BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

XI ZR 107/24

Verkündet am:
22. Juli 2025
Weber,
Justizamtsinspektorin
als Urkundsbeamtin
der Geschäftsstelle

in dem Rechtsstreit

Nachschlagewerk: ja

BGHZ: nein

BGHR: ja

JNEU: ja

BGB § 675v Abs. 3 Nr. 2 Buchst. a, § 675v Abs. 4 Satz 1 Nr. 1

a) Zur grob fahrlässigen Verletzung einer Pflicht durch den Zahler im Sinne von § 675v Abs. 3 Nr. 2 Buchst. a BGB.

b) Ist der Schaden durch eine Überweisung eingetreten und hat der Zahlungsdienstleister für das Auslösen dieser Überweisung eine starke Kundenauthentifizierung gemäß § 1 Abs. 24 ZAG verlangt, ist sein Schadensersatzanspruch aus § 675v Abs. 3 BGB gegen den Zahler nicht gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB ausgeschlossen, unabhängig davon, ob der Zahlungsdienstleister für die Anmeldung im Online-Banking eine starke Kundenauthentifizierung verlangt hat.

BGH, Urteil vom 22. Juli 2025 - XI ZR 107/24 - OLG Naumburg
LG Halle

ECLI:DE:BGH:2025:220725UXIZR107.24.0

Der XI. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 22. Juli 2025 durch den Vizepräsidenten Prof. Dr. Ellenberger, die Richter Dr. Grüneberg und Dr. Matthias, die Richterin Dr. Derstadt und den Richter Dr. Schild von Spannenberg

für Recht erkannt:

Die Revision der Kläger gegen das Urteil des 5. Zivilsenats des Oberlandesgerichts Naumburg vom 22. Mai 2024 wird auf ihre Kosten zurückgewiesen.

Von Rechts wegen

Tatbestand:

1 Die Kläger verlangen von der beklagten Sparkasse, eine Belastungsbuchung auf ihrem Girokonto rückgängig zu machen.

2 Die Kläger führen bei der Beklagten ein Gemeinschaftsgirokonto. Am 3. Juni 2014 vereinbarten die Parteien, dass die Kläger künftig Aufträge zu diesem Konto per Online-Banking erteilen können. Nach der Vereinbarung waren zur Anmeldung im Online-Banking ein persönlicher Anmeldename sowie eine Geheimzahl (PIN) und für den jeweiligen Auftrag eine im sogenannten chipTAN-Verfahren mittels eines gesonderten Geräts, eines TAN-Generators, dynamisch erzeugte Transaktionsnummer (TAN) einzugeben.

3 Am 2. Juli 2022, einem Samstag, versuchte die Klägerin mehrfach, die PIN, die zum Einloggen in das Online-Banking auf der Internetseite der Beklagten erforderlich ist, zu ändern, weil sie diese und ihren Benutzernamen aus Versehen abgespeichert hatte. Trotz mehrfacher Versuche gelang ihr die Änderung der PIN nicht. Dabei zeigte der TAN-Generator jeweils "Vorgang abgebrochen" an. Als die Klägerin am gleichen Tag gegen 22:30 Uhr noch einmal versuchte, die PIN zu ändern, öffnete sich auf ihrem PC ein Fenster, welches darauf hinwies, dass der Online-Banking-Zugang binnen eines Tages ablaufe, wenn nicht eine neue Sicherheitssoftware installiert werde. Die Klägerin klickte darauf, woraufhin sich ein neues Fenster öffnete und persönliche Angaben abgefordert wurden. Die Klägerin behauptet, dieses Fenster sofort wieder geschlossen zu haben.

4 Wenige Augenblicke später erhielt die Klägerin einen Telefonanruf. Auf dem Display wurde die Telefonnummer der Beklagten angezeigt und die Anruferin stellte sich als Mitarbeiterin der Beklagten vor. Sie erkundigte sich, was denn bei der Klägerin "los sei". Die Klägerin teilte mit, dass sie versucht habe, die PIN zu ändern. Daraufhin erklärte die Anruferin, dass die Installation eines neuen Sicherheitsprogramms erforderlich sei. In diesem Zusammenhang nannte die Anruferin auch den Namen der für die Kläger zuständigen Sachbearbeiterin der Beklagten. Da es bereits gegen 23 Uhr war, erkundigte sich die Klägerin bei der Anruferin, warum diese noch so spät anrufe. Die Anruferin erklärte, sie sei Mitarbeiterin im Online-Banking und "24 Stunden rund um die Uhr für die Kunden da". Die Klägerin hielt dies für schlüssig, weil sie sich daran erinnerte, bei einem USA-Urlaub in einer Kreditkartenangelegenheit die Beklagte zu nächtlicher Stunde (Ortszeit in Deutschland) telefonisch erreicht zu haben.

5 Die Anruferin teilte mit, dass die Klägerin sich identifizieren müsse, und forderte die Klägerin dazu auf, die Zahlenfolge ihrer Sparkassen-Kartennummer

anzugeben, wobei die Anruferin die ersten drei Ziffern vorgab. Zur weiteren Legitimation nannte die Anruferin die letzten drei Buchungsvorgänge, die auf dem Konto der Kläger erfolgt waren. Sie bot an, den Identifizierungsvorgang für das vermeintlich neue Sicherheitsprogramm mit dem TAN-Generator durchzuführen. Die Klägerin war einverstanden und die Anruferin teilte mit, dass sie nun Zahlenfolgen durchgeben werde, die die Klägerin in ihren TAN-Generator eingeben müsse, um dann im Gegenzug der Anruferin die generierte TAN durchzugeben. Die Klägerin, die bis zu diesem Zeitpunkt nur das Flickercode-Verfahren genutzt hatte, folgte den Anweisungen, "vertippte" sich jedoch mehrfach. Das Gespräch brach dann unvermittelt ab.

6 Die Anruferin meldete sich sodann erneut unter der Telefonnummer der Beklagten und gab wieder eine Zahlenfolge durch. Ausweislich der von der Beklagten vorgelegten Transaktionsprotokolle wurde im Online-Banking um 22:50 Uhr unter Verwendung der ersten von der Klägerin erzeugten TAN das Tageslimit temporär auf 111.111 € erhöht. Anschließend wurden nacheinander drei Überweisungen von jeweils 36.666 € in Auftrag gegeben, die sämtlich aufgrund der Eingabe einer falschen TAN nicht ausgeführt wurden. Dann teilte die Anruferin mit, dass die Bestätigung möglichweise aufgrund Zeitablaufs nicht mehr möglich sei, und bot an, den Vorgang am Folgetag fortzusetzen. Die Frage der Klägerin, ob dies bereits um 8 Uhr möglich sei, verneinte die Anruferin, weil sie erst ab 11:30 Uhr bis 20 Uhr im Dienst sei. Daraufhin wurde der Anruf für 18 Uhr vereinbart. Anschließend loggte sich die Klägerin im Online-Banking ein und stellte nichts Ungewöhnliches fest.

7 Am nächsten Tag, dem 3. Juli 2022, einem Sonntag, fuhren die Kläger wie geplant in den Urlaub. Da die Klägerin den Anruf erwartete, nahm sie den TAN-Generator und ihre Sparkassenkarte mit. Gegen 18:15 Uhr meldete sich die An-

ruferin des Vortages unter der Telefonnummer der Beklagten auf dem Mobiltelefon der Klägerin, wiederholte die Prozedur mit der Abfrage der Sparkassen-Kartennummer der Klägerin und gab sodann wiederum mehrere Zahlenfolgen durch, die von der Klägerin in den TAN-Generator eingegeben wurden. Die Klägerin gab dann die generierte TAN an die Anruferin weiter. Schließlich teilte die Anruferin mit, dass alles geklappt habe und verabschiedete sich. Im Verlauf dieses Telefonats generierte die Klägerin mit dem TAN-Generator im manuellen chipTAN-Verfahren mehrere TANs, die sie an die Anruferin weitergab. Zur selben Zeit wurden im Online-Banking der Kläger mehrere Vorgänge ausgelöst. So wurde um 18:24:22 Uhr das Überweisungslimit auf 55.555 € bis 23:59 Uhr desselben Tages erhöht. Um 18:26:26 Uhr wurde eine Echtzeit-Überweisung in Höhe von 35.555 € zugunsten des Kontos einer den Klägern unbekannten Person bei einer anderen Bank beauftragt, durch Eingabe der entsprechend individuell generierten TAN freigeschaltet und ausgeführt.

8 Mit ihrer Klage begehren die Kläger, das bei der Beklagten geführte Konto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung vom 3. Juli 2022 in Höhe von 35.555 € befunden hätte, sowie die Erstattung vorgerichtlicher Rechtsanwaltskosten nebst Rechtshängigkeitszinsen. Das Landgericht hat der Klage im Wesentlichen stattgegeben. Auf die Berufung der Beklagten hat das Berufungsgericht nach persönlicher Anhörung der Klägerin die Klage abgewiesen. Mit der vom Senat zugelassenen Revision erstreben die Kläger die Wiederherstellung des landgerichtlichen Urteils.

Entscheidungsgründe:

9 Die Revision ist unbegründet.

I.

10 Das Berufungsgericht hat zur Begründung seiner unter anderem in ZIP 2025, 23 veröffentlichten Entscheidung im Wesentlichen ausgeführt:

11 Die Kläger hätten zwar gegen die Beklagte einen Anspruch aus § 675u Satz 2 BGB, weil die der streitgegenständlichen Belastungsbuchung in Höhe von 35.555 € zugrundeliegende Echtzeit-Überweisung nicht gemäß § 675j Abs. 1 BGB durch die Kläger autorisiert worden sei. Das Berufungsgericht sei aufgrund der Würdigung des Inhalts der gesamten Verhandlung davon überzeugt, dass ein unbefugter Dritter, der aufgrund einer Anmeldung auf einer gefälschten Webseite oder aufgrund eines anderweitigen vorangegangenen und unbemerkt gebliebenen Angriffs die Online-Banking-Zugangsdaten der Kläger gekannt habe, im Online-Banking jeweils mittels der von der arglosen Klägerin erzeugten TANs die Erhöhung des Überweisungslimits auf 55.555 € und die Echtzeit-Überweisung in Höhe von 35.555 € beauftragt und bestätigt habe, während die Klägerin die TANs in dem Glauben, eine Bankmitarbeiterin sei ihr bei der Installation eines neuen Sicherheitsprogramms behilflich, erzeugt und weitergegeben habe.

12 Dem Anspruch der Kläger aus § 675u Satz 2 BGB könne jedoch die Beklagte gemäß § 242 BGB einen Schadensersatzanspruch aus § 675v Abs. 3 Nr. 2 BGB in gleicher Höhe entgegenhalten. Die Klägerin habe grob fahrlässig gegen ihre Sorgfaltspflichten verstoßen, indem sie sich auf die telefonische Installation eines „neuen Sicherheitsprogrammes“ eingelassen, die TAN erzeugt und an die Anruferin weitergegeben habe.

13 Dabei könne dahinstehen, ob die Parteien die von der Beklagten vorgelegten "Bedingungen für das Online-Banking" wirksam einbezogen hätten. Denn

bereits nach § 675l Abs. 1 Satz 1 BGB sei der Zahlungsdienstnutzer verpflichtet, unmittelbar nach Erhalt eines Zahlungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Hierzu gehörten auch alle Arten von TANs. Überdies sei aufgrund der umfangreichen Berichterstattung in den letzten Jahren in den öffentlichen Medien zu den vielfachen und mannigfaltigen Angriffen beim Internet-Banking allgemein bekannt, dass die TAN ausschließlich zur Bestätigung eines in Auftrag gegebenen Vorgangs verwendet werden solle.

14 Von der Klägerin, die nach eigenen Angaben das Online-Banking seit 2014 nutze, sei zu erwarten gewesen, dass sie den hier erfolgten Angriff abwehre. Es hätte sie schon stutzig machen müssen, als sich am Abend des 2. Juli 2022 auf ihrem PC ein Fenster geöffnet habe, mit dem persönliche Angaben abgefordert worden seien. Für die Klägerin sei erkennbar gewesen, dass diese Mitteilung ungewöhnlich gewesen sei. Denn nach ihren eigenen Angaben habe sie dieses Fenster sofort wieder geschlossen. Umso mehr hätte sie erstaunen müssen, dass sie unmittelbar darauf und erstmals nach mehreren Jahren Teilnahme am Internet-Banking am Wochenende von einer vermeintlichen Mitarbeiterin der Beklagten zur Identifizierung für ein neues Sicherheitsprogramm angerufen worden sei. Auch wenn der Klägerin die Möglichkeit, eine Anrufernummer vorzutäuschen (Call-ID-Spoofing), nicht bekannt gewesen sein sollte, sei ihr die Unüblichkeit von Anrufen eines Bankmitarbeiters am Wochenende bewusst gewesen. Im Rahmen ihrer persönlichen Anhörung habe die Klägerin zwar angegeben, selbst häufig bei der Sparkasse angerufen, Angelegenheiten telefonisch geregelt und auch aus dem Ausland angerufen zu haben. Daran, dass Mitarbeiter der Beklagten sie ohne vorherige Anfrage durch die Kläger angerufen hätten, habe sich die Klägerin allerdings nicht erinnern können. Außerdem hätten die vorangegangenen Telefonate der Klägerin mit der Beklagten nie das Online-Banking betroffen.

Sehr ungewöhnlich sei auch gewesen, dass die Installation des "neuen Sicherheitsprogrammes" noch am selben Tag habe erforderlich sein und außerhalb üblicher Banköffnungszeiten an einem Samstagabend habe erfolgen sollen. Die Klägerin habe angesichts des Inhalts der von den Klägern vorgelegten Rahmenvereinbarung über die Teilnahme am Online-Banking auch nicht davon ausgehen dürfen, die Beklagte habe einen telefonischen Beratungszugang zum Online-Banking eröffnet. Der Umstand, dass die Klägerin während einer USA-Reise zur (deutschen) Nachtzeit ein "Institut der Beklagten" bzw. einen "Servicemitarbeiter der Beklagten" erreicht habe, entlaste die Klägerin nicht, Verdachtsmomente bei den hier streitgegenständlichen Telefonaten am 2. und 3. Juli 2022 wahrzunehmen und pflichtgemäß zu handeln.

15 Die Klägerin hätte spätestens alarmiert sein müssen, nachdem sie aufgefordert worden sei, ihren TAN-Generator zu verwenden, mit dem sie bis dahin selbst nur TANs zur Autorisierung von im Online-Banking ausgelösten Zahlungsvorgängen generiert habe. Es entlaste die Kläger auch nicht, dass sie bis dahin nur das optische chipTAN-Verfahren genutzt hätten und insbesondere der Klägerin das manuelle chipTAN-Verfahren unbekannt gewesen sei. Bei Wahrung der erforderlichen Sorgfalt hätte sich ihr aufdrängen müssen, dass sie den TAN-Generator wie bisher auch dieses Mal zur Erzeugung von TANs benutze, die zur Bestätigung von Zahlungsvorgängen im Online-Banking benötigt würden. Die Klägerin habe im Rahmen des ersten Telefonats insgesamt vier TANs erzeugt. Ab der zweiten TAN hätte sie auch bei Anwendung des manuellen chipTAN-Verfahrens auf ihrem TAN-Generator sehen können, dass sie jeweils eine Empfänger-IBAN und einen Überweisungsbetrag eingegeben habe. Die der Klägerin abverlangte Eingabe einer Empfänger-IBAN und eines Überweisungsbetrags von 36.666 € habe sich mit der angeblichen Identifizierung für die Installation eines neuen Sicherheitsprogramms nicht vereinbaren lassen.

16 Schlichtweg unverständlich sei, dass die Klägerin das Geschehen nicht einmal im Nachhinein reflektiert habe und sich am Folgetag auf ein erneutes Telefonat eingelassen und zwei weitere TANs generiert und weitergegeben habe, wobei sie beim zweiten Mal wieder eine Empfänger-IBAN und einen Überweisungsbetrag, diesmal 35.555 €, eingegeben habe. Auch wenn sich am Kontostand nach dem ersten Anruf nichts geändert habe, sei von der Klägerin zu erwarten gewesen, dass sie sich vor einem erneuten Telefonat am Folgetag zu der angeblichen Installation eines neuen Identifizierungsverfahrens selbst bei der Beklagten erkundigt oder auf sonstige Weise vergewissert, dass es sich bei der Anruferin tatsächlich um eine Mitarbeiterin der Beklagten handelt.

17 Die Klägerin habe mithin in der von den üblichen Vorgängen abweichenden Situation ganz naheliegende Überlegungen nicht angestellt und jegliche Vorsicht vermissen lassen. Ihr hätte sich wie jedem anderen Zahlungsdienstnutzer in dieser Situation aufdrängen müssen, dass sie möglicherweise nicht mit der Beklagten, sondern einem Dritten kommuniziere. Bei der insoweit erforderlichen Gesamtbetrachtung sämtlicher Umstände stelle sich das Handeln der Klägerin als objektiv schwerwiegender und subjektiv nicht entschuldbarer Verstoß gegen die Anforderungen der im Verkehr erforderlichen Sorgfalt dar. Aufgrund der mit der Beklagten vereinbarten Einzelverfügungsbefugnis müsse der Kläger sich die Pflichtverletzung der Klägerin zurechnen lassen.

18 Der Schadensersatzanspruch der Beklagten sei nicht nach § 675v Abs. 4 Satz 1 Nr. 1 BGB ausgeschlossen, auch wenn sie bei der Anmeldung im Online-Banking keine starke Kundenauthentifizierung verlangt habe. Es könne insoweit dahinstehen, ob nach der Anmeldung im Online-Banking nur die Kontobewegungen, aber keine sensiblen Daten wie Geburtsdatum, Telefonnummer und Kartennummer des Kunden hätten eingesehen werden können und sich die Beklagte deshalb auf die Ausnahmevorschrift des Art. 10 der Delegierten Verordnung (EU)

2018/389 der Kommission vom 27. November 2017 (ABl. 2018, L 69, S. 23, berichtigt in ABl. 2020, L 88, S. 11, künftig: Delegierte VO (EU) 2018/389) berufen könne. Denn es lasse sich schon nicht ausschließen, dass die unbekannten Täter Geburtsdatum, Telefonnummer und Kartennummer der Kläger bereits vorher durch einen Phishingangriff erlangt hätten. Im Übrigen ergebe sich aus dem Gesamtzusammenhang der gesetzlichen Regelung, dass der Haftungsausschluss nach § 675v Abs. 4 Satz 1 Nr. 1 BGB nur eingreife, wenn der Zahlungsdienstleister bei dem konkreten Zahlungsvorgang keine starke Kundenauthentifizierung verlangt habe. Dies sei hier aber nicht der Fall gewesen.

19 Die Beklagte müsse sich auch nicht ein anspruchsminderndes Mitverschulden nach § 254 BGB anrechnen lassen. Wenn unterstellt werde, die Täter hätten aufgrund einer pflichtwidrig nicht verlangten starken Kundenauthentifizierung bei der ersten Anmeldung im Online-Banking das Geburtsdatum der Klägerin, ihre Telefonnummer und die Kartennummer erfahren und Kenntnis von den letzten Kontobewegungen erlangt, hätte dies den Tätern zwar ermöglicht, den Anschein zu erwecken, ein Bankmitarbeiter rufe die Klägerin an. Dies hätte aber nicht zu dem hier geltend gemachten Schaden führen müssen, weil von der Klägerin zu erwarten gewesen sei, dass sie diesen Angriff abwehre. Der Verursachungsbeitrag der Beklagten trete hinter dem maßgeblichen und schwerwiegenden Verursachungsbeitrag der Kläger zurück.

II.

20 Diese Ausführungen halten einer revisionsrechtlichen Überprüfung stand.

21 1. Rechtsfehlerfrei ist das Berufungsgericht davon ausgegangen, dass den Klägern ein Anspruch gegen die Beklagte aus § 675u Satz 2 BGB zusteht.

Im Fall eines nicht autorisierten Zahlungsvorgangs, der zur Belastung des Zahlungskontos des Zahlers geführt hat, ist der Zahlungsdienstleister nach § 675u Satz 2 Halbsatz 2 BGB verpflichtet, das Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. Das Berufungsgericht hat in revisionsrechtlich nicht zu beanstandender Weise (vgl. Senatsurteil vom 5. März 2024 - XI ZR 107/22, BGHZ 240, 23 Rn. 46 mwN) angenommen, dass die streitgegenständliche Überweisung vom 3. Juli 2022 nicht von der Klägerin autorisiert worden ist. Gegen diese Beurteilung hat auch die Revisionserwiderung nichts erinnert.

22 2. Die Beklagte kann aber, wie das Berufungsgericht ebenfalls rechtsfehlerfrei angenommen hat, dem Anspruch der Kläger aus § 675u Satz 2 BGB gemäß § 242 BGB entgegenhalten, dass ihr wegen des nicht autorisierten Zahlungsvorgangs ein Schadensersatzanspruch gegen die Kläger zusteht.

23 a) Auch wenn § 675u Satz 1 und 2 BGB Ansprüche des Zahlungsdienstleisters ausschließt, die als Folge einer fehlenden Autorisierung in der Sache darauf gerichtet sind, dem Zahlungsdienstleister einen Anspruch auf Erstattung seiner Aufwendungen gegen den Zahler zu gewähren, können gleichwohl bei fehlender Autorisierung Schadensersatzansprüche des Zahlungsdienstleisters gegen den Zahler bestehen, selbst wenn sie wirtschaftlich vollständig an die Stelle des nach § 675u Satz 1 BGB entfallenden Aufwendungsersatzanspruchs treten. Besteht ein Schadensersatzanspruch des Zahlungsdienstleisters, kann letzterer in Höhe dieses Anspruchs die Erfüllung des Anspruchs des Zahlers aus § 675u Satz 2 BGB gemäß den Grundsätzen von Treu und Glauben verweigern (Senatsurteile vom 17. November 2020 - XI ZR 294/19, BGHZ 227, 343 Rn. 23 ff. und vom 5. März 2024 - XI ZR 107/22, BGHZ 240, 23 Rn. 50).

24 b) Das Berufungsgericht hat rechtsfehlerfrei das Bestehen eines Schadensersatzanspruchs der Beklagten wegen der nicht autorisierten Überweisung aus § 675v Abs. 3 Nr. 2 BGB bejaht.

25 aa) Nach § 675v Abs. 3 Nr. 2 BGB ist der Zahler seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Zahler den Schaden durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Pflichten gemäß § 675l Abs. 1 BGB oder einer oder mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments herbeigeführt hat. Gemäß § 675l Abs. 1 Satz 1 BGB ist der Zahlungsdienstnutzer verpflichtet, unmittelbar nach Erhalt eines Zahlungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Solche Sicherheitsmerkmale sind auch TANs (vgl. Senatsurteil vom 25. Juli 2017 - XI ZR 260/15, BGHZ 215, 292 Rn. 29; Grüneberg/Grüneberg, BGB, 84. Aufl., § 675l Rn. 2; Maihold in Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rn. 71, 264; Kirchner, RdZ 2025, 44, 45 f.). Ob der Zahler grob fahrlässig gehandelt hat, richtet sich nach den allgemeinen Grundsätzen des § 276 BGB (BT-Drucks. 18/11495, S. 165 f.; Grüneberg/Grüneberg, aaO § 675v Rn. 9; Nobbe in Ellenberger/Findeisen/Nobbe/Böger, Kommentar zum Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 81).

26 bb) Die Annahme des Berufungsgerichts, die Klägerin habe grob fahrlässig gegen ihre Pflicht aus § 675l Abs. 1 Satz 1 BGB verstoßen, indem sie am 3. Juli 2022 im Rahmen des zweiten Telefonats mehrere TANs an die unbekannte Anruferin weitergegeben hat, ist nicht zu beanstanden.

27 Grobe Fahrlässigkeit erfordert einen in objektiver Hinsicht schweren und in subjektiver Hinsicht nicht entschuldbaren Verstoß gegen die Anforderungen

der im Verkehr 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. Es muss eine auch subjektiv schlechthin unentschuldbare Pflichtverletzung vorliegen, die das in § 276 Abs. 2 BGB bestimmte Maß erheblich überschreitet. Ob die Fahrlässigkeit im Einzelfall als einfach oder grob zu werten ist, unterliegt der tatrichterlichen Würdigung, die mit der Revision nur beschränkt angreifbar und vom Revisionsgericht nur daraufhin zu überprüfen ist, ob der Tatrichter den Rechtsbegriff der groben Fahrlässigkeit verkannt oder bei der Beurteilung des Grades der Fahrlässigkeit wesentliche Umstände außer Betracht gelassen hat (vgl. BGH, Urteile vom 17. Oktober 2000 - XI ZR 42/00, BGHZ 145, 337, 340, vom 25. Mai 2011 - IV ZR 151/09, NJW-RR 2011, 1113 Rn. 6 f., vom 10. Oktober 2013 - III ZR 345/12, BGHZ 198, 265 Rn. 26, 29 und vom 26. Juli 2016 - VI ZR 322/15, NJW-RR 2017, 146 Rn. 18 f. sowie Beschlüsse vom 15. Dezember 2020 - XI ZB 24/16, BGHZ 228, 133 Rn. 103 und vom 29. September 2022 - IX ZB 48/21, WM 2022, 2445 Rn. 17, jeweils mwN). Einen solchen Fehler zeigt die Revision nicht auf.

28 (1) Sie beruft sich ohne Erfolg auf ein Augenblicksversagen der Klägerin.

29 Der Ausdruck des Augenblicksversagens beschreibt den Umstand, dass ein Handelnder für eine kurze Zeit die im Verkehr erforderliche Sorgfalt außer Acht lässt. Ein solches Augenblicksversagen kann es zwar nicht für sich allein, wohl aber zusammen mit weiteren Umständen im konkreten Einzelfall als gerechtfertigt erscheinen lassen, unter Abwägung aller Umstände den Schuldvorwurf geringer als grob fahrlässig zu bewerten (vgl. BGH, Urteile vom 8. Juli 1992 - IV ZR 223/91, BGHZ 119, 147, 149 f., vom 29. Januar 2003 - IV ZR 173/01, NJW 2003, 1118, 1119, vom 10. Mai 2011 - VI ZR 196/10, NJW-RR 2011, 1055 Rn. 12 f. und vom 26. Juli 2016 - VI ZR 322/15, NJW-RR 2017, 146 Rn. 26).

30 Entgegen der Auffassung der Revision fehlt es hier schon an einem Augenblicksversagen der Klägerin, weil keine durch eine Überrumpelung, momentane Ablenkung bzw. Unaufmerksamkeit oder Ähnliches bedingte kurzfristige Fehleinschätzung (vgl. BGH, Urteile vom 29. Januar 2003 - IV ZR 173/01, NJW 2003, 1118, 1119 und vom 26. Juli 2016 - VI ZR 322/15, NJW-RR 2017, 146 Rn. 26) vorliegt. Denn die entscheidende Sorgfaltspflichtverletzung ist in der Weitergabe der TANs im Rahmen des zweiten Telefonats am Abend des 3. Juli 2022 zu sehen. Dieses fand nach Terminvereinbarung zwischen der Klägerin und der angeblichen Mitarbeiterin der Beklagten am Abend des auf das erste Telefonat folgenden Tages statt, so dass - wie das Berufungsgericht zutreffend ausgeführt hat - die Klägerin fast einen ganzen Tag Zeit hatte, die ungewöhnlichen Umstände des ersten Telefonats zu reflektieren und entsprechende Schlüsse daraus zu ziehen.

31 (2) Die tatrichterliche Würdigung des Berufungsgerichts ist entgegen der Auffassung der Revision auch nicht deshalb rechtsfehlerhaft, weil es das Verhalten der Klägerin als grob fahrlässig beurteilt hat, obwohl die Kläger vor dem streitgegenständlichen Geschehen nur das optische chipTAN-Verfahren genutzt hatten und der Klägerin das manuelle chipTAN-Verfahren unbekannt war. Denn Unerfahrenheit schließt grobe Fahrlässigkeit nicht zwingend aus, sondern kann es nur im Einzelfall rechtfertigen, einen Pflichtenverstoß geringer als grob fahrlässig zu bewerten (BGH, Urteil vom 10. Mai 2011 - VI ZR 196/10, NJW-RR 2011, 1055 Rn. 15; Staudinger/Caspers, BGB, Neubearb. 2025, § 276 Rn. 100; Nobbe in Ellenberger/Findeisen/Nobbe/Böger, Kommentar zum Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 83). Im Einklang damit hat das Berufungsgericht die fehlende Erfahrung der Klägerin mit dem manuellen chipTAN-Verfahren im Rahmen der von ihm vorgenommenen Gesamtwürdigung berücksichtigt, aber nicht als geeignet angesehen, die Klägerin von dem Vorwurf grober Fahrlässigkeit zu entlasten, weil sich ihr trotz dieser Unerfahrenheit aufdrängen musste, dass sie

den TAN-Generator im manuellen chipTAN-Verfahren wie bisher zur Erzeugung einer TAN für die Bestätigung eines konkreten Zahlungsvorgangs benutzte. Gegen die Richtigkeit der dieser Würdigung zugrundeliegenden Feststellungen des Berufungsgerichts zur Funktionsweise des manuellen chipTAN-Verfahrens erhebt die Revision keine Rüge.

32 (3) Revisionsrechtlich ebenfalls nicht zu beanstanden ist ferner, dass das Berufungsgericht das Verhalten der Klägerin als grob fahrlässig bewertet hat, obwohl ihr auf dem Display ihres Telefons die Telefonnummer der Beklagten angezeigt wurde. Das Berufungsgericht hat im Rahmen der von ihm vorgenommenen Gesamtwürdigung berücksichtigt, dass der Klägerin die Möglichkeit des Vortäuschens einer Anrufnummer unbekannt gewesen sein mag, diesen Umstand aber, insbesondere aufgrund der Angaben der Klägerin in ihrer persönlichen Anhörung zu ihren bisherigen telefonischen Kontakten mit der Beklagten, aufgrund der allgemeinen Warnung der Beklagten auf ihrer Website und im Online-Banking vor den Gefahren des Missbrauchs und vor betrügerischen Telefonanrufen vermeintlicher Sparkassen-Mitarbeiter und aufgrund der umfangreichen Berichterstattung in den letzten Jahren in den öffentlichen Medien zu den vielfachen und mannigfaltigen Angriffen beim Internet-Banking, insbesondere dem Phishing, als nicht ausreichend angesehen, um die Klägerin vom Vorwurf der groben Fahrlässigkeit zu entlasten. Angesichts dieser Erwägungen ist schließlich auch nicht zu beanstanden, dass das Berufungsgericht den Einwand der Kläger, die Beklagte habe trotz Kenntnis von einer aktuellen Betrugsserie zum Nachteil ihrer Kunden keine darauf bezogenen konkreten Warnungen ausgesprochen, nicht gesondert beschieden hat.

33 c) Der Schadensersatzanspruch der Beklagten ist nicht gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB ausgeschlossen.

34 Der Zahler ist nach dieser Vorschrift seinem Zahlungsdienstleister abweichend von § 675v Abs. 1 und 3 BGB nicht zum Schadensersatz verpflichtet, wenn letzterer eine starke Kundenauthentifizierung im Sinne des § 1 Abs. 24 ZAG nicht verlangt. Hier hat die Beklagte nach den von der Revision nicht angegriffenen Feststellungen des Berufungsgerichts für das Auslösen der streitgegenständlichen Überweisung eine starke Kundenauthentifizierung gemäß § 1 Abs. 24 ZAG verlangt. Entgegen der Auffassung der Revision ist unerheblich, ob die Beklagte abweichend von § 55 Abs. 1 Satz 1 Nr. 1 ZAG für die Anmeldung im Online-Banking keine starke Kundenauthentifizierung verlangt hat und ob sie hierzu nach Art. 10 Abs. 1 der Delegierten VO (EU) 2018/389 befugt war. Denn Bezugspunkt für die Anwendung von § 675v Abs. 4 Satz 1 Nr. 1 BGB ist - wie das Berufungsgericht zutreffend angenommen hat (ebenso OLG Naumburg, NJW-RR 2025, 561 Rn. 50) - ausschließlich der im Streit stehende Zahlungsvorgang (OLG Bremen, WM 2024, 1508, 1512; OLG Frankfurt a.M., Beschluss vom 22. September 2023 - 3 U 84/23, juris Rn. 20; LG Nürnberg-Fürth, ZIP 2024, 744, 747; MünchKommHGB/Linardatos, 5. Aufl., Band 6 Bankvertragsrecht, K Rn. 224; Maihold in Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rn. 386; Nobbe in Ellenberger/Findeisen/Nobbe/Böger, Kommentar zum Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 125; Hoffmann, VuR 2016, 243, 248; Ostoja-Starzewski, RDi 2022, 259 Rn. 23; Werner, ZBB 2017, 345, 350; ders., WM 2024, 966 Rn. 48, 74; aA OLG Brandenburg, Urteil vom 15. Januar 2025 - 4 U 32/24, juris Rn. 55; LG Berlin II, WM 2025, 1292 Rn. 22 f.; Schulte am Hülse/Steinsdörfer, VuR 2025, 172, 174).

35 § 675v Abs. 4 Satz 1 BGB regelt, wie die Bezugnahme auf § 675v Abs. 1 und 3 BGB zeigt, die Haftung des Zahlers im Fall eines nicht autorisierten Zahlungsvorgangs. Zahlungsvorgang ist gemäß § 675f Abs. 4 Satz 1 BGB jede Bereitstellung, Übermittlung oder Abhebung eines Geldbetrags, unabhängig von der zugrundeliegenden Rechtsbeziehung zwischen Zahler und Zahlungsempfänger.

Nach der Gesetzesbegründung stellt der Zahlungsvorgang den "tatsächlichen Geldfluss dar, also die Bereitstellung, den Transfer oder die Abhebung von Buch- oder Bargeldbeträgen" (BT-Drucks. 16/11643, S. 102; Senatsurteil vom 11. Juli 2023 - XI ZR 111/22, BGHZ 238, 18 Rn. 23). Auch die Gleichstellung mit der Konstellation, dass der Zahlungsempfänger oder sein Zahlungsdienstleister eine starke Kundenauthentifizierung nicht akzeptiert (§ 675v Abs. 4 Satz 1 Nr. 2 BGB), spricht dafür, dass ausschließlich maßgeblich ist, ob für das Auslösen des in Rede stehenden Zahlungsvorgangs eine starke Kundenauthentifizierung verlangt worden ist.

36 Etwas anderes folgt nicht daraus, dass Anknüpfungspunkt für die Haftung des Zahlers gemäß § 675v Abs. 3 BGB auch eine Verletzung von Pflichten oder Bedingungen sein kann, die nicht unmittelbar im Zusammenhang mit der Auslösung des Zahlungsvorgangs erfolgt ist (so aber OLG Brandenburg, Urteil vom 15. Januar 2025 - 4 U 32/24, juris Rn. 55; Schulte am Hülse/Steinsdörfer, VuR 2025, 172, 174). Denn § 675v Abs. 3 Nr. 2 BGB knüpft allgemein an die Herbeiführung des Schadens an, zumal ein nicht autorisierter Zahlungsvorgang auch ohne unmittelbare Mitwirkung des Zahlers erfolgen kann, wenn dieser im Vorfeld seine gesetzlich oder vertraglich festgelegten Pflichten verletzt hat. Sollte der Zahlungsdienstleister für zeitlich frühere Vorgänge wie die erste Anmeldung im Online-Banking durch die unbekannten Täter, die diesen erst ermöglicht hätten, sensible Zahlungsdaten der Klägerin zu erlangen, um damit deren Vertrauen zu erschleichen, entgegen den gesetzlichen Vorgaben keine starke Kundenauthentifizierung verlangt haben, könnte dieser Umstand - wie auch das Berufungsgericht angenommen hat - gegebenenfalls über § 254 BGB zu einer Reduzierung der Haftung des Zahlers führen, da dem Anspruch des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB grundsätzlich der Einwand des Mitverschuldens nach § 254 BGB entgegengehalten werden kann (vgl. Senatsurteil vom 17. November 2020 - XI ZR 294/19, BGHZ 227, 343 Rn. 49; OLG Frankfurt a.M., WM

2024, 690 Rn. 106 f.; MünchKommBGB/Zetzsche, 9. Aufl., § 675v Rn. 57 ff.; Grüneberg/Grüneberg, BGB, 84. Aufl., § 675v Rn. 7; Maihold in Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rn. 380 ff.; Nobbe in Ellenberger/Findeisen/Nobbe/Böger, Kommentar zum Zahlungsverkehrsrecht, 3. Aufl., § 675v BGB Rn. 107; Herresthal in Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., Kap. 3 § 675v BGB Rn. 71 ff.; Kirchner, RdZ 2025, 44, 50 f.).

37 d) Schließlich hat das Berufungsgericht rechtsfehlerfrei eine Minderung des Anspruchs der Beklagten gegen die Kläger aus § 675v Abs. 3 Nr. 2 BGB nach § 254 Abs. 1 BGB ausgeschlossen.

38 Die Gewichtung und Abwägung des beiderseitigen Fehlverhaltens und die Bemessung der Haftungsanteile der Parteien gemäß § 254 Abs. 1 BGB sind Sache des Tatrichters, die das Revisionsgericht nur eingeschränkt überprüfen kann (Senatsurteile vom 8. Oktober 1991 - XI ZR 207/90, WM 1991, 1912, 1915 und vom 17. November 2020 - XI ZR 294/19, BGHZ 227, 343 Rn. 49). Revisionsrechtlich erhebliche Rechtsfehler zeigt die Revision nicht auf. Insbesondere belegt sie nicht, dass das Berufungsgericht Streitstoff übergangen oder gegen Denkgesetze oder Erfahrungssätze verstoßen hat (vgl. Senatsurteile vom 15. Juli 2014 - XI ZR 418/13, WM 2014, 1670 Rn. 28, vom 15. März 2016 - XI ZR 122/14, WM 2016, 780 Rn. 19 und vom 17. November 2020, aaO).

39 Das Berufungsgericht hat im Rahmen der Prüfung von § 254 BGB unterstellt, dass die Beklagte pflichtwidrig für die erste Anmeldung der unbekannten Täter im Online-Banking der Kläger keine starke Kundenauthentifizierung verlangt habe und die Täter dadurch Kenntnis von dem Geburtsdatum der Klägerin, ihrer Telefonnummer, ihrer Kartennummer und den letzten Kontobewegungen

erlangt hätten, was ihnen ermöglicht hätte, bei der Klägerin den Anschein zu erwecken, ein Mitarbeiter der Beklagten rufe sie an. Entgegen der Ansicht der Revision ist das Berufungsgericht nicht davon ausgegangen, der unterstellte Verstoß gegen § 55 Abs. 1 Satz 1 Nr. 1 ZAG sei nicht mehr ursächlich für den eingetretenen Schaden. Vielmehr hat es aufgrund der Abwägung des beiderseitigen Fehlverhaltens (dazu Senatsurteil vom 17. November 2020 - XI ZR 294/19, BGHZ 227, 343 Rn. 49; Grüneberg/Grüneberg, BGB, 84. Aufl., § 254 Rn. 57 ff.) angenommen, dass der Verursachungsbeitrag der Beklagten vollständig hinter demjenigen der Klägerin zurücktritt. Diese Würdigung ist angesichts der besonderen Umstände des Einzelfalls, insbesondere der oben unter II. 2. b) bb) (1) (Rn. 30) genannten, revisionsrechtlich nicht zu beanstanden.

Ellenberger Grüneberg Matthias

Derstadt Schild von Spannenberg

Vorinstanzen:
LG Halle, Entscheidung vom 04.01.2024 - 4 O 187/23 -
OLG Naumburg, Entscheidung vom 22.05.2024 - 5 U 11/24 –