Quelle: https://voris.wolterskluwer-online.de/document/f37fe91f-712d-44f5-abc6-c3583b66311d

Bibliografie	
Gericht	OLG Oldenburg
Datum	24.04.2025
Aktenzeichen	8 U 103/23
Entscheidungsform	Urteil
Referenz	WKRS 2025, 21074
Entscheidungsname	[keine Angabe]
ECLI	ECLI:DE:OLGOL:2025:0424.8U103.23.00

Oberlandesgericht Oldenburg
Urt. v. 24.04.2025, Az.: 8 U 103/23

Erstattung von Geldbeträgen durch Überweisung vom Girokonto nach einem sog. Phishing-Vorfall

Redaktioneller Leitsatz

Die Regeln des Anscheinsbeweises sind auf den Nachweis der subjektiven Voraussetzungen grober Fahrlässigkeit grundsätzlich dann nicht anwendbar, sofern es sich (wie hier) um ein individuelles Versagen handelt. Ein objektiv grober Pflichtenverstoß rechtfertigt für sich allein nicht den Schluss auf ein gesteigertes personales Fehlverhalten, selbst wenn dieses in vergleichbaren Fällen häufig vorliegen sollte.

Die Regeln des Anscheinsbeweises können auch nicht zum Nachweis der objektiven Voraussetzungen grober Fahrlässigkeit des Zahlungsdienstnutzers im Online-Banking herangezogen werden.

Tenor:

Die Berufung der Kläger gegen das am 18. Juli 2023 verkündete Urteil der 3. Zivilkammer des Landgerichts Oldenburg wird auf Kosten der Kläger zurückgewiesen.

Dieses Urteil ist wie auch das angefochtene Urteil ohne Sicherheitsleistung vorläufig vollstreckbar.

Der Vollstreckungsschuldner darf die Vollstreckung gegen Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die vollstreckende Partei vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Gründe

I.

Die Kläger begehren die Erstattung von Geldbeträgen, die nach einem sogenannten Phishing-Vorfall von ihrem gemeinsamen, bei der Beklagten geführten Girokonto überwiesen wurden. Im Januar 2013 hatten die Kläger mit der GG Landesbank, deren Gesamtrechtsnachfolgerin die Beklagte ist, die Teilnahme am Online-Banking vereinbart. Die Klägerin zu 1, die zugleich Mitarbeiterin der Beklagten ist, nutzte dabei zunächst das sogenannte smsTAN-Verfahren und wechselte im Dezember 2020 zum sogenannten PushTAN-Verfahren.

Am 4. März 2021 erhielt die Klägerin zu 1 eine Phishing-E-Mail von der Absenderadresse "(...)". Die Klägerin zu 1 öffnete die E-

© 2026 Wolters Kluwer Deutschland GmbH

Mail und klickte auf den dort angegebenen Link. Sodann öffnete sich eine gefälschte Website, auf der die Klägerin zu 1 - jedenfalls - ihr Geburtsdatum sowie die Kartennummer ihrer girocard eingab. Anschließend erhielt die Klägerin zu 1 auf ihrem Mobiltelefon eine SMS mit einem Registrierungs-Link zur Einrichtung des PushTAN-Verfahrens. Nachdem im Anschluss eine Neuregistrierung in der PushTAN-App stattgefunden hatte, kam es zu einer Erhöhung des Tageslimits und Umbuchungen. Schließlich erfolgten zulasten des Girokontos der Kläger zwei Echtzeit-Überweisungen (31.170 € und 9.999 €) an ein estnisches Konto mit der IBAN (...). Die Klägerin bemerkte dies am 5. März 2021 und informierte die Beklagte telefonisch über die Zahlungsvorgänge.

Die Kläger haben die Auffassung vertreten, dass die Beklagte zur Erstattung der genannten Beträge verpflichtet sei. Sie haben behauptet, die streitgegenständlichen Überweisungen seien von ihnen nicht autorisiert, sondern durch unbekannte Täter ausgelöst worden.

Die Kläger haben beantragt,

1. die Beklagte zu verurteilen, an sie als Gesamtgläubiger 41.069 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz p.a. seit dem 9. März 2021 zu zahlen und ihr Konto mit der Kontonummer (...) auf den Stand zu bringen, auf dem es sich ohne die Belastungen vom 4. März 2021 in Höhe von 9.999 € sowie 31.170 € befunden hätte und

2. an sie als Gesamtgläubiger zum Ersatz vorgerichtlicher Rechtsanwaltskosten 2.304,79 € zuzüglich Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz p.a. seit Rechtshängigkeit zu zahlen.

Die Beklagte hat beantragt,

die Klage abzuweisen.

Die Beklagte hat die Auffassung vertreten, dass ihr jedenfalls ein Gegenanspruch zustehe. Dazu hat sie vorgetragen, dass die Kläger grob fahrlässig die Verfügungen der Täter verursacht hätten. Die Klägerin zu 1 habe erkennen müssen, dass es sich bei der E-Mail vom 4. März 2021 um eine Phishing-E-Mail handelte. Sie habe neben ihrem Geburtsdatum und der Kartennummer ihrer girocard auch die Zugangsdaten für das Online-Banking, also Anmeldename und PIN, preisgegeben. Ferner habe die Klägerin zu 1 die SMS mit dem Registrierungs-Link für das PushTAN-Verfahren weitergeleitet oder den in der SMS enthaltenen Registrierungs-Code händisch eingegeben oder anderweitig den Tätern zugänglich gemacht.

Wegen der weiteren Einzelheiten wird gemäß § 540 Abs. 1 Satz 1 Nr. 1 ZPO Bezug genommen auf die tatsächlichen Feststellungen im angefochtenen Urteil, mit dem das Landgericht nach Durchführung einer Beweisaufnahme durch Vernehmung von Zeugen und Einholung eines Sachverständigengutachtens die Klage abgewiesen hat.

Dagegen richtet sich die Berufung der Kläger, die unter Wiederholung und Vertiefung ihres Vorbringens ihre erstinstanzlichen Anträge weiterverfolgen.

Die Beklagte verteidigt das angefochtene Urteil und beantragt,

die Berufung zurückzuweisen.

Der Senat hat die Klägerin zu 1 persönlich angehört und Beweis erhoben durch Vernehmung des früheren Prozessbevollmächtigten der Kläger, Rechtsanwalt CC, als Zeugen sowie Anhörung des Sachverständigen Dr.-Ing. DD. Wegen der Einzelheiten wird auf die Sitzungsprotokolle vom 21. November 2024 (GA III 138 ff.) und 10. April 2025 (GA III 173 ff.) Bezug genommen.

II.

Die zulässige Berufung ist nicht begründet. Das Landgericht hat die Klage mit Recht abgewiesen, weil die geltend gemachten Ansprüche den Klägern unter keinem rechtlichen Gesichtspunkt zustehen.

1. Zur Begründung seiner Entscheidung hat das Landgericht ausgeführt (LGU 7 ff., unter I):

"1. Den Klägern steht zwar grundsätzlich gegen die Beklagte ein Anspruch aus § 675u Satz 2 BGB auf Erstattung der streitgegenständlichen Zahlungsbeträge in Höhe von insgesamt 41.069,- € zu, da die streitgegenständlichen Überweisungen nicht autorisiert waren.

Zwischen den Parteien besteht ein Geschäftsbesorgungsvertrag über die Erbringung von Zahlungsdiensten in Form eines

© 2026 Wolters Kluwer Deutschland GmbH

Zahlungsdiensterahmenvertrages gemäß §§ 675c Abs. 1, 675f Abs. 2 Satz 1 BGB.

Im Fall einer nicht autorisierten Überweisung hat der Zahlungsdienstleister nach § 675u Satz 2 BGB dem Zahler den Zahlungsbetrag unverzüglich zu erstatten, indem er das Zahlungskonto wieder auf den Stand bringt, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte.

Die streitgegenständlichen Überweisungen sowie die im Vorfeld erfolgte Erhöhung des Tageslimits waren nicht autorisiert. Sie wurden durch die Kläger nicht veranlasst, sondern durch die unbekannten Täter ohne ihr Wissen und Wollen ausgelöst. Dass die Überweisungen durch die Kläger nicht autorisiert worden sind, hat die Beklagte zwar zunächst bestritten. Aufgrund der Angaben der Klägerin zu 1) im Rahmen ihrer persönlichen Anhörung sowie des Umstands, dass das Zielkonto laut Ermittlungsakte (vgl. Bl. 25 der beigezogenen Ermittlungsakte) aus anderen Betrugsverfahren bekannt ist, hat die Kammer keinen Zweifel daran, dass die Überweisungen nicht autorisiert waren. Auf die Frage der Darlegungs- und Beweislast für die Autorisierung der Überweisungen kommt es nicht an.

2. Die Beklagte hat gegen die Kläger jedoch einen Schadenersatzanspruch auf Rückbelastung in gleicher Höhe gemäß § 675v Abs. 3 Nr. 2a) BGB, den sie den Klägern erfolgreich im Wege des dolo-agit Einwandes nach § 242 BGB entgegenhalten kann. Denn nach § 675v Abs. 3 Nr. 2a) BGB ist der Zahler dem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn er ihn durch grob fahrlässige Verletzung einer Pflicht aus § 675l BGB herbeigeführt hat.

Die Klägerin zu 1) hat zur Überzeugung der Kammer vorliegend grob fahrlässig Pflichten gemäß §§ 675v Abs. 3 Nr. 2a) i.V.m. 675l Abs. 1 BGB verletzt. Dieses Verhalten muss sich der Kläger zu 2) gem. § 278 BGB zurechnen lassen.

a) Eine Pflichtverletzung in Sinne von §§ 675v Abs. 3 Nr. 2a) i.V.m. 675l Abs. 1 BGB seitens der Klägerin zu 1) liegt vor.

aa) Zu den Pflichten, die der Zahler verletzen kann, zählen sowohl die gesetzlichen Pflichten aus § 675l Abs. 1 BGB als auch alle wirksam vertraglich vereinbarten Sorgfaltspflichten im Hinblick auf das Zahlungsinstrument und die personalisierten Sicherheitsmerkmale (vgl. Zetzsche, in MüKo BGB, 9. Aufl. 2023, § 675v Rn. 44 f.). Die gesetzlichen Pflichten des § 675l BGB sehen vor, dass der Zahlungsdienstnutzer alle zumutbaren Vorkehrungen zu treffen hat, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Personalisierte Sicherheitsmerkmale sind gemäß § 1 Abs. 25 ZAG - in der hier maßgeblichen, vom 29.12.2020 bis 30.06.2021 geltenden Fassung - personalisierte Merkmale, die der Zahlungsdienstleister einem Zahlungsdienstnutzer zum Zwecke der Authentifizierung bereitstellt. Darunter fallen insbesondere die PIN, mit der sich der Kunde unter anderem beim Online-Banking legitimiert (Casper/Terlau, ZAG, 3. Aufl., § 1 Rn. 530).

Der Inhalt der Sorgfaltspflicht des § 675l Abs. 1 BGB fordert vom Kunden, alle zumutbaren Vorkehrungen zum Schutz gegen unbefugten Zugriff zu treffen. So hat der Zahlungsdienstnutzer allgemein dafür Sorge zu tragen, dass nicht dritte Personen die unkontrollierte Zugriffsmöglichkeit auf sein Online-Banking mittels Zugangsdaten und TAN bekommen und so ohne sein Wissen und Wollen Transaktionen von seinem Konto bei dem Zahlungsdienstleister durchführen können. Speziell beim Online-Banking zählt damit zu den Sorgfaltspflichten die Vorbeugung vor einem Missbrauch von Anmeldenamen und PIN und/ oder TAN. So stellt unter anderem die Mitteilung von Anmeldedaten an Dritte eine Sorgfaltspflichtverletzung dar. Der Zahlungsdienstnutzer muss unter Zugrundelegung des typischen Wissens und der gebotenen Sorgfalt zudem wissen, dass die vollständige PIN sowie entsprechende Legitimationskennzeichen von den Zahlungsdienstleistern oder ihren Mitarbeitern weder per E-Mail, SMS, am Telefon oder in sonstiger Weise abgefragt werden und es zu den ihn treffenden Sorgfaltspflichten gehört, diese sensiblen Daten nicht über die vorgenannten Kanäle preiszugeben (vgl. LG Essen, BeckRS 2015, 1693) Der Inhalt der gesetzlichen Sorgfaltspflichten des § 675l Abs. 1 BGB ist zudem der vertraglichen Ausgestaltung durch die Parteien zugänglich (vgl. Hofmann, in BeckOGK BGB, 1.9.2022, § 675l Rn. 12 ff.; Schmalenbach, in BeckOK BGB, 1.5.2023, § 675l Rn. 8).

bb) Aufgrund der durchgeführten Beweisaufnahme sieht die Kammer einen Verstoß der Klägerin zu 1) gegen diese sich aus § 675l Abs. 1 BGB oder aus Ziff. 9 Satz 1 der zwischen den Parteien am 04.01.2013 geschlossenen Rahmenvereinbarung zur Teilnahme am Online-Banking (Anlage B3) als erwiesen an. Die Klägerin zu 1) hat nach der Überzeugung der Kammer auf den Link in der streitgegenständlichen E-Mail geklickt und auf der sich sodann geöffneten gefälschten Website neben ihrem Geburtsdatum und ihrer Girokartennummer auch ihre Anmeldedaten zum Online-Banking in Form ihres Anmeldenamens sowie der PIN preisgegeben. Vor diesem Hintergrund kann die zwischen Parteien streitige Frage, ob die Bedingungen für das Online-Banking in der Fassung aus Oktober 2009 (Anlage B5) zwischen den Parteien Geltung haben oder die Bedingungen für das Online-Banking aus September 2019 (Anlage B2) wirksam vereinbart worden sind, dahingestellt bleiben, weil bereits die Rahmenvereinbarung zur Teilnahme am Online-Banking vom 04.01.2013 entsprechende Sorgfaltspflichten hinsichtlich der Preisgabe der Anmeldedaten statuiert.

Nach dem in § 286 Abs. 1 Satz 1 ZPO normierten Grundsatz der freien Beweiswürdigung ist ein Beweis erbracht, wenn das Gericht unter Berücksichtigung des gesamten Ergebnisses der Beweisaufnahme und der sonstigen Wahrnehmungen in der mündlichen Verhandlung von der Richtigkeit einer Tatsachenbehauptung überzeugt ist und alle vernünftigen Zweifel ausgeräumt sind. Die in § 286 ZPO genannte Überzeugung erfordert dabei keine absolute Gewissheit und auch keine "an

© 2026 Wolters Kluwer Deutschland GmbH

Sicherheit grenzende Wahrscheinlichkeit", es reicht vielmehr ein für das praktische Leben brauchbarer Grad an Gewissheit aus, der vernünftigen Zweifeln Schweigen gebietet (st. Rspr., vgl. nur BGH, NJW 2014, 71

[BGH 16.04.2013 - VI ZR 44/12] Rn. 8; Thomas/Putzo, ZPO, 43. Aufl. 2022, § 286 Rn. 2 ff.; Prütting, in MüKo, ZPO, 6. Aufl. 2020, § 286 Rn. 35 f.).
Die Klägerin zu 1) hat in ihrer persönlichen Anhörung ihrerseits nicht ausgeschlossen, über ihr Geburtsdatum und die Kartennummer ihrer Girokarte hinaus weitere Daten preisgegeben zu haben, nachdem sie auf den Link geklickt hat und auf die vermeintliche Website der Sparkasse weitergeleitet worden ist. So hat die Klägerin zu 1) zwar zunächst angegeben, dass sie lediglich ihr Geburtsdatum und die Kartennummer ihrer Girokarte auf die Website eingegeben habe. Auf Nachfrage der Kammer, ob sie sich sicher sei, dass sie nur diese beiden Daten eingegeben hat, gab die Klägerin zu 1) an, dass sie davon ausgehe, da sie dies auch in ihrer damaligen Stellungnahme so angegeben hätte. Sie könne jedoch nicht mehr zu hundert Prozent sagen, dass sie ausschließlich diese beiden Daten eingegeben hat.

Der Sachverständige hat sowohl in seinem Gutachten als auch in seiner Anhörung ausgeführt, dass die Klägerin zu 1) durch ihre Reaktion auf die Phishing-E-Mail die Überweisungen durch die unbekannten Täter ermöglicht habe. Es sei weder technisch möglich noch plausibel, dass die Betrugstäter die Überweisungen auf die dokumentierte Art und Weise allein mit den unstreitig preisgegebenen Daten, und zwar dem Geburtsdatum und der Kartennummer der Girokarte der Klägerin zu 1), vorgenommen haben könnten. Die Betrugstäter hätten für die Überweisungen und die im Vorfeld erfolgte Änderung des Limits Anmeldenamen und PIN für das Online-Banking sowie Geburtsdatum und Girokartennummer als zusätzliche Sicherheitsabfragen benötigt. Insgesamt gebe es keine andere Erklärung für die Überweisungen, als dass die Klägerin zu 1) die für die Überweisungen erforderlichen Daten - mithin auch ihre Anmeldedaten in Form von Anmeldenamen und PIN - an die Betrugstäter weitergeleitet habe. Hinweise auf eine technische Störung oder ein Datenleck bei der Beklagten lägen nicht vor. Es sei technisch ausgeschlossen und unplausibel, dass die Täter die für die Überweisungen erforderlichen Daten, so auch den Anmeldenamen und die PIN, anderweitig als durch eine Weiterleitung durch die Klägerin zu 1) erlangt hätten.

Das Gericht folgt den überzeugenden schriftlichen und mündlichen Ausführungen des Sachverständigen. Als öffentlich bestellter und vereidigter Sachverständiger mit dem Bestellungstenor "Systeme und Anwendungen der Informationsverarbeitung, insbesondere IT-Sicherheit" ist der Sachverständige für die vorliegende Begutachtung qualifiziert. Das Gutachten ist auch in sich schlüssig und nachvollziehbar. Insbesondere ist der Sachverständige von zutreffenden Tatsachen ausgegangen und hat die daraus gezogenen Konsequenzen logisch und widerspruchsfrei erläutert.

..."

Diesen in rechtlicher Hinsicht zutreffenden (zur Annahme grober Fahrlässigkeit näher sogleich, unter 2 c) und in tatsächlicher Hinsicht überzeugenden Ausführungen ist nichts hinzuzufügen. Überdies ist der Senat an die insoweit vom Landgericht getroffenen Tatsachenfeststellungen gebunden. Denn das Berufungsgericht hat gemäß § 529 Abs. 1 Nr. 1 ZPO die erstinstanzlich festgestellten Tatsachen seiner Verhandlung und Entscheidung zugrunde zu legen, soweit nicht konkrete Anhaltspunkte Zweifel an der Richtigkeit oder Vollständigkeit der entscheidungserheblichen Feststellungen begründen. Derartige Anhaltspunkte haben die Parteien nicht aufgezeigt; sie sind auch sonst nicht ersichtlich. Die Kläger verweisen hinsichtlich der Eingabe von Daten zwar auf die unmittelbar nach dem Vorfall verfasste Stellungnahme der Klägerin zu 1 (Ermittlungsakten, Bl. 5). Aus dieser ergibt sich aber schon nicht ausdrücklich, dass die Klägerin ausschließlich ihr Geburtsdatum sowie ihre Kartennummer und keine weiteren Daten eingegeben hat. Vielmehr hat die Klägerin zu 1 auch im Rahmen ihrer Anhörung vor dem Senat am 21. November 2024 nochmals ausdrücklich erklärt, sie könne nicht sicher sagen und nicht zu 100 Prozent ausschließen, dass sie neben ihrem Geburtsdatum und ihrer EC-Kartennummer noch weitere Daten eingegeben habe (GA III 140), was ihren Angaben bei der mündlichen Verhandlung vom 1. März 2022 vor dem Landgericht (GA I 138) entspricht. Auch mit ihrem Einwand, der Sachverständige habe nicht festgestellt, dass die Klägerin zu 1 die Zugangsdaten zum Online-Banking auf der gefälschten Website eingegeben habe, sondern er habe nur allgemeine Feststellungen zu der Frage getroffen, auf welche Weise die Täter an die Daten gelangt seien, dringen die Kläger nicht durch. Vielmehr ist die auf das Beweisergebnis gestützte Folgerung des Landgerichts, die Klägerin zu 1 habe auch ihren Anmeldenamen zum Online-Banking und ihre PIN auf der gefälschten Website eingegeben, in jeder Hinsicht plausibel. Dagegen ist es nicht nachvollziehbar, dass die unbekannten Täter hier einerseits - unstreitig - mit der E-Mail vom 4. März 2021 einen Phishing-Angriff gestartet haben und damit auch insoweit erfolgreich waren, als die Klägerin zu 1 auf den Link in der E-Mail geklickt und die Daten zur Sicherheitsabfrage (Geburtsdatum und girocard-Nummer) auf der dadurch geöffneten gefälschten Website eingegeben hat, andererseits die weiteren für ihren Computerbetrug erforderlichen Daten auf eine andere - unbekannte - Art und Weise erlangt haben sollen.

2. Der Senat folgt auch der Würdigung des Landgerichts, dass die Klägerin zu 1 die ihr gemäß § 675l Abs. 1 Satz 1 BGB obliegenden Pflichten grob fahrlässig verletzt hat (§ 675v Abs. 3 Nr. 2 Buchst. a BGB). Dabei geht der Senat von einer weiteren Pflichtverletzung der Klägerin zu 1 durch Weiterleitung oder sonstige Weitergabe des per SMS versandten Registrierungs-Links für die Neuregistrierung zum PushTAN-Verfahren aus (was vom Landgericht ausdrücklich offengelassen wurde, LGU 17).

a) Dazu ist mit der Ladungsverfügung vom 28. Juni 2024 folgender Hinweis ergangen (GA III 51 ff.):

© 2026 Wolters Kluwer Deutschland GmbH

"Nach vorläufiger Beurteilung können der Berufung Erfolgsaussichten nicht ohne weiteres abgesprochen werden.

a) Allerdings dürfte das Landgericht aufgrund der durchgeführten umfangreichen Beweisaufnahme jedenfalls im Ergebnis mit Recht davon ausgegangen sein, dass die Klägerin zu 1 Pflichten gemäß § 675l Abs. 1 Satz 1 BGB verletzt hat, indem sie nicht alle zumutbaren Vorkehrungen traf, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

Dabei kommt neben der Annahme des Landgerichts, die Klägerin zu 1 habe nach dem Klick auf den Link in der Phishing-E-Mail vom 4. März 2021 auf der sodann geöffneten gefälschten Website ihren Anmeldenamen zum Online-Banking sowie die PIN preisgegeben (LGU 9), auch eine Weiterleitung oder sonstige Weitergabe des per SMS versandten Registrierungslinks für die Neuregistrierung zum Push-TAN-Verfahren in Betracht.

aa) Denn personalisierte Sicherheitsmerkmale sind gemäß § 675c Abs. 3 BGB in Verbindung mit § 1 Abs. 25 ZAG personalisierte Merkmale, die der Zahlungsdienstleister einem Zahlungsdienstnutzer zum Zwecke der Authentifizierung bereitstellt. Darunter sind Datenschlüssel, Zeichenabfolgen oder Codewörter zu fassen, die dem Zahlungsdienstnutzer durch den Zahlungsdienstleister exklusiv zur Kenntnis gebracht werden, sodass das Innehaben dieser Informationen gegenüber dem Zahlungsdienstleister oder anderen Zahlungsinstituten die Berechtigung indiziert (Findeisen in: Ellenberger/Findeisen/Nobbe/ Böger, Kommentar zum Zahlungsverkehrsrecht, 3. Aufl., § 1 ZAG Rn. 858; OLG München, Beschluss vom 4. September 2023 - 19 U 1508/23 e, juris Rn. 73). Als "Vorstufe" dürfte auch der per SMS verschickte Registrierungslink umfasst sein, der die Legitimation gegenüber der Beklagten ermöglichte, wodurch die Freischaltung der PushTAN-App auf einem (mobilen) Endgerät und in der Folge die Erlangung von TAN erfolgen konnte (vgl. OLG München, Beschluss vom 4. September 2023 - 19 U 1508/23 e, juris Rn. 77).

bb) Dazu hat die Beklagte vorgetragen, die Klägerin zu 1 habe entweder die (unstreitig) auf ihrem Smartphone eingegangene SMS mit dem Registrierungslink an die Betrüger weitergeleitet oder die Daten aus der SMS manuell abgetippt und auf der Phishing-Homepage in eine dafür vorgesehene Maske eingegeben (Schriftsatz vom 28. Oktober 2021, S. 4 = GA I 45). Dieser Vortrag könnte aufgrund des erstinstanzlichen Beweisergebnisses - insbesondere der Ausführungen des Sachverständigen DD einschließlich der abschließenden Angaben in der mündlichen Verhandlung vom 19. Juni 2023 (Protokoll, S. 10 f. = GA II 89 f.) - gemäß § 138 Abs. 3 ZPO als zugestanden gelten.

Denn der Klägerin obliegt hinsichtlich der von ihr vorgenommenen Vorgänge in Bezug auf die Handlungen im Online-Banking am 4. März 2021 eine sekundäre Darlegungslast (vgl.

BGH Urteil vom 8. März 2021 - VI ZR 505/19, juris Rn. 27 mwN). Dieser sekundären Darlegungslast ist die Klägerin nachgekommen. Sie hat angegeben, dass sie nach dem Klick auf den Link in der Phishing-E-Mail vom 4. März 2021 auf der sodann geöffneten gefälschten Website lediglich ihr Geburtsdatum und ihre Girokartennummer eingegeben und sonst keine Eingaben gemacht oder Informationen weitergegeben habe.
Damit liegt die Darlegungs- und Beweislast wieder bei der Beklagten als Beweispflichtige (vgl.

BGH, Urteil vom 26. Juni 2023 - VIa ZR 533/21, juris Rn. 23). Wenn diese die Unrichtigkeit des gegnerischen Vorbringens beweisen kann, was hier angesichts der bereits genannten Angaben des Sachverständigen in Betracht kommt, wird das Bestreiten unbeachtlich mit der Folge, dass das Vorbringen des primär Darlegungs- und Beweisbelasteten als zugestanden gemäß § 138 Abs. 3 ZPO gilt (vgl. BGH, Urteil vom 24. November 2020 - VI ZR 415/19, juris Rn. 12 f.; BGH, Beschluss vom 9. Februar 2021 - VIII ZR 316/19, juris Rn. 29 f.). Damit wäre auch der Vortrag als zugestanden anzusehen, die Klägerin zu 1 habe den Registrierungslink an die unbekannt gebliebenen Täter weitergegeben.
b) Dies dürfte jedenfalls in objektiver Hinsicht einen Sorgfaltspflichtverstoß begründen. Allerdings wird hier - im Anschluss an die Ausführungen des Sachverständigen - angenommen, dass die Registrierungs-SMS nur den in Anlage K4 (Anlagenband Kläger) dargestellten Inhalt hatte und nicht auch den im Schriftsatz der Beklagten vom 13. Juni 2022 auf Seite 2 (GA I 190R) dargestellten Warnhinweis enthielt.

c) Auch damit stünde aber noch nicht fest, dass die Klägerin zu 1 grob fahrlässig Pflichten gemäß § 675l Abs. 1 Satz 1 BGB verletzt hat (dazu LGU 13 ff.), was Voraussetzung für einen Anspruch der Beklagten aus § 675v Abs. 3 Nr. 2 lit. a BGB ist.

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. Die Regeln des Anscheinsbeweises sind auf den Nachweis der subjektiven Voraussetzungen grober Fahrlässigkeit grundsätzlich dann nicht anwendbar, wenn es sich - wie hier - um ein individuelles Versagen handelt. Denn ein objektiv grober Pflichtenverstoß rechtfertigt für sich allein noch nicht den Schluss auf ein gesteigertes personales Fehlverhalten, selbst wenn dieses in vergleichbaren Fällen häufig vorliegen sollte. Die Regeln des Anscheinsbeweises können auch nicht zum Nachweis der objektiven Voraussetzungen grober Fahrlässigkeit des Zahlungsdienstnutzers im Online-Banking herangezogen werden (vgl.

BGH, Urteil vom 26. Januar 2016 - XI ZR 91/14, BGHZ 208, 331 Rn. 71, 73, 74 f. mwN).
Zur Beurteilung, ob im vorliegenden Fall unter Würdigung der Gesamtumstände ein in diesem Sinne grob fahrlässiges

© 2026 Wolters Kluwer Deutschland GmbH

Verhalten der Klägerin zu 1 zu bejahen ist, erscheint eine erneute Anhörung der Klägerin zu 1 geboten."

b) Nach ergänzender Aufklärung des Sachverhalts durch zweimalige Anhörung der Klägerin zu 1, Vernehmung des Zeugen CC und Anhörung des Sachverständigen Dr.-Ing. DD geht der Senat davon aus, dass die Klägerin zu 1 nicht nur - wie bereits vom Landgericht festgestellt - auf der gefälschten Website ihre Anmeldedaten zum Online-Banking in Form ihres Anmeldenamens sowie ihrer PIN preisgegeben, sondern auch eine Weiterleitung oder sonstige Weitergabe des per SMS versandten Registrierungs-Links beziehungsweise des entsprechenden Registrierungs-Codes für die Neuregistrierung zum PushTAN-Verfahren vorgenommen und auch dadurch ihre Pflicht gemäß § 675l Abs. 1 Satz 1 BGB verletzt hat.

aa) Die Klägerin zu 1 hat allerdings bei ihrer Anhörung am 21. November 2024 erklärt (GA III 139 f.):

"Im Anschluss an meine Eingaben am Nachmittag des 04.03.2021 habe ich nicht damit gerechnet, dass ich eine SMS auf meinem Handy bekommen würde. Auf der Seite, auf der ich die Eingaben vorgenommen hatte, war mitgeteilt worden, dass die PushTAN-App in 48 Stunden wieder funktioniert. Von einer SMS war keine Rede. Ich habe mir darüber auch keine Gedanken gemacht. Die auf meinem Handy um 15:08 Uhr eingegangene SMS habe ich nicht bemerkt. Ich habe erst im Nachhinein gemeinsam mit Rechtsanwalt EE festgestellt, dass mein Handy so eingestellt war, dass eingehende SMS nicht angezeigt werden, auch nicht durch eine Zahl bei dem SMS-Symbol. Zuvor hatte Rechtsanwalt CC mich bei einem Besprechungstermin gefragt, ob ich eine SMS erhalten habe. Das habe ich verneint. Daraufhin hat er mein Handy genommen und nachgeschaut. Da haben wir festgestellt, dass ich etliche SMS und auch Anrufe in Abwesenheit erhalten hatte, die mir nicht angezeigt worden waren."

Bei der weiteren Anhörung am 10. April 2025 ist die Klägerin nochmals konkret zum Ablauf des Besprechungstermins bei Rechtsanwalt CC befragt worden und hat dazu Folgendes erklärt (GA III 173 f.):

"Wir, also mein Ehemann und ich, waren im Anschluss an das Schreiben der Nord/LB vom 11. März 2021 bei Herrn CC im Anwaltsbüro. Wir haben ihm den Sachverhalt geschildert. Ich muss sagen, dass Herr CC sehr IT-affin ist. Er war in der Kanzlei auch für die IT-Sicherheit zuständig. Dementsprechend hatte er sehr direkt nachgefragt, wie der Vorgang abgelaufen ist. Er hat auch gefragt ob ich eine SMS bekommen habe. Daraufhin habe ich gefragt: "Welche SMS?". Er sagte, ich müsste eine SMS bekommen haben, damit die Registrierung für das PushTAN-Verfahren erfolgen kann. Davon wusste ich nichts. Daraufhin hat Herr CC selbst mein Handy genommen und nachgeschaut. Er hat gesehen, dass dort eine SMS mit dem Registrierungs-Link angekommen war. Ich hatte das selbst vorher noch gar nicht gesehen. Herr CC hatte dann auch noch festgestellt, dass es noch mehrere SMS-Nachrichten gab, die nicht gelesen worden sind."

bb) Es ist möglich und aus Sicht des Senats nicht fernliegend, dass die Klägerin zu 1 subjektiv von der Richtigkeit dieser Angaben überzeugt ist. Der Senat sieht die Schilderung der Klägerin zu 1 aber aufgrund des übrigen Beweisergebnisses als widerlegt an.

(1) Bei dieser Beweiswürdigung berücksichtigt der Senat zunächst eine auffällige Diskrepanz zwischen den Angaben der Klägerin zu 1 und der Zeugenaussage ihres früheren Prozessbevollmächtigen, Rechtsanwalt CC. Die Klägerin zu 1 hat vor dem Senat zwei Mal erklärt, dass sie die auf ihrem Mobiltelefon eingegangene SMS mit dem Registrierungs-Link nicht bemerkt und erst bei dem Besprechungstermin mit Rechtsanwalt CC erstmals gesehen habe. Das entspricht auch ihren Angaben vor dem Landgericht in der mündlichen Verhandlung vom 19. Juni 2023, nach denen sie die SMS erst im Büro bei Rechtsanwalt CC festgestellt habe (GA II 81). Aus der Aussage des Zeugen CC ergibt sich aber, dass diese von der Klägerin zu 1 mehrfach vorgetragene Schilderung falsch ist. Der Zeuge hat zwar bestätigt, dass die SMS in dem Mandantengespräch mit den Klägern, das nach seinen Akten am 12. März 2021 stattgefunden habe, die SMS zur Sprache gekommen sein müsse. Er erinnere sich noch, dass die Klägerin zu 1 ihm ihr Handy gegeben habe und sie sich dann auch den gespeicherten Verlauf sowohl hinsichtlich eingegangener als auch ausgegangener SMS gemeinsam angesehen hätten. Auf konkrete Nachfrage des Vorsitzenden hat der Zeuge dann weiter erklärt (GA III 174 f.):

"Ich meine, dass meine Nachfrage nach der SMS für Frau AA überraschend war. Sie war auf diese Frage nicht vorbereitet. Sie war nicht auf die Idee gekommen, in dem Ausgang nachzuschauen. Ich weiß heute nicht mehr, ob Frau AA die eingegangene Nachricht schon kannte. Insofern muss ich jetzt sagen, dass ich mir das damals sogar notiert habe. In meinen Notizen steht: "SMS spät gesehen, nach Eingang Brief 9.3.". Ob wir gemeinsam noch ungelesene Nachrichten im Eingang des Handys von Frau AA festgestellt haben, habe ich nicht mehr in Erinnerung."

Aus der vom Zeugen verlesenen Notiz ergibt sich, dass die Klägerin zu 1 die SMS nicht erst bei Rechtsanwalt CC festgestellt hat. Denn die Notiz "SMS spät gesehen, nach Eingang Brief 9.3." wäre so nicht erfolgt, wenn die Klägerin zu 1 die SMS tatsächlich, wie von ihr angeben, noch gar nicht gekannt hätte und die Nachricht erst durch Rechtsanwalt CC entdeckt worden wäre. Es ist ein gravierender Unterschied, ob die Klägerin zu 1 die SMS zu dem hier maßgeblichen Zeitpunkt des Mandantengesprächs "spät" oder "noch gar nicht" gesehen hatte. Eine bloß nachlässige Formulierung der Notiz erscheint deshalb ausgeschlossen (abgesehen davon, dass der Zeuge CC dem Senat als ausgesprochen sorgfältig formulierender Rechtsanwalt bekannt ist). Der Umstand, dass

© 2026 Wolters Kluwer Deutschland GmbH

die Klägerin zu 1 erst im Mandantengespräch - für sie überraschend - erfahren hätte, dass es eine entsprechende SMS gibt, wäre vielmehr (als Indiz für die Richtigkeit der klägerischen Darstellung) so bedeutsam gewesen, dass nicht nur eine schriftliche Niederlegung in den Notizen des Rechtsanwalts, sondern auch eine Mitteilung gegenüber der Beklagten zu erwarten gewesen wäre. Eine solche Mitteilung ist aber nicht erfolgt. Vielmehr heißt es in dem von Rechtsanwalt CC im Anschluss an das Mandantengespräch verfassten Schreiben vom 16. März 2021 an die Beklagte (Anlage K7, Anlagenband Kläger) auf Seite 3:

> "Ihre Behauptung, meine Mandantin habe die Registrierung-SMS für die Änderung des PushTAN-Gerätes nicht selber durch Anklicken auf den in der SMS erhaltenen Link genutzt, sondern diesen Link bzw. die ganz SMS an die Betrüger weitergeleitet, ist schlichtweg unzutreffend. Ich habe mich am Mobiltelefon ihrer Kundin sogar persönlich davon überzeugt, dass die SMS nicht weitergeleitet wurde. Ihre diesbezügliche Behauptung lässt jedoch den Schluss zu, dass sie bis heute nicht wissen, wie es den Tätern technisch eigentlich gelungen ist, Zugriff auf das Konto meiner Mandanten zu erhalten, weshalb mich ihre Ablehnung auch geschäftspolitisch irritiert."

Daraus ergibt sich lediglich, dass Rechtsanwalt CC, wie von ihm in seiner Zeugenaussage bekundet, das Mobiltelefon persönlich überprüft und dabei auch auf ausgehende SMS untersucht hat. Davon, dass der Klägerin zu 1 die SMS vor der persönlichen Überprüfung durch den Zeugen noch gar nicht bekannt war, ist hingegen nicht die Rede.

Dass ein von der Klägerin zu 1 wiederholt geschilderter Umstand (die erstmalige Entdeckung der SMS bei Rechtsanwalt CC) in Wahrheit - durch die handschriftliche Notiz des Zeugen belegt - so nicht stattgefunden hat, ist neben dem Ergebnis der Beweisaufnahme im Übrigen und insbesondere den Ausführungen des Sachverständigen zu den denkbaren Angriffsszenarien hinsichtlich der PushTAN-Registrierung (dazu sogleich, unter (2)) ein für die Beweiswürdigung maßgeblicher Aspekt. Denn dies weckt auch berechtigte Zweifel an der Richtigkeit und Vollständigkeit der weiteren Angaben der Klägerin zu 1.

Zu diesen Zweifeln trägt auch bei, dass die Klägerin zu 1 auf Fragen des Senats zum Teil nicht spontan, sondern mit Nachfragen reagierte und bei der Beantwortung von Fragen mehrmals zu allgemeineren Ausführungen ausholte, die wenig mit der gestellten Frage zu tun hatten, sondern einem Plädoyer in eigener Sache glichen. Im Kontrast dazu fielen manche Antworten erstaunlich knapp aus, wie etwa die Angabe der Klägerin zu 1 vom 21. November 2024, sie habe vor dem 4. März 2021 Mails von der Beklagten an ihre private E-Mail-Adresse bekommen, könne aber so nicht sagen, wie das Design dieser Mails aussehe (GA III 139). Das wiederum erscheint bei der Klägerin zu 1, die bei der Beklagten beschäftigt ist, merkwürdig.

Dabei hält es der Senat, wie bereits ausgeführt, für möglich und nicht fernliegend, dass die Klägerin zu 1, die sich seit inzwischen mehr als vier Jahren mit dem Vorfall beschäftigen muss, subjektiv von der Richtigkeit ihrer Angaben überzeugt ist. Denn es handelt sich hier um einen erheblichen Schaden, der durch einen Angriff von Straftätern entstanden ist und bei dem von Anfang an von der Beklagten (zugleich Arbeitgeberin der Klägerin zu 1) eigene Fehler der Klägerin zu 1 behauptet wurden.

Die Klägerin zu 1 hat bei ihrer Anhörung am 21. November 2024 im Zusammenhang mit ihrer Erklärung zur möglichen Eingabe weiterer Daten (neben ihrem Geburtsdatum und der Kartennummer ihrer girocard), die sie nicht ausschließen konnte, selbst zu bedenken gegeben, dass sie sich am 5. März 2021 und danach wegen des Phishing-Vorfalls in einem Ausnahmezustand befunden habe (GA III 140). Das ist angesichts des hier entstandenen Schadens und der von Anfang an im Raum stehenden eigenen Fehler der Klägerin zu 1 einerseits verständlich. Andererseits begründet es weitere Zweifel an der Richtigkeit und Vollständigkeit der Angaben der Klägerin zu 1.

Das gilt auch schon für die vom Zeugen CC notierte Angabe vom 12. März 2021, dass die Klägerin zu 1 die SMS mit dem Registrierungs-Link erst "spät" und nicht vor dem 9. März 2021 (also erst nach den schädigenden Verfügungen der Täter) gesehen habe. Der Senat hält es für naheliegend, dass bereits diese Schilderung von dem durch die Klägerin zu 1 geschilderten Ausnahmezustand und einer dadurch - im Sinne einer Beschönigung oder Negierung eigenen Verhaltens - beeinflussten Erinnerung geprägt war.

Das gilt umso mehr, wenn man berücksichtigt, dass die Klägerin zu 1 am 21. November 2024 berichtet hat, dass sie am Vorfallstag (4. März 2021) im Home-Office gearbeitet habe, es ein stressiger Tag gewesen sei und sie die Bearbeitung der Phishing-Mail und die Eingabe der Daten "zwischendurch erledigt" habe (GA III 140). Denn das Öffnen der bereits um 15:08 Uhr - kurz nach Eingabe der Daten auf der gefälschten Website, die nach den Angaben der Klägerin zu 1 um ca. 15 Uhr stattgefunden hat (GA III 139) - auf dem Mobiltelefon der Klägerin zu 1 eingegangenen SMS mit dem Registrierungs-Link und deren Weiterleitung beziehungsweise die händische Eingabe des in der SMS enthaltenen Registrierungs-Codes sind Handlungen, die in kurzer Zeit erledigt werden können und dadurch im Zweifel keinen bleibenden Eindruck hinterlassen, erst recht wenn sie unter Stress und/oder Zeitdruck erfolgen. Es erscheint deshalb plausibel, dass die Klägerin zu 1 diese Vorgänge angesichts des entstandenen Schadens und vor dem Hintergrund der ihr gegenüber von der Beklagten im Schreiben vom 11. März 2021 (Anlage K3, Anlagenband Kläger) erhobenen Vorwürfe schon bei dem Mandantengespräch bei Rechtsanwalt CC nicht mehr vollständig in Erinnerung hatte.

(2) Dass es sich entgegen dieser Annahme tatsächlich so zugetragen hat, wie von der Klägerin zu 1 geschildert - sie also die SMS nicht bemerkt und insbesondere den Registrierungs-Link beziehungsweise den entsprechenden Registrierungs-Code nicht weitergeleitet oder sonst weitergegeben hat, hält der Senat nach Würdigung aller Umstände, insbesondere unter Berücksichtigung

© 2026 Wolters Kluwer Deutschland GmbH

der Ausführungen des Sachverständigen, für ausgeschlossen (§ 286 Abs. 1 ZPO).

Denn nach den fehlerfreien Feststellungen des Landgerichts (§ 529 Abs. 1 Nr. 1 ZPO) haben die Täter Kenntnis von den Registrierungs-Daten aus der an die Klägerin zu 1 gesandten SMS erlangt (LGU 17), weil sie sonst nicht in der Lage gewesen wären, sich für die PushTAN-App zu registrieren und anschließend Verfügungen zulasten des Girokontos der Kläger vorzunehmen. Die vom Landgericht - aus dessen Standpunkt konsequent - offen gelassene Frage, wie die Täter die Kenntnis erlangt haben, beantwortet der Senat dahin, dass die Täter die Kenntnis durch Weiterleitung oder sonstige Weitergabe seitens der Klägerin zu 1 erlangt haben. Die zwischenzeitlich vom Senat erwogene Möglichkeit, dass eine mögliche Erklärung für die Kenntnis der Täter von den Registrierungs-Daten darin liegen könnte, dass der iMac und das iPhone der Klägerin am 4. März 2021 so miteinander verbunden (synchronisiert) waren, dass die SMS auch auf dem Bildschirm des iMac angezeigt wurde (und die Täter durch Installation einer entsprechenden Schad-Software nach dem Öffnen des in der Phishing-E-Mail enthaltenen Links auch den Bildschirm des iMac sehen konnten) kommt nicht in Betracht, weil die Kläger auf entsprechende Nachfrage ausdrücklich erklärt haben, dass es eine solche Verbindung der Geräte (mit der Folge einer Anzeige eingehender SMS auf dem Bildschirm des iMac) nicht gegeben habe (GA III 163 f.). Dass die konkrete Art der Weitergabe durch die Klägerin zu 1 nicht weiter aufgeklärt werden kann, ändert daran nichts. Insofern ist der - den Vorgang mangels eigener Kenntnis nur allgemein beschreibende - Vortrag der Beklagten gemäß § 138 Abs. 3 ZPO als zugestanden anzusehen, weil die im Rahmen der sekundären Darlegungslast der Kläger erfolgten Angaben der Klägerin zu 1 widerlegt sind (vgl.

BGH, Urteil vom 24. November 2020 - VI ZR 415/19, juris Rn. 12 f.; BGH, Beschluss vom 9. Februar 2021 - VIII ZR 316/19, juris Rn. 29 f.).
Der Sachverständige Dr.-Ing. DD hat in seinem ersten schriftlichen Gutachten vom 16. Oktober 2022 zunächst auf Seite 5 den Begriff des sogenannten "Social Engineering" erläutert, bei dem das Opfer beispielsweise durch einen Telefonanruf eines angeblichen Bankmitarbeiters dazu gebracht wird, eine gültige TAN für eine Transaktion des Angreifers zu erzeugen und diese dem Angreifer mitzuteilen. Ergänzend hat der Sachverständige weiter unten im Gutachten ausgeführt, dass es Angreifern immer wieder gelinge, betrügerische Transaktionen zu ihren Gunsten abzusetzen, meist mit einer Kombination aus Phishing und Social Engineering, wobei die Zugangsdaten zum Online-Banking durch Phishing in die Hände eines Angreifers gebracht und dann durch Telefonanrufe TANs erbeutet und Transaktionen angestoßen werden (S. 16). Auf den Seiten 10 ff. wird ferner dargestellt, welche technischen Angriffe gegen eine SMS-Registrierung möglich sind. Weitere Ausführungen zu den technischen Angriffen hat der Sachverständige im schriftlichen Ergänzungsgutachten vom 31. Januar 2023 auf den Seiten 5 ff. gemacht. Danach

> "gibt es drei Varianten, um SMS abzufangen oder zu manipulieren.
>
> - auf dem Gerät des SMS-Empfängers befindet sich Schadsoftware, die die SMS weiterleitet oder dem Empfänger einen manipulierten Inhalt anzeigt.
> - Der Angreifer registriert eine eigene SIM-Karte für die Mobilfunknummer des Opfers und fängt die SMS ab (SIM-Swapping).
> - Der Angreifer verschafft sich Zugang zum Providernetzwerk SS7 und hat Zugriff auf die SMS des Opfers."

Bei seiner Anhörung durch das Landgericht in der mündlichen Verhandlung vom 19. Juni 2023 hat der Sachverständige sich unter anderem wie folgt geäußert (GA II 89 f.):

> "...
>
> Aus meiner Sicht ist das Versenden der SMS kein sonderlich sicheres Verfahren, es wird aber nach wie vor genutzt. Ich habe in meinem Gutachten verschiedene Wege aufgezeigt, wie die Täter Kenntnis von dem Inhalt des Aktivierungslinks bekommen haben. Es gibt verschiedene technische Fehler, so etwa Trojaner. Für ein IPhone möchte ich diese aber ausschließen.
>
> Einen Banking Trojaner gibt es meiner Kenntnis nach für IPhones nicht. Dann kann in den sog. Provider eingebrochen worden sein, dies gab es früher mal, so in den Jahren 2015/2016. Dies ist heute ebenfalls unwahrscheinlich. Diese technischen Fehler sind aus meiner Sicht grundsätzlich unwahrscheinlich. Diese sind erst recht unwahrscheinlich im Zusammenhang mit dem hier vorliegenden Social Engineering. Aus meiner Kenntnis liegt nahe, dass der Link in der SMS in irgendeiner Form seitens der Kläger weitergegeben wurde. Entweder wurde die SMS weitergeleitet, der Link wurde vorgelesen, er wurde auf eine Internetseite eingegeben oder es wurde ein Screenshot gefertigt. Dieses sind verschiedene Möglichkeiten, die ich hier sehe. Möglicherweise erinnert sich die Klägerin hieran nicht mehr.
>
> ...
>
> In meinem Gutachten habe ich noch eine weitere Möglichkeit eines technischen Fehlers benannt. Dies war das sog. SIM-Swapping. Hier erfolgt die Registrierung einer anderen SIMKarte. Dass dies der Fall ist, schließe ich aber aus, weil die

© 2026 Wolters Kluwer Deutschland GmbH

Klägerin hier die SMS erhalten hat.

..."

Bei seiner Anhörung durch den Senat am 10. April 2025 hat der Sachverständige zunächst erläutert, dass es auch in der Zwischenzeit keine neueren Erkenntnisse gegeben habe, die zu einer anderen Bewertung führen könnten. Es seien zwar einige Trojaner (Schad-Software) für Android-Geräte bekannt geworden. Davon könne das Gerät der Klägerin zu 1 aber nicht betroffen gewesen sein, weil es sich um ein iPhone handelte. Ein ebenfalls denkbares Eindringen in das sogenannte SS7-Netzwerk halte er trotz der Möglichkeit zum Erwerb eines Provider-Zugangs außerhalb Europas auch für das Jahr 2021 für ausgeschlossen, weil nach erfolgreichen Angriffen in den Jahren 2015/2016 durch Verbesserungen der Firewall deutlich höhere Anforderungen an den Zugang zu diesem Netzwerk gestellt worden seien (GA III 175 f.). Auf die abschließenden Fragen der Parteivertreter zu seiner Bewertung hat der Sachverständige sich wie folgt geäußert (GA III 176):

"Auf Frage des Klägervertreters:

...

Wenn ich nochmals zu meiner Bewertung, dass ein anderer Angriff als durch sogenanntes Social Engineering "technisch möglich, aber unplausibel" sei, befragt werde, so sage ich Folgendes: Richtig ist, dass ein entsprechender technischer Eingriff machbar ist. Theoretisch könnte ja auch jemand bestochen worden sein. Es ist immer so, dass wir keine 100-prozentigen Kenntnisse über die Täterfähigkeiten haben. Es bleibt aber bei meiner Bewertung, dass ich das im vorliegenden Fall für unplausibel halte.

Das bezieht sich ausdrücklich auch darauf, dass die Täter an den Registrierungs-Link gelangt sind, was hier so sein muss.

Auf Frage des Beklagtenvertreters:

Wenn ich nochmals "ganz platt" gefragt werde, wie die Täter hier an den Registrierungs-Link gekommen sind, sage ich Folgendes: Es gibt zum einen die Möglichkeit des technischen Angriffs und zum anderen die Möglichkeit des sogenannten Social Engineering. Beispielsweise ruft in diesen Fällen dann eine "Frau XXX von der Sparkasse" bei dem Opfer an und sagt, dass man jetzt den Registrierungs-Link brauche. Das kenne ich so aus verschiedenen anderen Fällen. Allgemein halte ich die letztere Variante für die wahrscheinlichere."

Der Senat folgt den überzeugenden Ausführungen des Gutachters, der als öffentlich bestellter und vereidigter Sachverständiger für "Systeme und Anwendungen der Informationsverarbeitung, insbesondere im Bereich IT-Sicherheit" über die erforderliche Sachkunde und Erfahrung verfügt. Aufgrund dieser Expertise ist der Sachverständige zu der überzeugend begründeten Einschätzung gekommen, dass die Täter bei dem hier zu beurteilenden Vorfall, der unstreitig mit einem Phishing-Angriff per E-Mail begonnen hat, im Anschluss an die durch Phishing veranlassten Eingaben auf der gefälschten Website den per SMS versandten Registrierungs-Link beziehungsweise den entsprechenden Registrierungs-Code durch Social Engineering erlangt haben (beispielsweise durch telefonische Aufforderung zur Weiterleitung des Links oder durch eine entsprechende Eingabeaufforderung auf der gefälschten Website). Dass die Täter die PushTAN-Registrierungsdaten, die sie für ihr weiteres Vorgehen benötigten, auf andere Weise erlangt haben könnten, ist eine theoretische Möglichkeit, die naturgemäß bei der hier vorliegenden Straftat durch unbekannte Täter, deren Vorgehensweise im Einzelnen nicht bekannt ist, nicht vollständig ausgeschlossen werden kann. Der Senat hält diese Möglichkeit aufgrund der Erläuterungen des Sachverständigen aber für so unwahrscheinlich, dass sich daraus keine relevanten Zweifel an der Überzeugung (§ 286 Abs. 1 ZPO) ergeben, nach der die Registrierungsdaten durch Weiterleitung oder sonstige Weitergabe seitens der Klägerin zu 1 an die Täter gelangt sind und die Schilderung der Klägerin zu 1 damit widerlegt ist.

c) Aus der hier gebotenen Gesamtbetrachtung unter Berücksichtigung der ergänzenden Feststellungen des Senats ergibt sich, dass die Klägerin zu 1 die ihr gemäß § 675l Abs. 1 Satz 1 BGB obliegenden Pflichten grob fahrlässig verletzt hat (§ 675v Abs. 3 Nr. 2 Buchst. a BGB).

Wie bereits ausgeführt, erfordert grobe Fahrlässigkeit einen in objektiver Hinsicht schweren und in subjektiver Hinsicht schlechthin unentschuldbaren Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt. Diese Sorgfalt muss in ungewöhnlich hohem Maße verletzt und es muss dasjenige unbeachtet geblieben sein, was im gegebenen Fall jedem hätte einleuchten müssen. Selbst ein objektiv grober Pflichtenverstoß rechtfertigt für sich noch keinen zwingenden Schluss auf ein entsprechend gesteigertes personales Verschulden. Die Regeln des Anscheinsbeweises sind auf den Nachweis der subjektiven Voraussetzungen grober Fahrlässigkeit grundsätzlich dann nicht anwendbar, wenn es sich - wie hier - um ein individuelles Versagen handelt. Denn ein objektiv grober Pflichtenverstoß rechtfertigt für sich allein noch nicht den Schluss auf ein gesteigertes personales Fehlverhalten, selbst wenn dieses in vergleichbaren Fällen häufig vorliegen sollte. Die Regeln des Anscheinsbeweises können auch nicht zum Nachweis der objektiven Voraussetzungen grober Fahrlässigkeit des Zahlungsdienstnutzers im Online-Banking herangezogen werden (vgl.

© 2026 Wolters Kluwer Deutschland GmbH

BGH, Urteil vom 26. Januar 2016 - XI ZR 91/14, BGHZ 208, 331 Rn. 71, 73, 74 f.; Urteil vom 10. Oktober 2013 - III ZR 345/12, BGHZ 198, 265 Rn. 26; jeweils mwN).
Das Verhalten der Klägerin zu 1 im Zusammenhang mit dem Phishing-Vorfall vom 4. März 2021, das der Kläger zu 2 sich gemäß § 278 BGB zurechnen lassen muss, erfüllt diese Voraussetzungen. Der Senat macht sich insoweit grundsätzlich die nachfolgend zitierten Ausführungen des Landgerichts (LGU 14 ff., unter I 2 b bb) zu den hier vorliegenden Umständen zu eigen:

Nach dieser Maßgabe ist unter Berücksichtigung aller Umstände des hiesigen Einzelfalls das Verhalten der Klägerin zu 1) insofern als grob fahrlässig einzustufen, als dass sie auf den Link in der E-Mail geklickt und sodann auf der sich geöffneten, gefälschten Internetseite ihren Anmeldenamen und ihre PIN eingegeben hat. Denn sie erkannte trotz der ungewöhnlichen Art der Kontaktaufnahme durch die Täter und der Gestaltung der E-Mail, die massive Anhaltspunkte für einen Phishing-Angriff bot, nicht, dass es sich um einen Phishing-Angriff handelte.

Zunächst hätte bei der Klägerin zu 1) ein Verdacht bereits aufgrund des Umstands aufkommen müssen, dass sie über einen in einer E-Mail enthaltenen Link einer Bank zur Eingabe ihrer Daten aufgefordert wird. Bei einer derartigen Kontaktaufnahme liegt nahe, dass eine Überprüfung des Absenders der E-Mail geboten ist. Eine Bank fordert ihren Kunden nicht per E-Mail dazu auf, über einen Link ihre Internetseite aufzurufen.

Einem Kunden muss bekannt sein, dass keine Bank mittels E-Mail kontorelevante Maßnahmen hinsichtlich der Identifikation und Zugangsdaten sowie der Online-Banking-Funktionen im Allgemeinen erfordert, sondern solche Handlungen ausschließlich über das digitale Postfach oder per Brief einleitet (vgl. LG Essen, BeckRS 2015, 1693; Borges, NJW 2012, 2385 (2386)).

Zudem ist die äußere Gestaltung der E-Mail als zumindest auffällig zu bezeichnen. Die E-Mail war weder von der Beklagten noch im Logo der Beklagten gehalten, sondern erschien als E-Mail der "Sparkasse". Ungewöhnlich ist insofern zudem, dass der Link, den die Klägerin zu 1) öffnete, nach dem klägerischen Vortrag unmittelbar auf eine Eingabemaske einer (vermeintlichen) Sparkasse führte und nicht der Eingabemaske der Beklagten entsprach. Allein dieser Umstand hätte bei der Klägerin zu 1) Zweifel an der Seriosität der E-Mail aufkommen lassen müssen. Daran ändert auch der Umstand nichts, dass die Beklagte für ihr Angebot für das Online-Banking Software der Sparkasse - insbesondere die PushTAN-App - verwendet. Dennoch erfolgt der Zugang zum Online-Banking als solcher und die Nutzung der digitalen Bankfiliale ausschließlich über die Website der Beklagten und nicht über die einer nicht näher benannten Sparkasse. So wird in Ziff. 8 der Rahmenvereinbarung über die Teilnahme am Online-Banking (Anlage B3) ausschließlich die Homepage der Rechtsvorgängerin der Beklagten als Kommunikationsweg genannt. Ob die Beklagte im Rahmen der Kommunikation mit den Klägern stets mit Ortsbezug oder jedenfalls teilweise unter der bloßen Bezeichnung "Sparkasse" aufgetreten ist, was zwischen den Parteien streitig ist, kann dahingestellt bleiben. Aus diesem Grunde bedurfte es auch nicht der von den Klägern in der mündlichen Verhandlung vom 19.06.2023 beantragten Vernehmung der weiteren Zeugin.

Auch der angegebene Absender "(...)" hätte die Klägerin zu 1) misstrauisch werden lassen müssen, da es sich bei diesem weder um die Beklagte noch um eine gängige Domain der Sparkassen handelt. Dies hat der Zeuge FF in seiner Aussage glaubhaft bekundet.

Als weiterer Verdachtsmoment kommt hinzu, dass die E-Mail nicht an die Kläger persönlich adressiert war, sondern die neutrale Formulierung "Sehr geehrter Kunde" verwendete. Die E-Mail weist auch eine auffällige Häufung von Unregelmäßigkeiten bei der Rechtschreibung auf, so wird die Anrede "Ihre" bzw. "ihre" teilweise groß, teilweise klein geschrieben, gleiches gilt für die Formulierung "S-PushTAN" bzw. "SpushTAN". Weiter heißt es "aktualiseren" anstelle von "aktualisieren".

Darüber hinaus war die Klägerin zu 1), die zugleich Mitarbeiterin der Beklagten ist, bereits seit 2013 mit dem Online-Banking vertraut. Zwar hat die Klägerin erst im Dezember 2021 von dem SMS-TAN-Verfahren auf das PushTAN-Verfahren gewechselt, allein dieser Wechsel des TAN-Verfahrens stellt jedoch keine derart erhebliche Veränderung dar, die dazu führt, dass es sich der Klägerin zu 1) nicht hätte aufdrängen müssen, dass hier möglicherweise ein Phishing-Angriff vorlag. Denn das Phänomen der Versendung von E-Mails, um an die sensiblen Daten Dritter zu kommen, steht nicht in Zusammenhang mit dem konkret genutzten TAN-Verfahren.

Die Kammer ist auch überzeugt davon, dass die Beklagte durch einen über ihre Online-Banking-Seite zugänglichen Warnhinweis zum damaligen Zeitpunkt vor vergleichbaren Phishing-Attacken via E-Mail gewarnt hat. Die Beklagte hat hierzu einen Screenshot mitsamt Datum der Veröffentlichung vorgelegt (Bl. 28 Bd. I), auf den wegen der Einzelheiten verwiesen wird. Zudem hat der Zeuge FF auf Vorhalt des entsprechenden Sicherheitshinweises glaubhaft bekundet, dass ein Hinweis in dieser Form am 16.02.2021 aufgenommen worden ist. Es hätte so an der Klägerin gelegen, sich nach Erhalt der E-Mails über etwaige Sicherheitshinweise über das Internet oder persönlich bei der Beklagten zu informieren. Unabhängig davon ist aufgrund der in den letzten Jahren vielfach in den Medien thematisierten Fälle die Erkenntnis, dass Kunden durch betrügerische Anrufe und E-Mails zur Preisgabe von Zugangsdaten zum Online-Banking auf gefälschten Webseiten veranlasst werden sollen, als Allgemeinwissen vorauszusetzen (vgl.

© 2026 Wolters Kluwer Deutschland GmbH

OLG Hamm v. 16.03.2015 31 U 31/15; LG Zweibrücken v. 23.01.2023 2 O 130/22 - beides zit. nach juris; Landgericht Essen a.a.O.). Die Klägerin zu 1) hätte von der Möglichkeit derartiger betrügerischer Vorgänge, wenn auch in unterschiedlicher Ausgestaltung, jedenfalls allgemein Kenntnis haben müssen.
Dass die Klägerin zu 1) im Vorfeld des 04.03.2021 mehrere gleichgelagerte E-Mails erhalten hat, entkräftet den Vorwurf der groben Fahrlässigkeit nicht. Vielmehr hätte es durchaus nahegelegen, sich binnen des hierdurch entstandenen Zeitraums durch Rückfrage bei der Kundenberaterin oder Recherche im Internet nach der Ordnungsmäßigkeit des Vorgangs zu erkundigen.

Sämtliche der vorgenannten Verdachtsmomente ignorierte die Klägerin zu 1) jedoch. Bei Gesamtbetrachtung sämtlicher Umstände des hiesigen Falles stellt sich das Handeln der Klägerin zu 1) - dem Kläger zu 2) zurechenbar - als objektiv schwerwiegender und subjektiv nicht entschuldbarer Verstoß gegen die Anforderungen der im Verkehr erforderlichen Sorgfalt dar. Es hätte sich der Klägerin zu 1) aufdrängen müssen, dass die Beklagte nicht die Urheberin der streitgegenständlichen E-Mail war.

Jedenfalls aufgrund der vom Senat darüber hinaus festgestellten weiteren Pflichtverletzung bleibt es bei dieser Beurteilung auch dann, wenn man die vom Landgericht zutreffend aufgezeigten Auffälligkeiten hinsichtlich der äußeren Gestaltung, der Absenderadresse, der Anrede sowie der Rechtschreibung der Phishing-E-Mail als weniger gravierend einordnet und darüber hinaus die Kontaktaufnahme durch eine an den gewöhnlichen E-Mail-Account des Kunden versandte E-Mail mit einem darin enthaltenen Link zur Eingabe kontorelevanter Daten für ungewöhnlich hält, aber nicht die Auffassung des Landgerichts teilt, einem Bankkunden müsse bekannt sein, dass ein Kreditinstitut solche Handlungen ausschließlich über das Online-Banking-Postfach oder per Brief einleitet.

Denn nach den Feststellungen des Senats kommt zu der Eingabe von sensiblen Daten nach Öffnen einer E-Mail und Klicken eines Links, der in dieser an den gewöhnlichen E-Mail-Account der Klägerin zu 1 und nicht an das Postfach des Online-Banking-Accounts versandten Nachricht enthalten war, zwangsläufig eine weitere Preisgabe von Daten, die erst in einem zweiten Schritt - nämlich nach Eingang der SMS mit dem PushTAN-Registrierungs-Link - erfolgt sein kann. Aus den dargestellten Gründen sind zwar keine konkreteren Feststellungen dazu möglich, wie die Klägerin zur Weitergabe des Registrierungs-Links beziehungsweise des entsprechenden Codes aufgefordert wurde und wie die Weitergabe erfolgt ist. Vielmehr gilt insoweit, wie bereits ausgeführt, der Vortrag der Beklagten, die Klägerin zu 1 habe entweder die auf ihrem Mobiltelefon eingegangene SMS mit dem Registrierungs-Link an die Betrüger weitergeleitet oder die Daten aus der SMS manuell abgetippt und auf der Phishing-Homepage in eine dafür vorgesehene Maske eingegeben (Schriftsatz vom 28. Oktober 2021, S. 4 = GA I 45), gemäß § 138 Abs. 3 ZPO als zugestanden. Alle danach in Betracht kommenden Aufforderungen zur Weitergabe der Registrierungsdaten stellen sich aber - auch im Zusammenhang mit der dargestellten, kurz zuvor erfolgten Kontaktaufnahme und Aufforderung zur Eingabe von sensiblen Daten nach Klicken eines in einer an den gewöhnlichen E-Mail-Account versandten E-Mail enthaltenen Links - als sehr ungewöhnlich dar. Spätestens aufgrund dieser ungewöhnlichen Aufforderung hätte die Klägerin zu 1 unbedingt argwöhnisch werden und den Vorgang sofort abbrechen müssen. Dabei geht der Senat, wie bereits in der Ladungsverfügung dargestellt, davon aus, dass die Registrierungs-SMS nur den in Anlage K4 (Anlagenband Kläger) dargestellten Inhalt hatte und nicht auch den im Schriftsatz der Beklagten vom 13. Juni 2022 auf Seite 2 (GA I 190R) dargestellten Warnhinweis ("*Bitte leiten Sie diese SMS nicht an dritte Personen weiter! Kein Mitarbeiter wird sie um Weitergabe dieser Daten bitten.*") enthielt. Denn auch ohne diesen Hinweis ist für Kundinnen und Kunden erkennbar, dass die SMS zur PushTAN-Registrierung keinen Inhalt hat, der üblicherweise weitergegeben oder an anderer Stelle eingegeben wird (wie etwa beim sogenannten SMS-TAN-Verfahren). Bei dieser Würdigung geht der Senat davon aus, dass die Klägerin zu 1 nur als Kundin (nicht als Mitarbeiterin der Beklagten) mit dem Online-Banking befasst war und dabei - ebenso wie allgemein bei der Nutzung von Computern und Smartphones - nur über durchschnittliche Kenntnisse und Erfahrungen verfügte. Der Senat berücksichtigt ferner, dass die Klägerin zu 1 zum Zeitpunkt der Eingabe beziehungsweise Weitergabe der Daten unter Stress stand und - aufgrund des Inhalts der Phishing-Mail - davon ausging, dass ihre PushTAN-Registrierung nach dem 6. März 2021 ablaufen und eine Neuregistrierung erforderlich werden würde, falls sie nicht handelt, was aus Sicht der Klägerin zu 1 auch wegen ihrer familiären Situation (Stellung als Alleinverdienerin, siehe BB 12 = GA III 32) schwerwiegend gewesen wäre. Diese Faktoren mögen die Urteilsfähigkeit der Klägerin zu 1 in der konkreten Situation eingeschränkt haben. Mit der Phishing-Mail und der anschließenden zweimaligen Aufforderung zur Preisgabe verschiedener sensibler Daten liegt aber eine solche Vielzahl von ungewöhnlichen Umständen vor, dass die Klägerin zu 1 hier auch unter Berücksichtigung der angespannten Gesamtsituation dasjenige unbeachtet gelassen hat, was im konkreten Fall jedem hätte einleuchten müssen.

d) Entgegen der Auffassung der Kläger ist der Schadensersatzanspruch der Beklagten aus § 675v Abs. 3 Nr. 2 Buchst. a BGB nicht infolge eines Mitverschuldens der Beklagten gemäß § 254 Abs. 1 BGB reduziert. Ein solches Mitverschulden ergibt sich weder aus der Verwendung des PushTAN-Verfahrens an sich noch daraus, dass die Klägerin zu 1 keinen Hinweis von der Beklagten erhalten hat, als sich ein fremdes Smartphone mit ihrer PushTAN-App registriert hat und das Handy der Klägerin gelöscht worden ist (GA III 122 f.).

Der Sachverständige hat zwar insbesondere die Versendung von Registrierungs-SMS für das PushTAN-Verfahren als "kein sonderlich sicheres Verfahren" bezeichnet (GA II 89). Das PushTAN-Verfahren ist jedoch verbreitet und üblich. Außerdem ergibt sich aus den Erläuterungen des Sachverständigen, dass es fortlaufend verbessert und dadurch der Schutz gegen Angriffe von

© 2026 Wolters Kluwer Deutschland GmbH

Straftätern erhöht wird. Unter diesen Umständen kann keine Rede davon sein, dass die Beklagte durch Verwendung des PushTAN-Verfahrens die Sorgfalt außer Acht gelassen hat, die eine verständige Person im eigenen Interesse aufwendet, um sich vor einem Schaden zu bewahren (vgl. MünchKommBGB/Oetker, 9. Aufl. 2022, § 254 Rn. 30 mwN). Entsprechendes gilt, soweit die Beklagte die Klägerin zu 1 nicht über die Registrierung eines anderen Smartphones informiert hat, und zwar auch dann, wenn die Beklagte inzwischen entsprechend verfährt und ihre Nutzer darauf hinweist, dass sie ihr Konto sofort sperren lassen sollen, wenn sie die Registrierung nicht selbst vorgenommen haben. Denn es ist weder vorgetragen noch sonst ersichtlich, dass Fälle der vorliegenden Art zum maßgeblichen Zeitpunkt (4. März 2021) in einem Ausmaß aufgetreten und der Beklagten bekannt geworden waren, dass das Unterlassen der dargestellten Sicherheitsmaßnahmen als Verletzung der Sorgfalt in eigenen Angelegenheiten anzusehen wäre.

Nichts anderes gilt schließlich auch für den vom Senat festgestellten und bereits erörterten Umstand, dass die Registrierungs-SMS nicht den inzwischen verwendeten Warnhinweis ("*Bitte leiten Sie diese SMS nicht an dritte Personen weiter! Kein Mitarbeiter wird sie um Weitergabe dieser Daten bitten.*") enthielt. Dabei übersieht der Senat nicht, dass der Sachverständige dies im schriftlichen Gutachten vom 16. Oktober 2022 als problematisch angesehen und bemängelt hat, dass ein Phishing-Opfer durch den Text der SMS nicht misstrauisch werde (S. 17, ferner auch S. 15 f.). Auch insofern ist aber weder vorgetragen noch sonst ersichtlich, dass im März 2021 das Unterlassen dieses Warnhinweises als Verletzung der Sorgfalt in eigenen Angelegenheiten anzusehen wäre.

Die spätere Einführung entsprechender Warnhinweise (bei Registrierung eines anderen Geräts für das PushTAN-Verfahren und schon vorher im Text der SMS) rechtfertigt ebenfalls nicht den Schluss, dass diese Maßnahmen - überhaupt und erst recht zum damaligen Zeitpunkt - zur Vermeidung des Vorwurfs einer Verletzung der Sorgfalt in eigenen Angelegenheiten erforderlich gewesen wären. Vielmehr zeigt die jeweils offenbar geänderte Praxis der Beklagten gerade, dass diese die Entwicklung der Angriffsmethoden der Täter im Bereich Phishing zur Kenntnis nimmt und ihre Sicherheitsmaßnahmen aufgrund dieser Kenntnisse fortlaufend verbessert. Das spricht nicht für, sondern gegen ein Mitverschulden der Beklagten.

3. Die Nebenentscheidungen beruhen hinsichtlich der Kosten auf § 97 Abs. 1 ZPO und hinsichtlich der vorläufigen Vollstreckbarkeit auf § 708 Nr. 10, § 711 ZPO. Die Voraussetzungen für eine Zulassung der Revision (§ 543 Abs. 2 ZPO) liegen nicht vor.

Hinweis:

Verkündet am: 24.04.2025

Hinweis:

Hinweis: Das Dokument wurde redaktionell aufgearbeitet und unterliegt in dieser Form einem besonderen urheberrechtlichen Schutz. Eine Nutzung über die Vertragsbedingungen der Nutzungsvereinbarung hinaus - insbesondere eine gewerbliche Weiterverarbeitung außerhalb der Grenzen der Vertragsbedingungen - ist nicht gestattet.

© 2026 Wolters Kluwer Deutschland GmbH