



BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

XI ZR 20/24

Verkündet am:
3. März 2026
Mazurkiewicz
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in dem Rechtsstreit

Nachschlagewerk: ja
BGHZ: ja
BGHR: ja
JNEU: ja

BGB § 675v Abs. 4 Satz 1 Nr. 1
ZAG § 1 Abs. 24, § 55
Delegierte Verordnung (EU) 2018/389 Art. 5 Abs. 1

Eine starke Kundenauthentifizierung im Sinne von § 675v Abs. 4 Satz 1 Nr. 1 BGB erfordert im manuellen chipTAN-Verfahren nicht die Angabe des Namens des Zahlungsempfängers im Display des TAN-Generators.

BGH, Urteil vom 3. März 2026 - XI ZR 20/24 - OLG Naumburg
LG Halle

Der XI. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 3. März 2026 durch den Vizepräsidenten Prof. Dr. Ellenberger, den Richter Dr. Grüneberg, die Richterin Dr. Derstadt, den Richter Dr. Sturm und die Richterin Ettl

für Recht erkannt:

Die Revision des Klägers gegen das Urteil des 5. Zivilsenats des Oberlandesgerichts Naumburg vom 10. Januar 2024 in der Fassung des Beschlusses vom 28. Februar 2024 wird auf seine Kosten zurückgewiesen.

Von Rechts wegen

Tatbestand:

- 1 Der Kläger verlangt von der beklagten Sparkasse, vier Belastungsbuchungen auf seinem Girokonto rückgängig zu machen.
- 2 Der als selbständiger Handwerker tätige Kläger unterhält bei der Beklagten seit 2003 ein Geschäftsgirokonto. Die Ehefrau des Klägers ist seitdem über das Konto verfügungsberechtigt und kümmert sich um den Zahlungsverkehr des Betriebs des Klägers. Am 28. Juni 2004 vereinbarten die Parteien die Teilnahme des Klägers am Online-Banking mit PIN und TAN. Die anfängliche Verwendung von auf zugesandten Listen vermerkten Transaktionsnummern (TAN) wurde abgelöst durch das sogenannte chipTAN-Verfahren, bei dem die TAN mittels eines

gesonderten Geräts, eines TAN-Generators, generiert und im Online-Banking eingegeben wird. Für Überweisungen war ein Tageslimit von 10.000 € vereinbart. Der Nutzung des Online-Banking liegen die "Bedingungen für das Online-Banking" der Beklagten zugrunde. Nr. 7 ("Sorgfaltspflichten des Teilnehmers") der im Zeitpunkt der streitgegenständlichen Buchungen geltenden Fassung dieser Bedingungen enthält unter Nr. 7.1 ("Schutz der Authentifizierungselemente") Abs. 2 Buchst. b Spiegelstrich 5 die folgende Regelung:

"(b) Besitzelemente, wie z.B. die Sparkassen-Card mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

[...]

- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online-Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden [...]"

3 Am 30. Oktober 2020 bemerkte die Ehefrau des Klägers bei dem Versuch, sich im Online-Banking der Beklagten einzuloggen, eine Meldung, dass der TAN-Generator "neu konfiguriert" werden müsse. Sodann loggte sie sich in den E-Mail-Account des Klägers ein und öffnete dort eine E-Mail des Absenders "noreply@r. -markt.gmbh" vom 27. Oktober 2020. Die E-Mail mit dem Logo der Beklagten im Textfeld enthielt die Mitteilung:

"mit unserer Online-Nachricht heute informieren wir Sie über wichtige Änderungen im Onlineerlebnis Ihrer Sparkasse. ab dem 30.10.2020 erhalten Sie ein einheitlich abgestimmtes neues System, kurz CISC, (Covid Intelligence Spa Connect). [...] Diese Umstellung ist eine Pflichtumstellung."

4 Die Ehefrau des Klägers klickte auf den in der E-Mail enthaltenen Button "Weiter zur Registration". Auf der sich öffnenden Internetseite gab sie Nachname, Geburtsdatum sowie die letzten vier Ziffern und das Ablaufdatum der Sparkassenkarte des Klägers ein. Danach erhielt der Kläger eine weitere E-Mail, nach der sich in Kürze ein Kundenberater melden würde.

- 5 Am Samstag, dem 31. Oktober 2020, ging zwischen 13:00 Uhr und 14:00 Uhr auf dem Festnetztelefon ein Anruf unter der Telefonnummer der Beklagten ein. Der Anrufer stellte sich als Mitarbeiter der Beklagten vor. Auf seine Aufforderung hin drückte die Ehefrau des Klägers die Tasten 1 und 2 auf dem TAN-Generator gleichzeitig drei Sekunden lang. Danach folgte sie den weiteren Anweisungen des Anrufers. Sie steckte die Sparkassenkarte in den TAN-Generator. Der Anrufer teilte einen "Start-Code" mit. Diesen tippte sie ein und bestätigte mit "OK". Danach teilte der Anrufer weitere Ziffernfolgen mit, die sie ebenfalls mit "OK" bestätigte. Anschließend erschien im TAN-Generator eine sechsstellige Nummer, die die Ehefrau des Klägers dem Anrufer mitteilte. Diesen Vorgang wiederholte sie auf Weisung des Anrufers, weil dieser mitteilte, dass "es technische Probleme gegeben habe". Schließlich kündigte der Anrufer an, am Sonntag noch einmal anzurufen, um alle Vorgänge ordnungsgemäß abzuschließen. Am Sonntag, dem 1. November 2020, rief er nochmals an und ließ die Ehefrau des Klägers erneut die beschriebenen Vorgänge wiederholt durchführen.
- 6 Ausweislich der von der Beklagten vorgelegten Transaktionsprotokolle wurden in Bezug auf das Geschäftsgirokonto des Klägers per Online-Banking im Wege des manuellen chipTAN-Verfahrens am 31. Oktober 2020 eine temporäre Limitänderung auf 94.999 € und zwei Echtzeit-Überweisungen in Höhe von 7.222 € und 7.445 € sowie am 1. November 2020 eine temporäre Limitänderung auf 80.000 € und zwei Echtzeit-Überweisungen in Höhe von 8.787 € und 16.000 € durchgeführt.
- 7 Mit seiner Klage begehrt der Kläger, seinem Girokonto wertmäßig 7.222 € und 7.445 € zum 31. Oktober 2020 sowie 8.787 € und 16.000 € zum 1. November 2020 gutzuschreiben. Das Landgericht hat der Klage nach Vernehmung der Ehefrau des Klägers als Zeugin stattgegeben (LG Halle, Urteil vom 23. Juni 2023 - 4 O 133/22, juris). Auf die Berufung der Beklagten hat das Berufungsgericht nach Vernehmung der Ehefrau des Klägers und eines bei der Beklagten beschäf-

tigten Mitarbeiters als Zeugen die Klage abgewiesen. Mit der vom Senat zugelassenen Revision erstrebt der Kläger die Wiederherstellung des landgerichtlichen Urteils.

Entscheidungsgründe:

8 Die Revision ist unbegründet.

I.

9 Das Berufungsgericht hat zur Begründung seiner Entscheidung (OLG Naumburg, Urteil vom 10. Januar 2024 - 5 U 83/23, juris) im Wesentlichen ausgeführt:

10 Der Kläger habe zwar gegen die Beklagte einen Anspruch aus § 675u Satz 2 BGB, weil die den streitgegenständlichen Belastungsbuchungen in Höhe von insgesamt 39.454 € zugrundeliegenden Überweisungen nicht gemäß § 675j Abs. 1 Satz 1 BGB durch den Kläger autorisiert worden seien. Das Berufungsgericht sei nach der Beweisaufnahme davon überzeugt, dass ein unbefugter Dritter, der aufgrund der Angaben der Ehefrau des Klägers im Rahmen der "Registration" oder aufgrund eines vorangegangenen und unbemerkt gebliebenen Angriffs die Online-Banking-Zugangsdaten des Klägers gekannt habe, im Online-Banking jeweils mittels der von der arglosen Ehefrau des Klägers erzeugten TANs die Erhöhungen des Überweisungslimits und die Echtzeit-Überweisungen auf das Konto einer unbekannten Person bestätigt habe.

11 Dem Anspruch aus § 675u Satz 2 BGB könne die Beklagte jedoch gemäß § 242 BGB einen Schadensersatzanspruch gegen den Kläger aus § 675v Abs. 3 Nr. 2 Buchst. b BGB in gleicher Höhe entgegenhalten. Von dem Kunden, der am

Online-Banking teilnehme, sei zu erwarten, dass er die Authentifizierungselemente, wie unter Nr. 7 der Bedingungen für das Online-Banking vorgesehen, schütze. Bei Weitergabe personalisierter Sicherheitsmerkmale am Telefon oder per E-Mail liege stets ein Sorgfaltspflichtverstoß vor und - abhängig von den Besonderheiten des Einzelfalls, insbesondere subjektiven Gesichtspunkten - der Vorwurf grob fahrlässigen Verhaltens nahe. Hier habe der Kläger durch das ihm zuzurechnende Verhalten seiner Ehefrau grob fahrlässig gegen seine Sorgfaltspflichten aus Nr. 7.1 Abs. 2 Buchst. b Spiegelstrich 5 der Bedingungen für das Online-Banking verstoßen.

12 Der Ehefrau des Klägers hätte bei sorgfältiger Kontrolle auffallen müssen, dass die E-Mail vom 27. Oktober 2020 nicht von der Beklagten gestammt und mehrere Rechtschreibfehler beinhaltet habe. Auch das darin in Aussicht gestellte "neue einheitlich abgestimmte System Covid Intelligence Spa Connect" hätte die Ehefrau des Klägers stutzig machen müssen, zumal in der E-Mail - anders als in der vorangegangenen Meldung - keinerlei Hinweise zu einer vermeintlichen "Neukonfigurierung des TAN-Generators" enthalten gewesen seien. Auch wenn dem Kläger und seiner Ehefrau die Möglichkeit, eine Anrufernummer vorzutäuschen (Call-ID-Spoofing), nicht bekannt gewesen sein sollte, hätten sie die Anrufzeiten am Samstag und Sonntag außerhalb üblicher Bankgeschäftszeiten ebenfalls stutzig machen müssen. Dem Kläger hätte es bei Wahrung der erforderlichen Sorgfalt oblegen, sich durch einen Anruf bei der Beklagten zu vergewissern, dass es sich bei dem Anrufer tatsächlich um einen Mitarbeiter der Beklagten handle. Hätte der Kläger sich im Internet informiert, hätte er überdies festgestellt, dass sich dort diverse Hinweise der Sparkassen zum Online-Banking, aber keine zur Erforderlichkeit einer "Neukonfigurierung des TAN-Generators" finden ließen.

13 Dem Kläger sei vorzuwerfen, dass sich seine Ehefrau auf die Vorgaben des Anrufers eingelassen, TANs erzeugt und an den Anrufer weitergegeben

habe, obwohl er schon in den Bedingungen für das Online-Banking dazu angehalten worden sei, die TAN ausschließlich im Online-Banking zu verwenden und weder mündlich noch in Textform weiterzugeben. Überdies sei aufgrund der umfangreichen Berichterstattung in den öffentlichen Medien zu den vielfachen und mannigfaltigen Angriffen beim Online-Banking allgemein bekannt, dass die TAN niemals außer zur Bestätigung eines in Auftrag gegebenen Vorgangs verwendet werden solle. Der Kläger nutze den TAN-Generator bereits seit Jahren und sei nie zuvor aufgefordert worden, diesen "neu zu konfigurieren".

- 14 Schließlich hätte die Ehefrau des Klägers erkennen können, dass sie TANs erzeuge und an den Anrufer weitergebe, auch wenn ihr nicht bekannt gewesen sein sollte, dass im Online-Banking das Tageslimit erhöht werden könne, und sie bisher nur das optische chipTAN-Verfahren genutzt habe, während ihr das manuelle chipTAN-Verfahren nicht bekannt gewesen sei. Aufgrund der Angaben des Zeugen sei das Berufungsgericht davon überzeugt, dass im Zusammenhang mit den Limiterhöhungen die Ehefrau des Klägers nach Eingabe des ihr mitgeteilten Startcodes jeweils die TAN-Taste betätigt und die ihr daraufhin mit der Bezeichnung "TAN" angezeigte sechsstellige Nummer weitergegeben habe. Im Zusammenhang mit den Überweisungen seien jeweils nacheinander IBAN, Betrag und TAN im Display des TAN-Generators angezeigt worden und die Ehefrau des Klägers habe jeweils IBAN und Betrag in den TAN-Generator eingegeben, die TAN erzeugt und diese an den Anrufer weitergegeben. Der als Zeuge vernommene Mitarbeiter der Beklagten habe schlüssig den Ablauf des manuellen chipTAN-Verfahrens geschildert und dies in Gegenwart der Ehefrau des Klägers anschaulich in der Verhandlung demonstriert. Eine Möglichkeit, Zahlen in den TAN-Generator einzugeben, ohne dass erkennbar sei, worum es sich handele, gebe es nicht. Davon habe sich das Berufungsgericht während der Demonstration im Echtbetrieb überzeugt. Die Ehefrau des Klägers habe ganz naheliegende Überlegungen nicht angestellt und jegliche Vorsicht vermissen lassen. Bei der erforderlichen Gesamtbetrachtung stelle sich ihr Handeln, welches sich der Kläger zurechnen lassen müsse, als objektiv schwerwiegender und subjektiv

nicht entschuldbarer Verstoß gegen die Anforderungen der im Verkehr erforderlichen Sorgfalt dar.

15

Der Schadensersatzanspruch der Beklagten sei nicht nach § 675v Abs. 4 Satz 1 Nr. 1 BGB ausgeschlossen. Die Anforderungen an eine starke Kundenauthentifizierung für einen elektronischen Fernzahlungsvorgang ergäben sich aus § 1 Abs. 24, § 55 Abs. 2 ZAG sowie aus Art. 4 und 5 der Delegierten Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (ABl. 2018, L 69, S. 23, berichtigt in ABl. 2020, L 88, S. 11, künftig: Delegierte VO (EU) 2018/389). Das hier bei den streitgegenständlichen Überweisungen zur Anwendung gelangte chipTAN-Verfahren entspreche diesen Anforderungen. Entgegen der Ansicht des Landgerichts sei nicht erforderlich, dass Zahlungsbetrag und Zahlungsempfänger dem Zahler in allen Phasen der Authentifizierung angezeigt werden. Denn Art. 5 Abs. 1 Buchst. a der Delegierten VO (EU) 2018/389 gebe keinen Zeitpunkt für die Anzeige von Zahlungsbetrag und -empfänger vor. Aus der Regelung in Art. 5 Abs. 1 Buchst. b der Delegierten VO (EU) 2018/389 folge, dass Zahlungsbetrag und -empfänger zum Zeitpunkt des Auslösens des Vorgangs anzuzeigen seien. Bei Verwendung eines TAN-Generators erfolge diese Anzeige mangels Verbindung des Generators mit dem Internet jedenfalls stets im Online-Banking, in dem der Zahlungsvorgang ausgelöst werde. Ein anderes Ergebnis folge auch nicht aus Art. 5 Abs. 2 der Delegierten VO (EU) 2018/389, nach dem die Zahlungsdienstleister Sicherheitsmaßnahmen vorzusehen haben, die die Vertraulichkeit, die Authentizität und die Integrität der genannten Angaben gewährleisten.

II.

16 Diese Ausführungen halten einer revisionsrechtlichen Überprüfung stand.

17 1. Rechtsfehlerfrei ist das Berufungsgericht davon ausgegangen, dass dem Kläger 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. Senatsurteile vom 5. März 2024 - XI ZR 107/22, BGHZ 240, 23 Rn. 46 mwN und vom 22. Juli 2025 - XI ZR 107/24, WM 2025, 1592 Rn. 21) angenommen, dass die streitgegenständlichen Überweisungen nicht vom Kläger - auch nicht in ihm zuzurechnender Weise durch seine Ehefrau - autorisiert worden sind. Gegen diese Beurteilung hat auch die Beklagte in der Revisionsinstanz nichts erinnert.

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

19 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., vom 5. März 2024 - XI ZR 107/22, BGHZ 240, 23 Rn. 50 und vom 22. Juli 2025 - XI ZR 107/24, WM 2025, 1592 Rn. 23).

20 b) Die Auffassung des Berufungsgerichts, dass die Voraussetzungen für einen Schadensersatzanspruch der Beklagten wegen der nicht autorisierten Überweisungen aus § 675v Abs. 3 Nr. 2 BGB gegeben sind, begegnet keinen revisionsrechtlichen Bedenken.

21 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. Nach den - im Revisionsverfahren nicht angegriffenen - Feststellungen des Berufungsgerichts war in Nr. 7.1 Abs. 2 Buchst. b Spiegelstrich 5 der im Zeitpunkt der streitgegenständlichen Verfügungen für das Vertragsverhältnis zwischen den Parteien geltenden Bedingungen für das Online-Banking bestimmt, dass Besitzelemente, wie z.B. die Sparkassen-Card mit TAN-Generator, vor Missbrauch zu schützen sind und insbesondere die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online-Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden dürfen.

22 Die Annahme des Berufungsgerichts, der Kläger habe durch das ihm zuzurechnende Verhalten seiner Ehefrau grob fahrlässig gegen diese Sorgfaltpflicht verstoßen, indem jene im Rahmen der Telefonate am 31. Oktober 2020 und 1. November 2020, die außerhalb üblicher Bankarbeitszeiten an einem Wochenende erfolgten, mehrere TANs erzeugt und an den ihr unbekannten Anrufer weitergegeben hat, ist nicht zu beanstanden. Grobe Fahrlässigkeit erfordert ei-

nen in objektiver Hinsicht schweren und in subjektiver Hinsicht nicht entschuld-
baren Verstoß gegen die Anforderungen der im Verkehr erforderlichen Sorgfalt.
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
(st. Rspr., vgl. nur Senatsurteil vom 22. Juli 2025 - XI ZR 107/24, WM 2025, 1592
Rn. 27 mwN). Solche Fehler sind hier nicht ersichtlich und die Revision erhebt
diesbezüglich auch keine Einwände.

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

24 Der Zahler ist nach dieser Vorschrift seinem Zahlungsdienstleister abwei-
chend 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. Dies ist hier nach den Feststellungen des Berufungsgerichts
zu den streitgegenständlichen Überweisungen nicht der Fall.

25 aa) Nach § 1 Abs. 24 ZAG ist eine starke Kundenauthentifizierung eine
Authentifizierung, die so ausgestaltet ist, dass die Vertraulichkeit der Authentifi-
zierungsdaten geschützt ist, und die unter Heranziehung von mindestens zwei
der folgenden, in dem Sinne voneinander unabhängigen Elementen geschieht,
dass die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in
Frage stellt: 1. Kategorie Wissen, also etwas, das nur der Nutzer weiß, 2. Kate-
gorie Besitz, also etwas, das nur der Nutzer besitzt, oder 3. Kategorie Inhärenz,
also etwas, das der Nutzer ist.

26 Für einen elektronischen Fernzahlungsvorgang im Sinne von § 1 Abs. 19,
§ 55 Abs. 1 Satz 1 Nr. 2 ZAG, wie eine Überweisung im Online-Banking, schreibt

§ 55 Abs. 2 ZAG zusätzlich vor, dass die starke Kundenauthentifizierung Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen. Hierfür ist gemäß § 55 Abs. 5 ZAG i.V.m. Art. 5 Abs. 1 der Delegierten VO (EU) 2018/389 erforderlich, dass Zahlungsbetrag und Zahlungsempfänger dem Zahler angezeigt werden, dass der generierte Authentifizierungscode speziell für den Zahlungsbetrag und den Zahlungsempfänger gilt, denen der Zahler beim Auslösen des Vorgangs zugestimmt hat, dass der vom Zahlungsdienstleister akzeptierte Authentifizierungscode dem ursprünglichen spezifischen Zahlungsbetrag und der Identität des Zahlungsempfängers entspricht, denen der Zahler zugestimmt hat, und dass jede Änderung beim Betrag oder Zahlungsempfänger die Ungültigkeit des generierten Authentifizierungscode nach sich zieht. Zudem hat der Zahlungsdienstleister nach Art. 5 Abs. 2 der Delegierten VO (EU) 2018/389 Sicherheitsmaßnahmen vorzusehen, die die Vertraulichkeit, die Authentizität und die Integrität der in der Vorschrift genannten Angaben gewährleisten.

27 bb) Das hier für das Auslösen der streitgegenständlichen Überweisungen eingesetzte sogenannte manuelle chipTAN-Verfahren genügt diesen Anforderungen, so dass dahinstehen kann, ob der in § 675v Abs. 4 Satz 1 Nr. 1 BGB geregelte Ausschluss der Haftung des Zahlers auch die Einhaltung der zusätzlichen Anforderungen aus § 55 Abs. 2 ZAG erfordert (so z.B. OLG Naumburg, NJW-RR 2025, 561 Rn. 43 ff.; Staudinger/Omlor, BGB, Neubearb. 2020, § 675v Rn. 37; Böger in Baas/Buck-Heeb/Werner, Anlegerschutzgesetze, Dritter Teil § 675m Rn. 70 ff., § 675v Rn. 24; aA Maihold in Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rn. 393 f.; OLG Schleswig, Beschluss vom 11. September 2024 - 5 U 99/24, juris Rn. 83 ff.).

28 (1) Das Berufungsgericht (OLG Naumburg, Urteil vom 10. Januar 2024 - 5 U 83/23, juris Rn. 15, 56) hat zum Ablauf des hier eingesetzten manuellen chipTAN-Verfahrens festgestellt, dass der Nutzer sich bei der Verwendung dieses Verfahrens mit seinem Anmeldenamen sowie seiner persönlichen PIN in sein

Online-Banking-Konto einloggen und dort den Überweisungsauftrag erstellen müsse. Anschließend müsse in den TAN-Generator, in den die Chipkarte - hier die Sparkassenkarte - eingesteckt werde, ein sogenannter Startcode, der aus acht Ziffern bestehe, eingegeben werden, um die korrekte Auftragsart in die TAN-Erzeugung einfließen zu lassen. Dieser Startcode sei bei jeder neuen Überweisung unterschiedlich und werde beim Online-Banking auf der Website vom System vorgegeben. Anschließend werde der Nutzer im Display des TAN-Generators aufgefordert, erst die IBAN des Empfängers einzugeben, die anschließend mit der Taste "OK" bestätigt werde, und dann den Betrag einzugeben, der mit der Taste "OK" bestätigt werde. Nach Eingabe und Bestätigung der manuell eingegebenen Daten in den TAN-Generator errechne der TAN-Generator auf Grundlage der an ihn zuvor übermittelten Daten sowie auf Basis der von der Chipkarte ausgelesenen Kartennummer und Kundenkontonummer eine auf die konkrete Überweisung bezogene sechsstellige TAN, die im entsprechenden Feld auf der Website des Online-Banking eingegeben werden müsse. Außerdem hat das Berufungsgericht festgestellt, dass die Ehefrau des Klägers jeweils IBAN und Betrag in den TAN-Generator eingegeben, dann durch Betätigung der TAN-Taste die TAN erzeugt und die mit der Bezeichnung "TAN" angezeigte sechsstellige Nummer an den Anrufer weitergegeben habe (OLG Naumburg, aaO Rn. 55).

- 29 (2) Dieses Verfahren erfüllt die Anforderungen an eine starke Kundenauthentifizierung, die zudem den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpft (vgl. Maihold in Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rn. 21 f., 36 ff., 89, 387 ff.; Staudinger/Omlor, BGB, Neubearb. 2020, § 675v Rn. 42; Omlor in Schäfer/Omlor/Mimberg, ZAG, 2. Aufl., § 55 Rn. 40; Zahrte in Bunte/Zahrte, AGB-Banken, AGB-Sparkassen, Sonderbedingungen, 6. Aufl., SB Online Rn. 16, 17b; ders. in Casper/Terlau, ZAG, 3. Aufl., § 55 Rn. 58; Omlor, RdZ 2020, 20, 23; Steiner, jurisPR-BKR 10/2025 Anm. 5; Zahrte, MMR 2013, 207 f.; BT-Drucks. 18/11495, S. 140).

- 30 (3) Entgegen der Auffassung der Revision (wohl ebenso Schulte am Hülse/Steinsdörfer, VuR 2025, 172, 173, 174 f., 176) kann aus § 55 Abs. 2, 5 ZAG, Art. 5 der Delegierten VO (EU) 2018/389 nicht abgeleitet werden, dass bei Verwendung des manuellen chipTAN-Verfahrens eine dynamische Verknüpfung des Zahlungsvorgangs mit einem bestimmten Zahlungsempfänger nur dann gegeben ist, wenn auf dem Display des TAN-Generators der Name des Zahlungsempfängers angezeigt wird.
- 31 Insoweit kann dahinstehen, ob die "Anzeige des Zahlungsempfängers" im Sinne von Art. 5 Abs. 1 Buchst. a der Delegierten VO (EU) 2018/389 die Anzeige von dessen Namen erfordert oder ob die Anzeige seiner IBAN genügt (so z.B. OLG Dresden, WM 2025, 1733 Rn. 127, 130), zumal nach Art. 5 Abs. 2 Buchst. a i.V.m. Nr. 2 Buchst. a des Anhangs der Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl. 2012, L 94, S. 22) der Zahler dem Zahlungsdienstleister für die Durchführung einer Überweisung zwingend die IBAN des Zahlungskontos des Zahlungsempfängers, dessen Namen aber nur "sofern verfügbar" übermitteln muss (vgl. Nasarek in Casper/Terlau, ZAG, 3. Aufl., Anh. § 55 Rn. 101).
- 32 Denn selbst wenn die Anzeige des Namens erforderlich sein sollte, schreibt Art. 5 Abs. 1 Buchst. a der Delegierten VO (EU) 2018/389 nicht vor, dass bei dem hier in Rede stehenden Einsatz eines TAN-Generators zusätzlich zu oder anstelle der Anzeige der IBAN im Display des TAN-Generators dort (auch) der Name angezeigt werden muss. Nach dieser Vorschrift haben die Zahlungsdienstleister zwar Sicherheitsmaßnahmen zu ergreifen, die unter anderem die Anforderung erfüllen, dass dem Zahler Zahlungsbetrag und Zahlungsempfänger angezeigt werden. Allerdings enthält Art. 5 Abs. 1 Buchst. a der Delegierten VO (EU) 2018/389 keine konkreten Vorgaben in Bezug auf bestimmte Authentifizie-

ungsverfahren und schreibt weder vor, wo genau bzw. wie die Anzeige des Zahlungsempfängers zu erfolgen hat, noch dass diese Anzeige unabhängig davon erfolgen muss, ob der Zahler sich selbst vertragswidrig verhält. Insoweit ist hier von Bedeutung, dass der von der Ehefrau des Klägers verwendete TAN-Generator dazu dient, eine TAN zu erzeugen, die sodann im Online-Banking eingegeben wird, und dass nach den zwischen den Parteien vereinbarten Bedingungen für das Online-Banking mit dem TAN-Generator erzeugte TANs nicht außerhalb des Online-Banking mündlich, z.B. per Telefon, weitergegeben werden dürfen. Damit sind bei der Prüfung, ob der Zahlungsdienstleister hier eine starke Kundenauthentifizierung verlangt hat, nicht nur die auf dem Display des TAN-Generators angezeigten Informationen, sondern auch diejenigen, die bei vereinbarungsgemäßer Verwendung des TAN-Generators im Online-Banking angezeigt werden, zu berücksichtigen. Die Revision macht nicht geltend, dass im Fall der Verwendung des TAN-Generators durch den Kunden zusammen mit dem Online-Banking der Name des Zahlungsempfängers auch im Online-Banking nicht angezeigt worden wäre. Entgegen der Ansicht der Revision ist unerheblich, dass es rein tatsächlich im manuellen chipTAN-Verfahren möglich ist, über den TAN-Generator eine TAN zu erzeugen, ohne dass hierzu von dem Zahler auf das Online-Banking Zugriff genommen werden muss.

- 33 Die Revision beruft sich auch ohne Erfolg auf Art. 5 Abs. 2 Buchst. a der Delegierten VO (EU) 2018/389. Denn nach dieser Vorschrift hat der Zahlungsdienstleister zwar Sicherheitsmaßnahmen vorzusehen, die die Vertraulichkeit, die Authentizität und die Integrität der Angaben von Zahlungsbetrag und Zahlungsempfänger in allen Phasen der Authentifizierung gewährleisten. Damit werden aber keine über Art. 5 Abs. 1 Buchst. a der Delegierten Verordnung (EU) 2018/389 hinausgehenden Anforderungen an die Anzeige von Zahlungsbetrag und -empfänger aufgestellt. Aus der englischen und französischen Fassung von Art. 5 Abs. 1 und 2 dieser Verordnung ergeben sich keine Anhaltspunkte für ein anderes Verständnis.

34 cc) Entgegen der Ansicht der Revision ist eine Vorlage an den Gerichtshof der Europäischen Union gemäß Art. 267 Abs. 3 AEUV nicht geboten. Die für die Entscheidung des vorliegenden Falls erforderliche Auslegung von Art. 5 Abs. 1 und 2 der Delegierten VO (EU) 2018/389 ist derart offenkundig, dass für vernünftige Zweifel kein Raum bleibt ("acte clair", vgl. EuGH, Urteile vom 6. Oktober 1982 - 283/81, Slg. 1982, 3415 Rn. 16 - C.I.L.F.I.T., vom 9. September 2015 - C-160/14, EuZW 2016, 111 Rn. 38 f. und vom 6. Oktober 2021 - C-561/19, NJW 2021, 3303 Rn. 39 ff., 66). Wie bereits ausgeführt, ergeben sich aus Wortlaut und Regelungssystematik von Art. 5 Abs. 1 und 2 der Delegierten VO (EU) 2018/389 keine Anhaltspunkte dafür, dass bei Einsatz des manuellen chipTAN-Verfahrens neben oder anstelle der Anzeige der IBAN des Zahlungsempfängers im Display des TAN-Generators die Anzeige seines Namens in diesem Display erforderlich sein und nicht die Anzeige des Namens im Online-Banking genügen soll.

35 Derartige Anhaltspunkte folgen auch nicht aus dem letzten Satz von Erwägungsgrund 95 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt (ABl. 2015, L 337, S. 35, berichtigt in ABl. 2016, L 169, S. 18, ABl. 2018, L 102, S. 97 und ABl. 2018, L 126, S. 10). Danach sollten zwar Zahlungsdienste, die über das Internet oder über andere Fernkommunikationskanäle angeboten werden und nicht davon abhängig sind, an welchem Ort sich das für die Auslösung des Zahlungsvorgangs verwendete Gerät oder das verwendete Zahlungsinstrument tatsächlich befinden, die Authentifizierung von Zahlungsvorgängen durch dynamische Codes enthalten, damit der Nutzer stets Klarheit über den Betrag und über den Empfänger der Zahlung hat, die er veranlasst. Abgesehen davon, dass es sich nur um einen Erwägungsgrund handelt und Art. 5 Abs. 1 und 2 der Delegierten VO (EU) 2018/389 davon abweichend formuliert ist, ergibt sich aus dieser Forderung nicht, dass dem Zahlungsdienstleister daraus auch für den Fall

Pflichten erwachsen, dass der Zahler das manuelle chipTAN-Verfahren anwendet und mit seinem TAN-Generator eine TAN generiert, ohne selbst im Online-Banking angemeldet zu sein und dort einen Vorgang ausgelöst zu haben.

Ellenberger

Grüneberg

Derstadt

Sturm

Ettl

Vorinstanzen:

LG Halle, Entscheidung vom 23.06.2023 - 4 O 133/22 -

OLG Naumburg, Entscheidung vom 10.01.2024 - 5 U 83/23 -