

Gericht:	OLG Karlsruhe 17. Zivilsenat
Entscheidungsdatum:	23.12.2025
Aktenzeichen:	17 U 113/23
ECLI:	ECLI:DE:OLGKARL:2025:1223.17U113.23.00
Dokumenttyp:	Urteil
Quelle:	
Normen:	§ 387 BGB, § 389 BGB, § 675f Abs 4 S 1 BGB, § 675j Abs 1 S 3 BGB, § 675j Abs 1 S 4 BGB ... mehr

Haftung des Zahlungsdienstleisters bei nicht autorisierten Zahlungsvorgängen und fehlender starker Kundenauthentifizierung

Leitsatz

Zu den Anforderungen an die starke Kundenauthentifizierung bei Nutzung einer digitalen Debitkarte mittels Apple Pay.

Orientierungssatz

1. Ein Zahlungsdienstleister trägt das Risiko nicht autorisierter Zahlungsvorgänge, wenn er bei Kartenzahlungen oder mobilen Zahlungen kein Verfahren einsetzt, das die Identität des Zahlers zuverlässig überprüft (Anschluss BGH, Urteil vom 22. Juli 2025 - XI ZR 107/24; BGH, Urteil vom 26. Januar 2016 - XI ZR 91/14 und OLG Brandenburg, Urteil vom 15. Januar 2025 - 4 U 32/24).(Rn.19) (Rn.26) (Rn.31)
2. Ein Verfahren zur Identitätsprüfung ist nur dann zuverlässig, wenn der Zahlungsdienstleister sicherstellt, dass sowohl das verwendete Gerät als auch die zur Freigabe eingesetzten persönlichen Merkmale zweifelsfrei dem Zahler zugeordnet sind (Anschluss OLG Naumburg, Urteil vom 10. Januar 2024 - 5 U 83/23).(Rn.38) (Rn.41)
3. Stellt der Zahlungsdienstleister bei der Einrichtung einer digitalen Zahlungskarte nicht sicher, dass diese ausschließlich auf einem Gerät des Zahlers hinterlegt wird, kann er sich im Fall eines Missbrauchs nicht auf eine Pflichtverletzung des Kunden berufen.(Rn.47)

Verfahrensgang

vorgehend LG Karlsruhe, 23. November 2023, 2 O 312/22

Tenor

1. Die Berufung der Beklagten gegen das Urteil des Landgerichts Karlsruhe vom 23. November 2023 - 2 O 312/22 - wird zurückgewiesen.
2. Die Beklagte trägt die Kosten des Berufungsverfahrens.
3. Dieses Urteil und das in Ziffer 1 genannte Urteil des Landgerichts Karlsruhe sind vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung abwenden durch Sicherheitsleistung in Höhe von 120 Prozent des auf Grund des Urteils vollstreckbaren Betrages,

wenn nicht der Kläger zuvor Sicherheit in Höhe von 120 Prozent des jeweils zu vollstreckenden Betrages leistet.

4. Die Revision gegen dieses Urteil wird zugelassen.

Gründe

I.

- 1 Der Kläger begehrt von der beklagten Bank die Erstattung ohne Autorisierung abgebuchter Beträge, die Beklagte wendet dagegen Schadensersatzansprüche in gleicher Höhe ein.
- 2 Der Kläger hat erstinstanzlich beantragt:
 - 3 1. die Beklagte zu verurteilen, das Konto des Klägers mit der IBAN DE ... valutengerecht wieder auf den Stand zu bringen, auf dem dieser sich ohne die Verfügungen im Zeitraum vom 11.04.2022 bis 20.04.2022 in Höhe von € 42.182,68 nebst Zinsen in Höhe von 5 Prozentpunkten über Basiszinssatz seit Rechtshängigkeit befunden hätte,
 - 4 hilfsweise
 - 5 die Beklagte zu verurteilen, an den Kläger € 42.182,68 nebst Zinsen in Höhe von 5 %-Punkten über Basiszinssatz seit Rechtshängigkeit zu zahlen;
 - 6 2. die Beklagte zu verurteilen, an den Kläger vorgerichtliche Rechtsverfolgungskosten in Höhe von € 1.877,11 nebst Zinsen in Höhe von 5 %-Punkten über Basiszinssatz seit Rechtshängigkeit zu zahlen.
- 7 Die Beklagte hat beantragt,
- 8 die Klage abzuweisen.
- 9 Wegen der Einzelheiten des erstinstanzlichen Parteivorbringens wird auf die in dem landgerichtlichen Urteil getroffenen Feststellungen Bezug genommen (§ 540 Abs. 1 Satz 1 Nr. 1 ZPO).
- 10 Das Landgericht hat der Klage mit Ausnahme der Zinsforderung stattgegeben. Zur Begründung hat es im Wesentlichen ausgeführt, dem Kläger stehe gemäß §§ 675 f, 675u BGB ein Anspruch auf Gutschrift von 42.162,68 EUR zu. Der Kläger habe die streitgegenständlichen 122 Zahlungsvorgänge nach der Überzeugung des Gerichts nicht autorisiert. Maßgeblich sei, ob der einzelne Zahlungsvorgang autorisiert worden sei, auf die Einrichtung des Bezahlverfahrens vor der ersten Transaktion komme es in diesem Zusammenhang nicht an. Der Beklagten stehe kein Gegenanspruch aus § 675v Abs. 3 Nr. 2 BGB zu. Der Kläger habe nicht grob fahrlässig gegen seine Pflichten aus § 675l Abs 1 Satz 1 BGB oder den Allgemeinen Geschäftsbedingungen der Beklagten verstoßen. Der Kläger habe allenfalls leicht fahrlässig das Bezahlverfahren Apple-Pay über die PushTAN-App auf seinem iPhone für das fremde iPhone des unbekannten Täters während eines Meetings mit seinem Chef und damit in einer besonderen Situation mit Ablenkungspotential versehentlich freigegeben, ohne dies zu bemerken und zu realisieren. Ein dahingehendes Erklärungsbewusstsein habe der Kläger nicht gehabt, möge er auch den Freigabe-Button versehentlich berührt oder gedrückt haben. Die in der PushTAN-App angezeigte, abs-

trakte Meldung „Registrierung Karte“ (Anlage B1, Schritt 4) habe der Kläger – soweit er diese Meldung ausreichend lange zu Gesicht bekommen habe – als belanglos ansehen und so verstehen können, dass er seinen weiteren Kontozugriff im Online-Banking aufrechterhalte und die Fortdauer der Nutzung der S.-Karte bestätige. Immerhin verlange die Beklagte selbst von Zeit zu Zeit eine Verifizierung zum Login ins Online-Banking über eine Freigabe mit der PushTAN-App. Eine versehentliche Berührung des Displays genau dort, wo der Freigabe-Button angezeigt wird, sei nach den Umständen ebenfalls subjektiv entschuldbar. Es sei offen, wie es den unbekannten Tätern im Vorfeld gelungen sei, sich in das Online-Banking des Klägers einzuloggen. Ein grobes Verschulden des Klägers folge daraus nicht. Den Kläger treffe auch kein Mitverschulden an der Entstehung oder hinsichtlich der Höhe des eingetretenen Schadens, da er nicht zu einer häufigeren Kontrolle des Kontostandes als etwa alle zwei Wochen verpflichtet gewesen sei. Daher könne es dahinstehen, ob einem Schadensersatzanspruch der Beklagten der Ausschlussstatbestand des § 675v Abs. 4 BGB entgegenstehe.

- 11 Wegen der Einzelheiten der Ausführungen des Landgerichts wird auf die Entscheidungsgründe des Urteils Bezug genommen (§ 540 Abs. 1 Satz 1 Nr. 1 ZPO).
- 12 Hiergegen wendet sich die Beklagte mit ihrer Berufung. Sie beantragt:
- 13 Das Urteil des Landgerichts Karlsruhe vom 23.11.2023, Az. 2 O 312/22 abzuändern und die Klage abzuweisen.
- 14 Zur Begründung trägt sie im Wesentlichen vor, der Kläger habe seine Pflicht, im PushTAN-Verfahren die zusammen mit der TAN übermittelten Daten des Auftrags daraufhin zu überprüfen, ob sie mit dem ausgelösten Auftrag übereinstimmten, grob fahrlässig verletzt. Die Angaben des Klägers in seiner informatorischen Anhörung seien nicht glaubhaft vor dem Hintergrund, dass der Kläger vorgebracht habe, sein Smartphone im Februar 2021 gewechselt zu haben, obwohl sich aus den Unterlagen der Beklagten ergebe, dass der Kläger zum streitgegenständlichen Zeitpunkt noch das Smartphone aus dem Jahr 2017 verwendet habe. Zudem sei das Verhalten des Klägers auch deshalb grob fahrlässig, weil er angesichts des Erhalts der PushTAN-Benachrichtigung „aus dem Nichts“ in besonderem Maße hätte stutzig werden müssen. Ihm hätte sich in eklatanter Weise aufdrängen müssen, dass er überhaupt keinen Auftrag erteilt habe. Auch der vom Landgericht angesprochenen Verifizierung zum Login in das Online-Banking gehe ein vom Kläger initiiertes Einloggen voraus. Dies gelte umso mehr, als der Auftrag mit „Registrierung Karte“ und der Hinweis-Bitte versehen gewesen sei, nur einen explizit erteilten Auftrag zu freizugeben. Darüber hinaus habe der Auftrag „Registrierung Karte“ für den Kläger einen konkreten Inhalt aufgewiesen, weil er – wie er in der mündlichen Verhandlung bestätigt habe – bei einem anderen Kreditinstitut eine Debitkarte im Online-Banking bei Apple Pay hinterlegt habe. Sofern der Kläger die Freigabe des Auftrages während eines Gesprächs mit seinem Vorgesetzten erteilt habe, sei dies als besonders leichtfertig zu bewerten. Entgegen der Auffassung des Landgerichts liege jedenfalls ein Mitverschulden des Klägers vor. Der Kläger sei verpflichtet gewesen, zumindest alle zwei Tage seinen Kontostand zu kontrollieren. Ein Ausschlussgrund gemäß § 675v Abs. 4 BGB liege nicht vor. Der Kläger habe die Digitalisierung der Karte über sein Freigabe-Medium (PushTAN-App) autorisiert. Darin sei ihm der Hinweis auf die Digitalisierung der Karte angezeigt worden. Da auf seinem Gerät erkennbar keine Provisionierung der Karte erfolgt sei, habe er erkennen müssen, dass die Installation auf einem dritten Gerät erfolgt sei.

15 Der Kläger verteidigt das erstinstanzliche Urteil und beantragt unter Wiederholung und Vertiefung seines erstinstanzlichen Vorbringens, die Berufung zurückzuweisen.

16 Wegen der Einzelheiten des Berufungsvorbringens der Parteien wird auf den Inhalt der im Berufungsrechtszug gewechselten Schriftsätze nebst Anlagen Bezug genommen.

II.

17 Die Berufung der Beklagten ist zulässig, aber unbegründet.

18 1. Dem Kläger steht gegen die Beklagte ein Anspruch auf Gutschrift in Höhe von 42.182,68 EUR in Höhe von § 675u Satz 2 Halbsatz 2 BGB zu.

19 a) 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. Voraussetzung für die Autorisierung eines Zahlungsvorgangs ist, dass das nach § 675j Abs. 1 Satz 3 BGB konkret vereinbarte Authentifizierungsverfahren vollständig eingehalten wurde; eine Autorisierung des über ein Zahlungsinstrument nach § 675j Abs. 1 Satz 4 BGB erteilten Zahlungsauftrags scheitert deshalb bereits dann, wenn auch nur eines der Elemente des vereinbarten Authentifizierungsverfahrens kompromittiert ist (vgl. Maihold in Ellenberger/Bunte, BankR-HdB, 6. Aufl., § 33 Rn. 145 zum Online-Banking; vgl. auch BeckOGK/Köndgen, Stand: 15. Januar 2025, § 675j BGB Rn. 126 ff.; BGH, Urteil vom 26. Januar 2016 – XI ZR 91/14 –, NJW 2016, 2024 Rn. 14 zum smsTAN-Verfahren).

20 b) Dies ist hier der Fall.

21 aa) Der Kläger hat die streitgegenständlichen Zahlungsvorgänge nicht autorisiert.

22 (1) Die streitgegenständlichen 122 Verfügungen am „Point of Sale“ sind Zahlungsvorgänge im Sinne der § 675u Satz 2, § 675f Abs. 4 Satz 1 BGB, da durch sie Geldbeträge übermittelt wurden.

23 (2) Das zwischen den Parteien vereinbarte Autorisierungsverfahren wurde bei den einzelnen Zahlungsvorgängen nicht eingehalten.

24 (a) Nach Ziffer 4 der Bedingungen für die digitale S.-Card (Debitkarte) mit individualisierten Authentifizierungsverfahren (Anlage B11) erfolgt die Autorisierung des konkreten Zahlungsvorgangs „mit dem Einsatz der digitalen Debitkarte durch Heranführen des mobilen Endgerätes mit der digitalen Debitkarte an das Kontaktlos-Terminal bzw. im Online-Handel durch Bestätigung der Bezahlenwendung (...). Dazu ist zusätzlich die Verwendung der biometrischen Merkmale des Karteninhabers oder Eingabe des Entsperrcodes des Geräts jeweils mit auf dem mobilen Endgerät vorhandenen Funktionen erforderlich“.

25 (b) Diese Voraussetzungen sind nicht erfüllt.

26 Der Kläger hat unstreitig nicht die einzelnen Kartenzahlungen durch Heranführen des mobilen Endgeräts mit der digitalen Debitkarte an das Kontaktlos-Terminal oder im Online-Handel durch Bestätigung der Bezahlenwendung veranlasst. Entgegen der Auffassung der Beklagten hat er durch die – unterstellte – Freigabe des Auftrags „Karte registrieren“ in seiner PushTAN-App nicht die einzelnen Transaktionen autorisiert (vgl. OLG

Brandenburg, Urteil vom Urteil vom 15. Januar 2025 – 4 U 32/24 –, Rn. 26 ff., juris; vgl. auch BGH, Urteil vom 26. Januar 2016 – XI ZR 91/14 –, Rn. 58, juris; aM Weinmann, jurisPK-BKR 2/2024 Anm 4). Eine derartige vorgelagerte Autorisierung sehen die vereinbarten Bedingungen nicht vor.

- 27 bb) Die Beklagte ist kontoführender Zahlungsdienstleister. Es kann dahinstehen, ob Apple Pay bei den hier in Rede stehenden Zahlungsvorgängen als Zahlungsauslösedienstleister iSd § 1 Abs. 33 ZAG fungiert (Ebenroth/Boujong/Schmieder, HGB, 5. Aufl., § 675f BGB Rn. 23; BeckOGK/Foerster, Stand: 15. August 2025, § 675c BGB Rn. 262 f.; aA Mimming in Schäfer/Omlor/Mimming, ZAG, 2. Aufl., § 1 Rn. 577 mwN; Casper/Terlau, ZAG, 3. Aufl., § 1 ZAG Rn. 626), da die Beklagte gemäß § 675u Satz 5 BGB auch in diesem Fall die Pflichten aus § 675u Satz 2 BGB treffen.
- 28 c) Die Beklagte ist daher nach § 675u Satz 2 Halbsatz 2 BGB dazu verpflichtet, das Zahlungskonto des Klägers wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch die nicht autorisierten Zahlungsvorgänge in einer Gesamthöhe von unstreitig 42.182,68 EUR befunden hätte.
- 29 2. Die Beklagte kann gegenüber dem Anspruch des Klägers aus § 675u Satz 2 BGB weder wirksam mit einem Schadensersatzanspruch nach § 675v Abs. 3 Nr. 2 BGB aufrechnen noch ihm das Bestehen eines solchen Anspruchs nach § 242 BGB entgegenhalten.
- 30 a) Der Anspruch des Klägers auf Gutschrift aus § 675u Satz 2 BGB ist nicht wegen der von der Beklagten erklärten Aufrechnung mit einem Schadensersatzanspruch nach § 675v Abs. 3 Nr. 2 BGB erloschen, § 389 BGB. Es fehlt bereits an einer Gleichartigkeit der gegenüber stehenden Leistungen, § 387 BGB.
- 31 b) 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 (BGH, Urteil vom 22. Juli 2025 – XI ZR 107/24 –, Rn. 23 mwN, juris).
- 32 Der Beklagten steht gegen den Kläger aber kein Anspruch auf Schadensersatz aus § 675v Abs. 3 Nr. 2 BGB zu. Der Kläger ist gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB nicht zum Schadensersatz verpflichtet, weil die Beklagte für die Auslösung der streitgegenständlichen 122 Zahlungsvorgänge eine starke Kundenauthentifizierung im Sinne des § 1 Abs. 24 ZAG nicht verlangt hat.
- 33 aa) Der Zahler ist nach § 675v Abs. 4 Satz 1 BGB 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 (Nr. 1) oder nicht akzeptiert (Nr. 2). Bezugspunkt für die Anwendung der Vorschrift ist ausschließlich der im Streit stehende Zahlungsvorgang (vgl. BGH, Urteil vom 22. Juli 2025 – XI ZR 107/24 –, Rn. 34, juris).

- 34 bb) Die Beklagte war bei den hier in Rede stehenden Zahlungsvorgängen dazu verpflichtet, eine starke Kundenauthentifizierung zu verlangen.
- 35 Es kann dahinstehen, ob ein Zahlungsdienstleister zur Meidung der Folgen des § 675v Abs. 4 BGB eine starke Kundenauthentifizierung für sämtliche Zahlungsvorgänge verlangen muss, auch wenn eine solche aufsichtsrechtlich nicht vorgeschrieben ist (so Hoffmann, VuR 2016, 243, 248; BeckOK BGB/Schmalenbach, Stand: 1. November 2025, § 675v Rn. 17 ff.; Maihold in Ellenberger/Bunte, BankR-HdB, 6. Aufl., § 33 Rn. 86; aA OLG Frankfurt, Urteil vom 6. Dezember 2023 – 3 U 3/23 –, Rn. 55, juris; OLG Bremen, Beschluss vom 15. April 2024 – 1 U 47/23 –, Rn. 34, juris; MüKoHGB/Linardatos, 5. Aufl., Teil 1. K. Rn. 224; Staudinger/Omlor, BGB, Bearb. 2020, § 675v, Rn. 36 f.).
- 36 Denn bei den streitgegenständlichen Verfügungen handelte es sich um elektronisch ausgelöste Karten- und mobile Zahlungen am „Point of Sale“, für die gemäß § 55 Abs. 1 Satz 1 Nr. 2 ZAG eine starke Kundenauthentifizierung erforderlich ist (vgl. Begr RegE, BT-Drucks. 18/11495, 140; Zahrt in Casper/Terlau, ZAG, 3. Aufl., § 55 Rn. 42; Mimberg, BKR 2024, 209, 211). Die aufsichtsrechtliche Ausnahme nach § 55 Abs. 5 ZAG iVm Art. 11 VO 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 (künftig: RTS), wonach bei kontaktlosen Kleinbetragszahlungen an der Verkaufsstelle grundsätzlich bei Zahlungsbeträgen bis 50 Euro ohne starke Kundenauthentifizierung verfahren werden kann, sofern die letzte starke Kundenauthentifizierung nicht mehr als 150 Euro Transaktionsvolumen oder fünf Zahlungsvorgänge zurückliegt, ist nicht einschlägig. Vorliegend fand die erste der vereinzelt unter 50 EUR liegenden Verfügungen erst am 19. April 2022 statt, als bereits kontaktlose elektronische Zahlungsvorgänge von zusammengekommen deutlich über 150 EUR ausgelöst worden waren (vgl. im Einzelnen Anlage K1), Art. 11 lit. b RTS.
- 37 cc) Die Beklagte hat für die Auslösung der streitgegenständlichen Zahlungsvorgänge keine starke Kundenauthentifizierung verlangt.
- 38 (1) (a) Entscheidend für den Ausschluss der Haftung nach § 675v Abs. 4 Satz 1 BGB ist, ob eine starke Kundenauthentifizierung verwendet wird, deren Nutzung bei dem im Streit stehenden Zahlungsvorgang verlangt wird und ob die Elemente der starken Kundenauthentifizierung vor Freigabe des konkreten Zahlungsvorgangs auch tatsächlich korrekt überprüft werden (vgl. OLG Naumburg, Urteil vom 10. Januar 2024 – 5 U 83/23 –, Rn. 59, juris; Maihold in Ellenberger/Bunte, BankR-HdB, 6. Aufl., § 33 Rn. 386; BeckOGK/Birne, Stand: 1. Dezember 2025, § 675v BGB Rn. 93; Herresthal in Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., Kap. 7, § 675v BGB Rn. 47).
- 39 (b) Starke Kundenauthentifizierung ist nach § 1 Abs. 24 ZAG eine Authentifizierung, die so ausgestaltet ist, dass die Vertraulichkeit der Authentifizierungsdaten 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. Kategorie Besitz, also etwas, das nur der Nutzer besitzt oder 3. Kategorie Inhärenz, also etwas, das der Nutzer ist.

- 40 Nach Ziffer 2 der Bedingungen für die digitale S.-Card (Debitkarte) mit individualisierten Authentifizierungsverfahren (Anlage B11) haben die Parteien als Authentifizierungselemente „die digitale Debitkarte auf dem mobilen Endgerät des Karteninhabers als erster Faktor (Besitzelement)“ und „biometrische Elemente des Karteninhabers, z.B. Fingerabdruck, Gesichtserkennung bzw. sonstige Entsperrmechanismen des mobilen Endgeräts (z.B. der Entsperrcode), jeweils als zweiter Faktor“ vereinbart.
- 41 (2) Die Beklagte hat vor den Freigaben der Zahlungsvorgänge das Besitzelement nicht ausreichend überprüft.
- 42 (a) Eine in einem „Wallet“ wie zB Apple Pay abgelegte tokenisierte Zahlungskarte kann als Besitzelement im Sinne des § 1 Abs. 24 ZAG fungieren (Mimberg in Schäfer/Omlor/Mimberg, ZAG, 2. Aufl., § 1 Rn. 474; Terlau in Casper/Terlau, ZAG, 3. Aufl., § 1 Rn. 503; Schwennicke in Schwennicke/Auerbach, ZAG, 4. Aufl., § 1 Rn. 207; MüKoBGB/Jungmann, 9. Aufl., § 675m Rn. 18; MüKoHGB/Linardatos, 5. Aufl., Teil 1, K. Rn. 28; Herresthal in Langenbucher/Bliesener/Spindler/Herresthal, Bankrechts-Kommentar, 3. Aufl., BGB vor § 675j-676c Rn. 55c; Mimberg, BKR 2024, 209, 211). Hierfür spricht Erwägungsgrund Nr. 6 der RTS, welcher als mögliche Sicherheitsmerkmale von Besitzelementen explizit „Algorithmuspezifikationen, Schlüssellänge und Informationsentropie“ benennt. Diese Verordnung ist seit dem 14. September 2019 unmittelbar geltendes Recht, Art. 38 RTS.
- 43 (b) Die Beklagte hat in dem Registrierungsverfahren für die digitale Debitkarte nicht ausreichend sichergestellt, dass nur der Kläger den Besitz an der digitalen Debitkarte erlangt. Dieses Versäumnis setzt sich bei den einzelnen Zahlungsvorgängen unmittelbar fort.
- 44 (aa) Gemäß Art. 24 Abs. 1 RTS stellt der Zahlungsdienstleister sicher, dass nur der Zahlungsdienstnutzer den personalisierten Sicherheitsmerkmalen – wie der digitalen Debitkarte (vgl. dazu vgl. MüKoHGB/Linardatos, 5. Aufl., Teil 1, G. Rn. 38 f.) – zugeordnet wird und dabei Sicherheit gewährleistet ist. Konzipiert der Zahlungsdienstleister sein starkes Kundenauthentifizierungsverfahren unter Einsatz eines Besitzelements, muss er sich daher davon überzeugen können, dass sich das jeweilige Element im Besitz des Nutzers befindet (vgl. Mimberg in Schäfer/Omlor/Mimberg, ZAG, 2. Aufl., § 1 Rn. 472 f.; Casper/Terlau, ZAG, 3. Aufl., § 1 Rn. 505). Dabei darf sich der Zahlungsdienstleister darauf verlassen, dass der Nutzer den ihm im Zusammenhang mit dem Besitzelement obliegenden Pflichten nachkommt (vgl. Mimberg in Schäfer/Omlor/Mimberg, ZAG, 2. Aufl., § 1 Rn. 472 f.; BeckOK BGB/Schmalenbach, Stand: 1. November 2025, § 675v Rn. 15b).
- 45 Die digitale Debitkarte wurde im vorliegenden Fall bestimmungsgemäß auf einem Mobiltelefon gespeichert (vgl. Ziffer 1 der Bedingungen für die digitale S.-Card (Debitkarte) mit individualisierten Authentifizierungsverfahren, Anlage B11). Die Beklagte hatte daher sicherzustellen, dass die digitale Debitkarte auf einem Mobiltelefon im Besitz des Klägers gespeichert wird.
- 46 (bb) Diesen Anforderungen ist die Beklagte nicht ausreichend nachgekommen.
- 47 (aaa) Die Einrichtung der digitalen Debitkarte für Apple Pay erfolgte im vorliegenden Fall über die S.-App (vgl. Schritte 1 bis 3, 5 bis 10 der „Karten-Provisionierung mit der S.-App 6.0“, Anlage B1). Die Initiative zur Einrichtung konnte zwar auch in der Wallet-App gestartet werden, dann führte der Weg zur Initiierung des Auftrages aber in jedem Fall über die S.-App. Dies setzte zunächst das Einloggen in die S.-App unter Eingabe der On-

line-Zugangsdaten des Klägers voraus. Eine gesonderte Verifizierung des dafür verwendeten Mobiltelefons als vertrauenswürdig war dafür nicht erforderlich. Die Auftragserteilung setzte weiter die Freigabe eines mit der Bezeichnung „Karte registrieren“ versehenen Auftrages in der PushTAN-App des Klägers voraus (vgl. Anlage B1, Schritt 4), für deren Einrichtung damals die Eingabe eines per Brief an den Kunden übermittelten Aktivierungs-codes erforderlich war. Die S.-App musste auf dem Endgerät installiert sein, auf dem später die digitale Debitkarte genutzt werden sollte, nicht dagegen die PushTAN-App (vgl. insgesamt die Angaben des Mitarbeiters der Beklagten Herrn A. in der mündlichen Verhandlung vom 11. November 2025, S. 2 f. = II 91 f.).

- 48 (bbb) Durch dieses Verfahren wird eine ausreichende Zuordnung der Debitkarte zum Zahlungsdienstnutzer nicht sichergestellt.
- 49 Für den Beginn des Einrichtungsvorgangs durch das Einloggen in die S.-App war keine Verifizierung des dafür verwendeten Mobiltelefons als vertrauenswürdig erforderlich. Die dafür notwendige Eingabe der Zugangsdaten für das Online-Banking des Klägers stellte die Zuordnung des Klägers mit dem davon unabhängigen Besitzelement nicht sicher. Eine ausreichend sichere Zuordnung wurde auch nicht in Verbindung mit der anschließenden – unterstellten – Freigabe in der PushTAN-App des Klägers hergestellt. Bei diesem Schritt konnte die Beklagte angesichts der dafür erforderlichen starken Kundenauthentifizierung (vermittelt über den Besitz des für die PushTAN-App registrierten Mobiltelefons und die Gesichtserkennung) zwar davon ausgehen, dass die Freigabe auch tatsächlich durch den Kläger erfolgte. Ein Rückschluss von der Freigabe auf den Besitz des Klägers an dem Mobiltelefon, auf dem die digitale Debitkarte in Auftrag gegeben und gespeichert wurde, war aber nicht zulässig. Denn die Beklagte durfte nicht annehmen, dass sich der Kläger bei der Freigabe bewusst war, die Speicherung einer digitalen Debitkarte auf einem anderen als dem für die Freigabe verwendeten Mobiltelefon freizugeben. Die allgemeine Formulierung „Karte registrieren“ lässt nach Auffassung des Senats für den Kläger bereits nicht sicher erkennen, dass damit überhaupt die Speicherung einer digitalen Debitkarte auf einem Mobiltelefon verbunden ist. Erst recht musste der Kläger nicht von einer Speicherung auf einem anderen Mobiltelefon ausgehen, weil er sein Mobiltelefon für die Einrichtung der PushTAN-App bereits gesondert registriert hatte und in Ziffer 2 der Bedingungen für die digitale S.-Card (Debitkarte) mit individualisierten Authentifizierungsverfahren (Anlage B11) als Besitzelement die digitale Debitkarte „auf dem mobilen Endgerät des Karteninhabers“ vereinbart war.
- 50 Eine andere Bewertung ist nicht deswegen angezeigt, weil sich die Beklagte darauf verlassen durfte, dass der Kläger den ihm im Zusammenhang mit dem Besitzelement obliegenden Pflichten nachkommen würde. Der Kläger hat durch die unterstellte Freigabe des Auftrages „Karte registrieren“ in seiner PushTAN-App keine ihm im Zusammenhang mit der digitalen Debitkarte als Besitzelement obliegenden Pflichten verletzt. Bei dem damit etwaig verbundenen Verstoß gegen die Pflicht des Zahlungsdienstnutzers aus Ziffer 7.3 der Bedingungen für das Online-Banking (Anlage K13 = AH K I 94), vor der Bestätigung eines Auftrages die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen, fehlt es angesichts der allgemeinen Bezeichnung des Auftrages „Karte registrieren“ an einem spezifischen Bezug zu dem Besitzelement. Die in Ziffer 7.1 Abs. 2 lit. b der Sonderbedingungen für das Online-Banking (Anlage K13 = AH K I 93 f.) vereinbarten spezifischen Sorgfaltspflichten zum Schutz des mobilen Endgeräts als Besitzelement beziehen sich erst auf den Zeitraum nach erfolgter Widmung zum Besitzelement und betreffen die hiesige Fallgestaltung nicht. Ohnehin weist der letzte

Spiegelstrich unter (b) darauf hin, dass ein neues Besitzelement nur mittels eines von der Bank übermittelten Codes aktiviert werden kann.

- 51 (3) Aus den obigen Ausführungen folgt zugleich, dass der zweite Faktor, nämlich die Inhärenz, die durch das Entsperren des Mobiltelefons verwirklicht wurde, weder ausreichend überprüft wurde noch die notwendige Unabhängigkeit der beiden Faktoren voneinander in dem Sinne erfüllt ist, dass die Nichterfüllung des einen Elements die Zuverlässigkeit des anderen Elements nicht infrage stellt, vgl. Erwägungsgrund 6 RTS.
- 52 Als zweiter Faktor waren nach Ziffer 2 der Bedingungen für die digitale S.-Card (Debitkarte) mit individualisierten Authentifizierungsverfahren, Anlage B11 „biometrische Elemente des Karteninhabers, z.B. Fingerabdruck, Gesichtserkennung bzw. sonstige Entsperrmechanismen des mobilen Endgeräts (z.B. der Entsperrcode)“ vereinbart.
- 53 Da der Besitz des Klägers an dem Mobiltelefon, auf dem die digitale Debitkarte gespeichert war, nicht ausreichend sichergestellt war, konnte die Beklagte auch nicht davon ausgehen, dass bei der Auslösung der streitgegenständlichen Zahlungsvorgänge biometrische Merkmale des Klägers zum Einsatz kamen.
- 54 dd) Daher kann offen bleiben, ob der Kläger den Schaden im Sinne des § 675v Abs. 3 Nr. 2 lit. a) oder b) BGB grob fahrlässig verursacht hat, indem er am 11. April 2022 in der PushTAN-App seines Mobiltelefons einen mit der Bezeichnung „Karte registrieren“ bezeichneten Auftrag (vgl. Anlage B1, Schritt 4) durch Drücken des roten Buttons „Auftrag freigeben“ freigegeben und auf diese Weise die Registrierung der digitalen Debitkarte in dem auf dem Smartphone des Täters eingerichteten A.-Wallet ermöglicht hat.

III.

- 55 Die Kostenentscheidung folgt aus § 97 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit basiert auf § 708 Nr. 10, § 711 ZPO.
- 56 Die Revision wird wegen grundsätzlicher Bedeutung (§ 543 Abs. 2 Satz 1 Nr. 1 ZPO) zugelassen. Hinsichtlich des Ausschlusses des Schadensersatzanspruchs aus § 675v Abs. 3 BGB gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB stellt sich über den vorliegenden Einzelfall hinaus die klärungsbedürftige Frage, welche Anforderungen an das „Verlangen“ einer starken Kundenauthentifizierung durch den Zahlungsdienstleister zu stellen sind.