LG Nürnberg-Fürth, Endurteil v. 29.06.2023 – 6 O 5996/22

Titel:

Unbegründete Ansprüche eines Kontoinhabers auf Kontoberichtigung und Schadensersatz gegen seine Bank

Normenketten:

§ 254 Abs. 1, § 675u, § 675v Abs. 4 S. 1 Nr. 1, § 675w, § 823 Abs. 2
ZAG § 1 Abs. 24 § 55 Abs. 1

Leitsätze:

1. Die Ausgestaltung des Begriffs der groben Fahrlässigkeit ist durch die Zahlungsdienste-Richtlinie dem einzelstaatlichen Recht überlassen. Hiernach liegt grobe Fahrlässig vor, wenn die im Verkehr erforderliche Sorgfalt in besonderem schwerem Maße verletzt wurde, wenn einfachste, ganz nahe liegende Überlegungen nicht angestellt wurden und das nicht beachtet wurde, was im gegebenen Fall jedem einleuchten muss. (Rn. 23 – 35) (redaktioneller Leitsatz)
2. Ein Schadensersatzanspruch besteht aufgrund des Mitverschuldens (§ 254 Abs. 1 BGB) der Kontoinhaberin ebenfalls nicht. Dieses überwiegt bei einer Abwägung mit den behaupteten Verursachungsbeiträgen der Bank, deren Vorliegen unterstellt, in derart hohem Maß, dass eine Schadensersatzpflicht im Ergebnis nicht besteht. (Rn. 37) (redaktioneller Leitsatz)

Schlagworte:

Kontoberichtigung, Girokonto, Kundenauthentifizierung, Online-Banking-System, TAN-Verfahren, Push-TAN-App, SMS, grob fahrlässig, Mitverschulden

Fundstellen:

ZBB 2024, 212
ZIP 2024, 744
LSK 2023, 20494

Tenor

1. Die Klage wird abgewiesen.

2. Die Klägerin hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 21.998,92 € festgesetzt.

Tatbestand

1
Die Klägerin begehrt von der Beklagten die Gutschrift von ihrem Girokonto abgehender Zahlungen.

2
Die Parteien schlossen am 12.01.2018 den Girovertrag „Privatgirokonto“ und den Rahmenvertrag über die Teilnahme am Online-Banking (jeweils Anlage B1). Auf dieser Grundlage unterhält die Klägerin bei der Beklagten ein Girokonto, das unter der IBAN […] geführt wird, sowie ein Geldmarktkonto S-Cash, das unter der IBAN […] geführt wird. Im Zeitraum vom 27.08.2022 bis zum 01.09.2022 kam es auf beiden vorgenannten Konten zu einer Vielzahl von Kontobewegungen. Hinsichtlich der Buchungen im Einzelnen wird auf Blatt 13/14 der Akten Bezug genommen.

3
Der Login des Kunden in das Online-Banking-System der Beklagten erforderte im Zeitraum der hier interessierenden Kontobewegungen im Regelfall lediglich die Angabe einer statischen Benutzerkennung

und eines statischen Kennworts. Eine darüber hinaus gehende Authentifizierung, etwa mittels einer TAN-App, war für den bloßen lesenden Zugriff nicht erforderlich. Im Online-Banking-System konnten Zahlungsvorgänge oder sonstige potentiell bestandsverändernde Handlungsschritte, so das Heraufsetzen des Überweisungslimits oder die Installation des Zahlungsdienstes Apple-Pay, angestoßen werden. Um diese auszulösen, war zusätzlich die Freigabe mittels einer TAN-App erforderlich, die sich auf dem gleichen mobilen Endgerät, auf dem der Login in das Online-Banking-System erfolgt ist, befinden konnte. Hierbei wurde durch Bewegen eines auf dem Bildschirm eingeblendeten Reglers von links nach rechts mittels Fingerdrucks die Freigabe erklärt. Die Neueinrichtung der Push-TAN-App auf einem anderen als dem bislang genutzten Mobilfunkgerät erfolgte durch Übersendung eines Aktivierungslinks per SMS, der erst nach Einloggen in das Online-Banking und Beantwortung einer Sicherheitsfrage an das bislang genutzte Mobiltelefon übersandt wird.

4
Zahlungen mittels Apple-Pay waren in diesem Zeitraum nur möglich, wenn sie durch Vorweisen eines Mobiltelefons, auf dem die entsprechende App installiert war, sowie durch ein weiteres Authentifizierungselement wie Face-ID, Touch-ID oder Code, freigegeben wurden.

5
Am 20.08.2022 gegen 19:22 Uhr erhielt die Klägerin unter der Rufnummer +49[…] eine SMS-Nachricht mit dem Inhalt: „Ihre Registrierung für das TAN-Verfahren läuft am 20.08.2022 ab. Bitte verlängern Sie ihre Legitimation unter […]“. Die Klägerin loggte sich auf der angegebenen Website, die nicht durch die Beklagte betrieben wird, ein und gab, wie dort zur Verlängerung des TAN-Verfahrens von ihr verlangt, ihre Kartennummer, Name und Adresse ein. Im Anschluss bekam sie die Mitteilung, dass das TAN Verfahren erfolgreich verlängert worden sei.

6
Am 27.08.2022 um 14:27 Uhr erhielt die Klägerin einen Anruf mit der Rufnummer der Beklagten. Der Anrufer stellte sich als Mitarbeiter der IT-Abteilung vor und fragte nach, ob die Klägerin in letzter Zeit etwaige SMS erhalten hätte. Hierauf teilte die Klägerin dem Anrufer mit, dass sie die oben beschriebene SMS erhalten habe. Der Anrufer teilte mit, dass ihr Banksystem eine IP-Adresse aus Russland erkannt hätte, mit der die Erhöhung des Tageslimits versucht worden sei. Aus diesem Grund hätte man das Konto gesperrt. Die Klägerin müsse jetzt aber noch die Zugangsdaten zum Online Banking sperren und Neue beantragen.

7
Dafür würde der Anrufer der Klägerin über das System eine Nachricht über die Push-TAN-App schicken, die sie bestätigen sollte. Die Klägerin hegte Zweifel und fragte den Anrufer, woran sie erkennen könne, dass er wirklich bei der S. tätig sei. Der Anrufer meinte, dass nur Angestellte der Bank Zugriff auf das System hätten und Anrufe über die Nummer der S. tätigen können. Der Anrufer teilte der Klägerin auch ihren vollständigen Namen, Adresse, Geburtsdatum und Name des Beraters mit. Der Anrufer wusste auch, dass der Bankberater vor Kurzem gewechselt hatte. Die um 14:32 Uhr generierte Push-TAN, die ihrem Wortlaut nach der Erhöhung des Überweisungslimits diente, bestätigte die Klägerin.

8
Anschließend bekam die Klägerin auch eine SMS von dem offiziellen System der S., von dem sie auch schon zuvor offizielle Nachrichten bekommen hatte. In dieser SMS war ein Link, den die Klägerin an ihren Sachbearbeiter bei der S. schicken sollte, damit die Sperrung ihres Online-Bankings fertiggestellt werden konnte. Die SMS bezog sich ihrem Wortlaut nach auf die Deaktivierung der Push-TAN-App auf dem Handy der Klägerin und die Neuinstallation der Push-TAN-App auf einem anderen Mobilfunkgerät. Sie enthielt den ausdrücklichen Hinweis, den Link nicht weiterzuleiten. Diese Nachricht kopierte sie dann und schickte sie über das offizielle Postfach der S.-App an ihren zuständigen Berater bei der S. in R. Anschließend sollte die Klägerin in der Push-TAN App eine Anfrage der S. bestätigen, um das Online-Banking zu deaktivieren. Der Anweisung folgte die Klägerin. Hierauf wurde die Klägerin darauf hingewiesen, dass das Konto nun die nächsten zwei Tage deaktiviert sei und am Montag bzw. Dienstag neue Zugangsdaten per Post kommen würden. Am 29.08.2022 stellte die Klägerin fest, dass erhebliche Zahlungsanweisungen, in der Mehrzahl mittels Apple-Pay, erfolgt waren. Sie meldete sich umgehend in ihrer Filiale.

9

Die Klägerin behauptet, sie habe die streitgegenständlichen Kontobewegungen nicht autorisiert. Sie habe sich weder an den Orten aufgehalten, an denen die Apple-Pay Zahlungsanweisungen ausgelöst wurden, noch habe sie sonst im Tatzeitraum eingekauft. Vielmehr habe sie am 27.08.2022 ein Fitnessstudio besucht, in der Nacht auf den 28.08.2022 bei einer Freundin übernachtet und den 28.08.2022 in einer Therme verbracht. Sie rügt das Fehlen der Vorlage unterstützender Beweismittel im Sinne von § 675w Satz 4 BGB durch die Beklagte. Den Zahlungsdienst Apple-Pay habe sie zu keinem Zeitpunkt verwendet. Aus der Tatsache, dass in der von ihr am 20.08.2022 empfangenen SMS das Wort „ihre“ als Anrede in der Höflichkeitsform nicht groß geschrieben worden sei, habe sie nicht schließen müssen, dass die Nachricht nicht von der S. stamme. Gleiches gelte für die Tatsache, dass das Endkürzel der Internetadresse, auf der sich die Klägerin einloggte, dem Staat „Tonga“ zugeordnet sei, zumal die Endung nicht auf den Standort des Servers schließen lasse und auch das Kürzel „de“ in der Adresse enthalten sei. In Bezug auf den Zahlungsdienst Apple-Pay könne sie bereits deshalb nicht grob fahrlässig gehandelt haben, da sie dieses Zahlungsinstrument gar nicht erhalten habe.

10
Die Klägerin meint, sie habe einen Kontoberichtigungsanspruch gemäß § 675u BGB, hilfsweise einen Schadensersatzanspruch gemäß §§ 823 Abs. 2 BGB, 55 Abs. 1, 1 Abs. 24 ZAG. Die Klägerin ist der Ansicht, sie habe im Zusammenhang mit den streitgegenständlichen Zahlungsbewegungen nicht grob fahrlässig gehandelt. Sie meint, die Beklagte könne sich auf eine – von ihr in Abrede gestellte – grobe Fahrlässigkeit zudem gemäß § 675v Abs. 4 BGB nicht berufen, da diese Vorschrift bereits für den bloßen Login eine starke Kundenauthentifizierung fordere. Zudem erfülle das Push-TAN-Verfahren der Beklagten nicht die Anforderungen an eine starke Kundenauthentifizierung, da es technisch möglich sei, für den Betrieb des Online-Bankings und für die Push-TAN-App dieselbe Hardwarekomponente zu verwenden.

11
Die Klägerin hat beantragt,

1. Die Beklagte wird dazu verurteilt, dem Kläger die nachfolgend dargestellten abgehenden Zahlungen … zu dem darin jeweils ausgewiesenen Wertstellungsdatum dem Konto mit der IBAN […] in den Kontokorrent als Haben-Betrag wieder gutzuschreiben nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz aus 21.998,92 EUR seit dem 31.08.2022 und etwaige Kreditzinsen, die durch das aufgelaufene Soll der oben dargestellten Zahlungen entstanden sind, auszubuchen.

2. Hilfsweise und nur für den Fall, dass das erkennende Gericht den Klageantrag zu Ziffer 1 für unzulässig erachtet, wird die Beklagte dazu verurteilt, an die Klägerin einen Geldbetrag in Höhe von 21.998,92 EUR nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 31.08.2022 zu zahlen.

3. Die Beklagte wird dazu verurteilt, an die Klägerin die außergerichtlich angefallene Geschäftsgebühr in Höhe von 2.069,41 EUR nebst fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 20.09.2022 zu zahlen.

12
Die Beklagte hat beantragt,

die Klage abzuweisen.

13
Die Beklagte trägt vor, die Zahlungen seien durch die Klägerin autorisiert worden. Die Beklagte meint, sie könne sich für die Autorisierung auf ein praktisch nicht überwindbares Sicherheitssystem stützen. Der Anscheinsbeweis sei durch die Klägerin nicht erschüttert worden, da ein alternativer Geschehensablauf durch die Klägerin nicht unter Beweis gestellt worden sei.

14
Die Beklagte ist der Ansicht, die Klägerin habe grob fahrlässig gegen ihre Sorgfaltspflichten als Kundin verstoßen, § 675v Abs. 3 BGB. Hinsichtlich der Gesichtspunkte, aus denen die Beklagte die grobe Fahrlässigkeit im Einzelnen ableitet, wird auf Blatt 83 bis 87 der Akten Bezug genommen. Die Beklagte meint, hieraus folge ein Schadensersatzanspruch der Beklagten, mit dem diese hilfsweise aufrechne.

15

Die Beklagte meint, § 675v Abs. 4 BGB sei nur dann zum Nachteil des Zahlungsdienstleisters anwendbar, wenn beim Zahlungsvorgang selbst keine starke Kundenauthentifizierung angeboten werde. Beim Einloggen das Online-Banking werde zudem eine Freigabe per Push-TAN gefordert, wenn sich der Nutzer nicht innerhalb der letzten 90 Tage bereits einmal per Push-TAN legitimiert habe. Das Geburtsdatum und die vollständige Kartennummer würden nicht angezeigt. Die seitens der Beklagten verwendete Push-TAN-App stelle aufgrund des Promon Shields auch dann eine starke Kundenauthentifizierung dar, wenn sie auf dem gleichen Gerät installiert sei, auf dem das Online-Banking betrieben werde. Mithin seien die für die Authentifizierung verwendeten Elemente voneinander unabhängig. Die zum Tatzeitpunkt verwendete Push-TAN-App sei praktisch nicht überwindbar. Dies habe der TÜV Saarland bestätigt.

16
Die Installation der Push-TAN-App auf einem neuen Mobilgerät sei nicht ohne Mitwirkung der Klägerin möglich gewesen. Gleiches gelte für die Aktivierung des Zahlungsdienstes Apple-Pay. Da Zahlungen mit Apple-Pay eine starke Kundenauthentifizierung erforderten, werde eine solche nicht s.-seitig zusätzlich gefordert.

17
Für die Einzelheiten des Parteivorbringens wird auf die gewechselten Schriftsätze sowie auf das Protokoll der mündlichen Verhandlung vom 25.05.2023 Bezug genommen. Das Gericht hat keinen Beweis erhoben.

Entscheidungsgründe

18
Die zulässige Klage erweist sich im Hauptantrag als unbegründet.

19
Die Klage ist zulässig. Insbesondere ist das Landgericht Nürnberg-Fürth nach §§ 23 Nr. 1, 71 Abs. 1 GVG sachlich und nach §§ 12, 17 ZPO örtlich zuständig.

20
Die Klage ist jedoch unbegründet.

21
Die Klägerin hat gegen die Beklagte weder Anspruch auf Kontoberichtigung gemäß § 675u BGB (1), noch auf Schadensersatz gemäß §§ 823 Abs. 2 BGB, 55 Abs. 1, 1 Abs. 24 ZAG (2).

22
(1) Die Klägerin hat gegen die Beklagte keinen Anspruch auf Kontoberichtigung gemäß § 675u Satz 2 BGB. Insoweit kann dahinstehen, ob die Klägerin die inmitten stehenden Zahlungsvorgänge autorisiert hat. Selbst, soweit dies nicht der Fall war, besteht ein Kontoberichtigungsanspruch nämlich aufgrund des grob fahrlässigen Handelns der Klägerin nicht, § 675 v Abs. 3 BGB (a). § 675v Abs. 4 BGB hindert die Beklagte nicht daran, sich hierauf zu berufen (b).

23
(a) Die Klägerin hat den ihr entstandenen Schaden durch grob fahrlässige Verletzung mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments gemäß § 675v Abs. 3 Nr. 2b) BGB herbeigeführt. Die Ausgestaltung des Begriffs der groben Fahrlässigkeit ist durch die Zahlungsdienste-Richtlinie dem einzelstaatlichen Recht überlassen. Hiernach ist nicht jedes unsachgemäße oder sorgfaltswidrige Verhalten des Zahlungsdienstenutzers als grob fahrlässig anzusehen. Grobe Fahrlässigkeit liegt vielmehr nur vor, wenn die im Verkehr erforderliche Sorgfalt in besonderem schwerem Maße verletzt wurde, wenn einfachste, ganz nahe liegende Überlegungen nicht angestellt wurden und das nicht beachtet wurde, was im gegebenen Fall jedem einleuchten musste (vgl. Schwintowski in:Juris-PK BGB, 10. Auflage 2023, Rdnr. 13, 14 zu § 675v BGB mit weiteren Nachweisen).

24
(aa) Das Verhalten der Klägerin am 20.08.2022 im Zusammenhang mit der an diesem Tag von ihr erhaltenen SMS war grob fahrlässig.

25
Die Klägerin hat sich am 20.08.2022 auf der Website „[…].to“ eingeloggt, mithin dort in einer Maske ihre Benutzerkennung und ihr Kennwort für das Online-Banking der Beklagten eingegeben. Sodann hat sie ihren

Namen, ihre Adresse und ihr Kartennummer angegeben. Hierdurch hat sie grob fahrlässig gehandelt. Der Link zu der Website wurde der Klägerin durch eine SMS übermittelt, in der die Klägerin auf den vermeintlichen Ablauf ihrer Registrierung für das TAN-Verfahren hingewiesen wurde. Eine Befristung für das von der Klägerin verwendete TAN-Verfahren, Push-TAN, war zwischen den Parteien ausweislich der Rahmenvereinbarung über die Teilnahme am Online-Banking nicht vereinbart. Bei der Rufnummer, von der die SMS abgesandt wurde, handelte es sich bereits nach dem Vortrag der Klägerin nicht um eine solche, die der Beklagten zugeordnet war. Schließlich war die Website, auf der die Klägerin ihre Benutzerkennung und ihr Kennwort (PIN) eingegeben hat, nicht eine der aus Ziffer 8 der Rahmenvereinbarung über die Teilnahme am Online-Banking ersichtlichen ausschließlichen Kommunikationswege für das Online-Banking-Angebot der Beklagten. Etwas anderes ergibt sich auch nicht aus der Tatsache, dass die Website neben dem Domain-Kürzel „.to“ auch das Domain-Kürzel „.de“ enthielt. Denn die Website ist regelmäßig dem Staat zuzuordnen, dessen Kürzel am Ende der Web-Adresse genannt wird. Schließlich wies die SMS auch einen Rechtschreibfehler auf, da die Höflichkeitsanrede „Ihre“ klein geschrieben war. Aufgrund der Vielzahl der dargelegten Anhaltspunkte für einen betrügerischen Ursprung der SMS und der Website hätte es sich der Klägerin aufdrängen müssen, dass die Bekanntgabe der persönlichen Daten auf der Website einem geplanten Angriff auf die Integrität des Online-Bankings dienen sollte. Jedenfalls hätte sie am nächstfolgenden Werktag bei der Beklagten nachfragen müssen, ob die SMS tatsächlich von dieser versandt wurde und ob die Website von dieser genutzt wird. Insoweit wäre es ihr auch zumutbar gewesen, den durch die SMS suggerierten Auslauf des TAN-Verfahrens, mithin die Unmöglichkeit, Transaktionen vorzunehmen, für einige wenige Tage in Kauf zu nehmen.

26
(bb) Das Verhalten der Klägerin am 27.08.2022 war grob fahrlässig, soweit sie an diesem Tag auf den Anruf eines vorgeblichen Mitarbeiters der Beklagten eine Push-TAN, die ihrem Wortlaut nach der Erhöhung des Überweisungslimits diente, freigab. Die Klägerin hat selbst nicht behauptet, zu diesem Zeitpunkt im Online-Banking-System einen Auftrag zur Erhöhung des vereinbarten Überweisungslimits erteilt zu haben. Dies wäre auch bereits deshalb abwegig, da die Klägerin sich hierfür in ihr Online-Banking hätte einloggen müssen und hierbei festgestellt hätte, dass das Konto – entgegen der Angaben des vorgeblichen Bankmitarbeiters – nicht gesperrt war. Etwas anderes ergibt sich auch nicht daraus, dass der Anruf von einer der Beklagten zugeordneten Telefonnummer aus erfolgte und der Anrufer persönliche Daten der Klägerin wie auch deren Bankberater und den insoweit stattgefundenen personellen Wechsel kannte. Denn die Push-TAN enthielt, wie die Klägerin im Termin zur mündlichen Verhandlung eingeräumt hat, folgenden Warnhinweis: „Bitte geben Sie keinen Auftrag frei, den Sie nicht explizit beauftragt haben. Wenden Sie sich bei Unklarheiten an Ihren Berater. Geben Sie telefonisch keine sensiblen Informationen weiter.“ Dieser Warnhinweis ist insbesondere hinsichtlich der Warnung, nur Aufträge freizugeben, die durch den Nutzer explizit beauftragt wurden, so deutlich, dass es jedermann einleuchten musste, dass der vorgebliche Mitarbeiter der Beklagten tatsächlich unlautere Absichten verfolgte und dass deshalb die Freigabe der Push-TAN geeignet war, Schäden zum Nachteil der Klägerin herbeizuführen oder zu vertiefen. Der hierin liegende Verstoß gegen Ziffer 7.3 der Bedingungen für das Online-Banking, die Auftragsdaten vor der Bestätigung zu prüfen, war mithin grob fahrlässig.

27
(cc) Die Klägerin verhielt sich am 27.08.2022 weiter grob fahrlässig, als sie einen ihr per SMS zugesandten Link über das Online-Banking-System der S. an den dort für sie zuständigen Mitarbeiter versandte. Dieser Link diente ausweislich des Wortlauts der SMS der Deaktivierung der Push-TAN-App auf dem bisher hierfür genutzten Mobilfunkgerät und der Neuinstallation auf einem anderen Mobilfunkgerät. Die SMS enthielt den ausdrücklichen Hinweis, diese Nachricht einem Dritten unter keinen Umständen weiterzuleiten. Zudem wurde eine Aufforderung durch Mitarbeiter der Beklagten, den Link zu übersenden, ausgeschlossen. Dies entspricht der Verpflichtung der Klägerin aus Ziffer 7.1 (2) (b) der Bedingungen für das Online-Banking, einen Code für die Aktivierung des Push-TAN-Verfahrens geheim zu halten. Dennoch kopierte die Klägerin den Aktivierungslink und sandte ihn über das Online-Banking-System der S. an diese. Bereits aufgrund der eindeutigen, unmissverständlichen Warnhinweise war die dennoch erfolgte Weiterleitung des Links grob fahrlässig, da jedermann hätte einleuchten müssen, dass die entgegen dieser Hinweise erfolgte telefonische Aufforderung hierzu betrügerischen Zwecken dienen wird. Zudem diente der Link ausweislich der SMS gerade nicht nur der – der Klägerin nach ihrem Vorbringen durch den Anrufer nahe gelegten – Sperrung der Online-Bankings, sondern der Deaktivierung des Push-TAN-Verfahrens und zugleich der Neuinstallation des Push-TAN-Verfahrens auf einem anderen Gerät. Mithin musste sich der Klägerin

aufgrund dieser Differenz zwischen den telefonischen Erklärungen des vorgeblichen Mitarbeiters der Beklagten und dem Wortlaut der SMS erschließen, dass sie zum Schutz ihres eigenen Vermögens von der begehrten Weiterleitung des Links absehen sollte.

28
(dd) Das unter (aa) bis (cc) geschilderte grob fahrlässige Verhalten der Klägerin hat den Schaden, mithin die streitgegenständlichen Abbuchungen, im Sinne von § 675v Abs. 3 Nr. 2b) BGB herbeigeführt. Das unter (aa) geschilderte Verhalten hat den Betreibern der dortigen Website ermöglicht, sich in das Online-Banking der Beklagten mit den Zugangsdaten der Klägerin einzuloggen und ihnen zugleich die Kartennummer der Klägerin verschafft, die durch die Beklagte abgefragt wird, wenn die Übersendung eines Links zur Neuinstallation der Push-TAN-App auf einem anderen als dem bisher genutzten Mobilfunkgerät erfolgen soll. Durch das unter (bb) geschilderte Verhalten hat die Klägerin die Verfügungsmöglichkeiten auch Dritter, denen sie durch ihr Verhalten den widerrechtlichen Zugriff auf ihr Konto ermöglichte, erhöht. Schließlich hat sie Dritten mittels des unter (cc) geschilderten Weiterleitens des Links die Installation der Push-TAN-App auf einem von diesen genutzten Mobiltelefon ermöglicht. Zwar erfolgte die Weiterleitung im Online-Banking-Account der Klägerin. Da sie durch das unter (aa) geschilderte Verhalten bereits Dritten hierzu Zugang ermöglicht hatte, hat sie hierdurch zugleich den Link diesen Personen zur Verfügung gestellt. Diese waren nunmehr zu jeglichen mittels Push-TAN freizugebenden Transaktionen vom Konto der Klägerin einschließlich der Installation und Nutzung des Zahlungsdienstes Apple-Pay in der Lage. Entgegen der Rechtsansicht der Klagepartei lässt die grobe Fahrlässigkeit der Klägerin die Haftung der Beklagten auch dann entfallen, wenn die Klägerin – wie von ihr vorgetragen – das Zahlungsinstrument „Apple-Pay“ zu keinem Zeitpunkt in Händen hatte. Die klägerseits insoweit zitierten Kommentarstellen (Blatt 164 der Akten) beziehen sich jeweils auf die begrenzte Haftung des Zahlungsdienstenutzers gemäß § 675v Abs. 1 BGB, nicht aber auf die unbeschränkte Haftung gemäß § 675v Abs. 3 BGB. Hierfür entscheidend ist der kausale Zusammenhang zwischen dem grob fahrlässigen Verhalten des Zahlungsdienstenutzers und dem eingetretenen Schaden, der, wie vorliegend, auch dann gegeben sein kann, wenn das grob fahrlässige Verhalten dritten Personen den Zugang zu einem Zahlungsinstrument ermöglicht, das der Zahlungsdienstenutzer selbst nie in Händen hatte.

29
Der Vortrag der Klägerin in einem nicht nachgelassenen Schriftsatz vom 25.05.2023 ist nach dem Schluss der mündlichen Verhandlung erfolgt und somit gemäß § 296a ZPO nicht berücksichtigungsfähig. Er ließe aber auch dann, wenn er zuzulassen wäre, die Kausalität nicht entfallen. Denn die Überweisungen vom Tagesgeldkonto der Klägerin auf deren Girokonto, die nach nunmehrigen Klägervortrag ohne Freigabe mittels Push-TAN, somit ohne starke Kundenauthentifizierung, erfolgt sind, wären ohne die Zugangsdaten der Klägerin zum Online-Banking nicht möglich gewesen; diese hat die Klägerin durch das unter (aa) geschilderte Verhalten grob fahrlässig Dritten zugänglich gemacht.

30
Entgegen der Rechtsansicht der Klägerin war die Beklagte auch nicht gemäß § 675w Satz 4 BGB zur Vorlage unterstützender Beweismittel gehalten. Denn sämtliche Tatsachen, auf denen sich die grobe Fahrlässigkeit der Klägerin gründet, sind zwischen den Parteien unstreitig geblieben. Erst, soweit die Pflichtverletzung des Zahlers streitig ist, greift jedoch § 675w BGB ein (vgl. Grüneberg/Grüneberg, Bürgerliches Gesetzbuch, 82. Auflage 2023, Rdnr. 1 zu § 675w BGB mit weiteren Nachweisen).

31
(b) Der Beklagten ist es nicht gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB verwehrt, sich auf die grobe Fahrlässigkeit der Klägerin zu berufen. Gemäß § 675v Abs. 4 Satz 1 Nr. 1 BGB trifft den Zahlungsdienstleister, vorliegend die Beklagte, die Obliegenheit, eine starke Kundenauthentifizierung zu fordern. Eine solche liegt vor, wenn der Zahler zur Authentifizierung mindestens zwei ausschließlich ihm eigene Elemente aus den Kategorien Wissen, Besitz und Inhärenz nutzt (vgl. Grüneberg/Grüneberg, Bürgerliches Gesetzbuch, 82. Auflage 2023, Rdnr. 10 zu § 675v BGB mit weiteren Nachweisen). Im hier interessierenden Zeitraum hat die Beklagte lediglich für bestandsverändernde Transaktionen, nicht aber für das Einloggen in das Online-Banking-System selbst eine starke Kundenauthentifizierung gefordert. Die Beklagte war indes nicht aus § 675v Abs. 4 BGB zu einer starken Kundenauthentifizierung für den bloßen lesenden Zugriff verpflichtet (aa). Für die einzelnen Zahlungsvorgänge hielt sie eine starke Kundenauthentifizierung vor (bb). Auf die Zahlungsvorgänge zwischen den Konten der Klägerin kommt es hierbei nicht an (cc).

32
(aa) Betrachtet man den Wortlaut des § 675v Abs. 4 Satz 1 Nr. 1 BGB isoliert, lässt er offen, ob er eine starke Kundenauthentifizierung nur für den einzelnen Zahlungsvorgang oder bereits für die bloße lesende Nutzung des Online-Bankings fordert. Höchst- oder obergerichtliche Rechtsprechung hierzu ist, soweit ersichtlich, bislang nicht ergangen. Aus Sicht der Kammer sprechen die besseren Argumente dafür, § 675v Abs. 4 Satz 1 Nr. 1 BGB dahingehend auszulegen, dass eine starke Kundenauthentifizierung nur für den einzelnen Zahlungsvorgang, nicht aber für den bloßen, lesenden Zugang zum Online-Banking vorzuhalten ist. Bereits aus dem systematischen Zusammenhang der Norm ergibt sich, dass sich diese ausschließlich auf die Authentifizierung beim Zahlungsvorgang selbst bezieht. So findet sich § 675v BGB im Kapitel 3, das mit „Erbringung und Nutzung von Zahlungsdiensten“ überschrieben ist. Nach den Unterkapiteln zu „Autorisierung von Zahlungsvorgängen; Zahlungsinstrumente; Verweigerung des Zugangs zum Zahlungskonto“ und zu „Ausführung von Zahlungsvorgängen“ beginnt mit § 675u BGB das Unterkapitel 3 „Haftung“. Hätte der Gesetzgeber eine unbedingte Haftung des Zahlungsdienstleisters auch dann festlegen wollen, wenn nur der bloße lesende Zugang keine starke Kundenauthentifizierung erfordert, wäre angesichts dieses systematischen Zusammenhangs eine ausdrückliche Klarstellung zu erwarten gewesen. Gleiches gilt für den systematischen Zusammenhang des § 675v Abs. 4 Satz 1 BGB mit den übrigen Absätzen, die sich jeweils ausschließlich mit der Haftung im Falle nicht autorisierter Zahlungsvorgänge befassen. Die hier zugängliche Literatur einschließlich der klägerseits insbesondere in der Replik vom 20.03.2023 zitierten Kommentare und Handbücher lässt diese Frage – entgegen der Auslegung der Klagepartei – unentschieden. Zwar wird in Übereinstimmung mit dem Gesetzestext stets das Erfordernis einer starken Kundenauthentifizierung betont, ohne aber zwischen einer solchen beim einzelnen Zahlungsvorgang und beim bloßen Einloggen ins Online-Banking zu unterscheiden. Einzig Maihold (Ellenberger/Bunte, Bankrechts-Handbuch, 6. Auflage 2022, Rdnr. 386 zu § 33) spricht, in Übereinstimmung mit der hier vertretenen Rechtsansicht, ausdrücklich von einer starken Kundenauthentifizierung lediglich für den einzelnen Zahlungsvorgang (zu den klägerseits hieraus gezogenen Folgerungen betreffend die starke Kundenauthentifizierung für den einzelnen Zahlungsvorgang sogleich).

33
(bb) Das beklagtenseits zur Verfügung gestellte Push-TAN-Verfahren stellte eine starke Kundenauthentifizierung im Sinne von § 675 Abs. 4 Satz 1 Nr. 1 BGB dar. Soweit die Klägerin hiergegen eingewandt hat, das Push-TAN-Verfahren sei dann nicht unabhängig von den weiteren Authentifizierungselementen, wenn es auf dem Smartphone betrieben werde, auf dem sich der Zahlungsdienstenutzer in das Online-Banking einlogge, dringt sie damit nicht durch. Denn die Klägerin hat nicht substantiiert bestritten, dass die Push-TAN-App, wie durch die Beklagte unter Verweis auf ein Sachverständigengutachten vorgetragen, auf dem Mobiltelefon in einer eigens dafür vorgehaltenen geschützten Umgebung betrieben wird, die von dem übrigen Betriebssystem des Mobiltelefons so abgeschottet ist, dass eine Kompromittierung technisch nicht möglich ist. Mithin war diese Tatsache als unstreitig zu behandeln.

34
Die von Maihold (aaO) hiergegen geäußerten Bedenken teilt die Kammer nicht. Die Unabhängigkeit der Elemente voneinander wird vorliegend nicht allein durch die verschlüsselte Übertragung, sondern durch die vollkommene Abschottung der Push-TAN-App mittels eines Promon-Shields hergestellt und geht mithin über die dort zugrunde gelegten technischen Vorkehrungen deutlich hinaus. Die Gefahr eines unbefugten Zugriffs auf das Mobiltelefon als Besitzelement selbst stellt die Unabhängigkeit vom Wissenselement der Zugangsdaten zum Online-Banking nicht in Frage.

35
Gleiches gilt, soweit die streitgegenständlichen abgehenden Zahlungen mittels des Zahlungsdienstes Apple-Pay ausgelöst wurden. Die Klägerin hat insoweit nicht bestritten, dass Zahlungen mittels Apple-Pay durch ein Besitzelement, nämlich das Mobiltelefon, auf dem der Dienst installiert ist, und ein Wissens- oder Inhärenzelement, nämlich Face-ID, Touch-ID oder einen Code freizugeben sind, und hat lediglich bestritten, selbst eine entsprechende Autorisierung der streitgegenständlichen, durch Apple-Pay ausgelösten Zahlungen vorgenommen zu haben. Auch insoweit wird mithin eine starke Kundenauthentifizierung verlangt.

36

(cc) Schließlich kann sich die Beklagte auch dann auf die grobe Fahrlässigkeit der Klägerin berufen, wenn der Vortrag der Klägerin in einem nicht nachgelassenen Schriftsatz vom 25.05.2023, der gemäß § 296a ZPO nach Schluss der mündlichen Verhandlung eingegangen und damit nicht mehr berücksichtigungsfähig ist, für die Entscheidung heranzuziehen wäre. Denn der klägerseits geltend gemachte Schaden resultierte nicht aus den dort geschilderten, angabegemäß ohne starke Kundenauthentifizierung durchgeführten Transaktionen vom Tagesgeldkonto der Klägerin auf deren Girokonto, sondern aus den auf verschiedene Weise von ihrem Girokonto abgehenden Zahlungen.

37
(2) Die Klägerin hat gegen die Beklagte keinen Anspruch auf Schadensersatz gemäß §§ 823 Abs. 2 BGB, 55 Abs. 1, 1 Abs. 24 ZAG. Es kann dahinstehen, ob die Beklagte durch die klägerseits dargelegten Verstöße gegen aufsichtsrechtliche Vorgaben, die starke Kundenauthentifizierung betreffend, dem Grunde nach gegenüber der Klägerin schadensersatzpflichtig geworden ist. Ein Schadensersatzanspruch würde nämlich auch dann aufgrund des Mitverschuldens der Klägerin, § 254 Abs. 1 BGB, entfallen. Dieses überwiegt bei einer Abwägung mit den klägerseits behaupteten Verursachungsbeiträgen der Beklagten, deren Vorliegen unterstellt, in derart hohem Maß, dass eine Schadensersatzpflicht der Beklagten im Ergebnis nicht besteht (vgl. Grüneberg/Grüneberg, Bürgerliches Gesetzbuch, 82. Auflage 2023, Rdnr. 64 zu § 254 BGB mit weiteren Nachweisen). Auf die Ausführungen unter (1) (a) wird umfassend Bezug genommen.

38
(3) Die Nebenforderungen teilen das Schicksal der Hauptforderung.

39
Über den Hilfsantrag ist nicht zu entscheiden, da das Gericht den Hauptantrag nicht als unzulässig, sondern als unbegründet ansieht.

40
Die Kostenentscheidung folgt aus § 91 ZPO, die Entscheidung zur vorläufigen Vollstreckbarkeit aus § 709 Satz 2 ZPO.