdings geht eine solche um Uhr am aus dem Activitylog hervor. Dies bewirkt eine automatisierte Sendung eines Rücksetzungslinks an die hinterlegte E-Mail-Adresse des Klägers. Es erscheint daher nicht nachvollziehbar, dass der Kläger angibt, eine solche nicht erhalten zu haben. Dagegen trägt der Kläger vor, dass er auf Bitten des Anrufers eine "Identifizierungs-E-Mail" sowie eine mit der IBAN an eine vom Anrufer bestimmte E-Mail-Adresse geschickt habe. Welchen Charakter diese E-Mail-Adresse hatte, insbesondere ob sie dem äußeren Anschein nach einer Domain der Beklagten zugehörig erschien, kann nicht festgestellt werden, da der Kläger insoweit die Adresse wie auch den 48

genauen Inhalt dieser E-Mails nicht vorgetragen hat. Insoweit erscheint nicht nachvollziehbar, dass dem Kläger diese E-Mails, die er selbst versendet haben will, nicht mehr vorliegen, zumal gerade deren Sicherung wegen des offensichtlichen Beweiswertes nahegelegen hätte. Der Kläger kommt insoweit seiner sekundären Darlegungslast nicht nach.

Mangels eines hinreichenden Vortrags des Klägers legt die Kammer daher den Beklagtenvortrag zugrunde, der sich im Übrigen auch ohne Weiteres mit dem Activitylog übereinbringen lässt, wonach der Kläger dem Anrufer auf dessen Bitte eine E-Mail mit dem Link zur Zurücksetzung seines Passwortes weitergesandt hat. 49

Auch nach seinem eigenen Vortrag hat der Kläger jedenfalls den Inhalt dieser Nachricht der Beklagten an die ihm vom Anrufer genannte Adresse weitergegeben. Der Kläger gab durch die Weiterleitung zugleich seine E-Mail-Adresse, die er bei der Beklagten hinterlegt hatte, weiter. Der Empfänger der Nachricht hatte somit neben der als Benutzernamen fungierenden E-Mail-Adresse des Klägers alle Möglichkeiten, das Passwort für das Online-Banking-Konto des Klägers zurückzusetzen, was funktional der Weitergabe des Passworts selbst gleichkommt. 50

Der Kläger hat auch angegeben, dass er auf Geheiß des Anrufers mindestens zwei ihm zuvor auf seine Handynummer geschickte SMS-Nachrichten an eine vom Anrufer angegebene Nummer weitergeleitet habe. Soweit der Kläger angegeben hat, dass diese Nachrichten "keinen wesentlichen Inhalt" gehabt hätten, erscheint das schon objektiv nicht nachvollziehbar, da weder eine automatisierte Sendung von inhaltslosen Nachrichten noch vor allem das Interesse des Anrufers an einer Weiterleitung derselben nachvollziehbar ist. Eine Version dieser Nachrichten, die auch auf seinem Mobilfunkgerät gespeichert worden sein müssen, legt der Kläger wiederum nicht vor. Auch insoweit genügt sein Vortrag nicht an den Anforderungen an eine sekundäre Darlegung, die zumindest nachvollziehbar ist. 51

Dagegen ergibt sich aus dem Activitylog, dass tatsächlich mindestens zwei SMS mit Bestätigungs-TANs („OTP“ = „One Time Password“) automatisiert von der Beklagten an die vom Kläger hinterlegte Handynummer am gesandt worden, mit denen sodann um Uhr die Hinterlegung einer neuen E-Mail-Adresse um und um Uhr die Installation der App auf einem neuen Gerät der Marke Samsung bestätigt wurde. Mit der App von diesem Gerät wurden dann die weiteren Transaktionen autorisiert. Die Kammer geht angesichts des unzureichenden abweichendes Vortrags des Klägers davon aus, dass es sich hierbei um die SMS handelt, die der Kläger nach seinem Bekunden an den Anrufer weitergeleitet hat, der unter Eingabe der enthaltenen TANs somit die App auf seinem Mobilgerät unter Verbindung mit dem Online-Banking-Konto des Klägers, mit der er sich durch E-Mail und Passwort bereits zuvor Zugang verschafft hatte, installieren und somit jedenfalls die Überweisungen freigeben konnte. Zudem ist dem Kläger nach dem unbestrittenen Vortrag der Beklagten auch per SMS ein Link zur Installation der App auf einem neuen Gerät übersandt worden. Dies ist – wie die Kammer aus zahlreichen anderen Verfahren bekannt ist – im Übrigen der reguläre Weg, wie die App auf einem neuen Gerät installiert werden kann. Auch diese muss der Kläger weitergeleitet haben. 52

Mit dem Zugriff auf E-Mail-Adresse und Passwort des Online-Bankings des Klägers hatten die hinter dem Anrufer stehenden Personen ohne Weiteres Zugriff auf das Online-Banking des Klägers und konnten entsprechende Überweisungen in Auftrag geben. Mit der App, deren Installation auf einem eigenen Gerät sie aufgrund der Weiterleitung des Links durch den Kläger vornehmen konnten, konnte dann eine Freigabe dieser Überweisungen ohne weitere Zwischenschritte erfolgen. 53

54

Diese objektiven Umstände begründen die grobe Fahrlässigkeit des Klägers hinsichtlich der ihm durch die AGB der Beklagten wie auch durch § 675l Abs. 1 BGB untersagten Weitergabe von Zugangsdaten zum Online-Banking und zur Autorisierung von Zahlungsvorgängen.

Dass wiederum so genannten Phishing-Anrufe von einer Vielzahl von Tätern eingesetzt werden, um an Zugangsdaten von Bankkunden zu gelangen, ist als weit verbreitetes Wissen anzusehen. Unabhängig von konkreten Warnungen der Beklagten auf ihrer Internetseite oder an anderen Orten und der Kenntnisnahme des Klägers hiervon kann daher eine allgemeine Kenntnis davon angenommen werden, dass Zugangsdaten zu Konten nicht an Telefonanrufer, auch wenn diese sich als Bankmitarbeiter ausgeben, weitergegeben werden dürfen. 55

Schließlich ist der Kammer, der die Streitigkeiten aus Bank- und Finanzgeschäften im Sinne von § 72a Abs. 1 Nr. 1 GVG als Sonderzuständigkeit zugewiesen sind, aus einer Vielzahl an ähnlichen, Phishing von Kontendaten von bei der Beklagten geführten Konten betreffenden Verfahren bekannt, dass die E-Mails der Beklagten bei angeforderter Passwortrücksetzung und die SMS, die zur Registrierung eines neuen Gerätes bei der App automatisiert versandt werden, den Hinweis enthalten, das dort enthaltene Links und Informationen unter keinen Umständen an andere Personen weitergeben oder geteilt werden dürfen. Es ist daher davon auszugehen, dass dies auch im hiesigen Fall so war und sich der Kläger daher mit Weitergabe auf Geheiß des Anrufers über diese Warnungen hinwegsetzte. 56

Diesem objektiven Vorwurf der groben Fahrlässigkeit steht auch ein subjektiv dem Kläger anlastbares krasses Fehlverhalten gegenüber, da sich dem Kläger auch nach seinen konkreten Erkenntnismöglichkeiten hätte aufdrängen müssen, nicht die Möglichkeit der Rücksetzung des Passworts für sein Online-Banking-Konto weiterzugeben und die Installation der App auf einem Fremdgerät nicht durch Weiterleitung des Links dazu und einer SMS-TAN hierfür zu ermöglichen. Der Kläger hat im Rahmen seiner Anhörung angegeben, dass er seit längerem, bestimmt seit fünf Jahren, Online-Banking nutze. Es ist daher jedenfalls nicht von einer unterdurchschnittlichen Vertrautheit des Klägers mit dessen üblichen Vorgängen und Gefahren bei der Weitergabe von persönlichen Daten auszugehen. 57

Da somit dem Kläger im Ergebnis in objektiver wie subjektiver Hinsicht grobe Fahrlässigkeit hinsichtlich der Weitergabe des Zugangs zum Online-Banking an unbefugte Dritte vorgeworfen werden kann, besteht der Gegenanspruch der Beklagten aus § 675v Abs. 3 Nr. 2 BGB. Der Kläger als Zahler ist danach der Beklagten als seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge der nicht autorisierte Zahlungsvorgänge – wenn man sie als nicht autorisiert ansieht – entstanden ist. Dies kann die Beklagte dem möglichen Anspruch des Klägers jedenfalls nach § 242 BGB entgegenhalten. 58

Dieser Gegenanspruch der Beklagten ist nicht durch § 675v Abs. 4 BGB ausgeschlossen. Danach sind Schadensersatzansprüche auch bei grober Fahrlässigkeit des Klägers dann ausgeschlossen, wenn die Beklagte für die Zahlungsautorisierung keine starke Kundenauthentifizierung im Sinne von § 1 Abs. 24 ZAG verlangt hätte. Dabei kann dahinstehen, ob insoweit die Definition in § 1 Abs. 24 ZAG im Lichte von § 55 ZAG einschränkend auszulegen ist. Denn auch ohne eine solche einschränkende Auslegung hatte die Beklagte hier eine starke Authentifizierung verlangt: So war zum Zugang zum Online-Banking und damit der Möglichkeit, Überweisungen zu beauftragen und das Kreditkartenkonto zu belasten, einmal ein Passwort erforderlich, somit ein Wissenselement (§ 1 Abs. 24 Nr. 1 ZAG). Zum anderen war die Freigabe mittels der App erforderlich, die wiederum auf einem bestimmten (und zu einem Zeitpunkt nur genau einem) Endgerät 59

installiert sein kann, sodass der Besitz dieses Gerätes im Sinne von § 1 Abs. 24 Nr. 2 ZAG das zweite Schutzelement in Form eines Besitzelementes darstellte. Im vorliegen Fall hat indes der Kläger dem Anrufer die Möglichkeit gegeben, dass Passwort zurückzusetzen, was funktionell der Preisgabe der Passwortes entspricht, und zudem gestattet und bestätigt, dass der Anrufer oder dessen Hinterleute die App auf einem anderen Gerät installierte und mit dem klägerischen Konto verknüpfte. Damit hat der Kläger letztlich beide getrennten Sicherheitselemente, jedes für sich, verraten, so dass auch die durch beide Elemente bewirkte starke Authentifizierung gebrochen wurde. Der Umstand, dass der Zugriff auf das Konto seitens des Klägers von demselben Gerät erfolgte, auf dem auch die App installiert war, ändert hieran nichts, da die Kompromittierung jeweils durch unterschiedliche Erlaubnisse, die der Kläger an Dritte gewährt hatte, erfolgte. Insbesondere hätte der Zugriff auch genauso erfolgen können, wenn der Kläger seinen Auftrag auf Rücksetzung des Passwortes von einem anderen Gerät abgesendet hätte als dem, auf dem auch die App installiert war.

Dieser jedenfalls bestehende Gegenanspruch ist schließlich nicht wegen Mitverschuldens der Beklagten zu kürzen. Der pauschale Vortrag des Klägers, dass das Online-Banking der Beklagten keine ausreichende Systemsicherheit gewährleiste und die Beklagte kein ausreichendes System zur Betrugsprävention vorhalte, ist bereits unsubstantiiert. Die Auslösung der Überweisungen war lediglich möglich, da der Kläger dem Anrufer den Zugang zu seinem Konto und zur App durch Weitergabe von E-Mail-Adresse, Passwortrücksetzung und SMS mit Link bzw. TANs ermöglicht hat. 60

In der Folge besteht auch der mit dem Klageantrag zu . geltend gemachte Nebenanspruch auf Ersatz vorgerichtlicher Rechtsanwaltskosten nicht. Da nach dem Dargelegten schon kein Hauptanspruch besteht, können Kosten, die zur vorgerichtlichen Geltendmachung des tatsächlich nicht bestehenden Anspruchs aufgewendet wurden, nicht von der Beklagten zu ersetzen sein; die Beauftragung seiner Prozessbevollmächtigten seitens des Klägers zur zunächst vorgerichtlichen Geltendmachung des Anspruchs war schon objektiv nicht erforderlich, da der Anspruch tatsächlich nicht bestand. Im Übrigen ist nicht ersichtlich, dass sich die Beklagte vor dem Anwaltschreiben für den Kläger vom in Verzug befand, insbesondere, dass der Kläger überhaupt zuvor an die Beklagte herangetreten war. Daher kommt ein auf die §§ 280 Abs. 1 u. 2, 286 BGB gestützter Schadensersatzanspruch mangels einer Verzug auslösenden Mahnung im Sinne von § 286 Abs. 1 BGB oder eines anderen Verzug begründenden Umstands nicht in Betracht. 61

Die Kostenentscheidung beruht auf § 91 Abs. 1 S. 1 ZPO als Folge der Abweisung der Klage in ihrem vollen Umfang. 62

Der Ausspruch zur vorläufigen Vollstreckbarkeit beruht auf § 709 S. 1 u. 2 ZPO. 63

Der Streitwert wird auf 21.499,36 EUR festgesetzt. 64