OLG München, Hinweisbeschluss v. 04.09.2023 – 19 U 1508/23 e

Titel:

Wechselseitige Ansprüche aus einem Zahlungsdiensterahmenvertrag

Normenketten:

BGB § 254, § 398, § 675l Abs. 1 S. 1, § 675u S. 2, § 675v Abs. 3
ZAG § 1 Abs. 25

Leitsätze:

1. Rechtsfolge von § 675u S. 2 BGB ist ein Erstattungsanspruch. „Erstattung" ist dabei der Oberbegriff für die Auszahlung und die Stornobuchung, d.h. die Wertstellung in Höhe der nicht autorisierten Zahlung. Der Anspruch ist in der Regel auf Wertstellung in Höhe der nicht autorisierten Zahlung gerichtet. Eine Auszahlung ist geboten, wenn der Nutzer beim Dienstleister kein Zahlungskonto unterhält, insbesondere falls die Kontobeziehung zwischenzeitlich aufgelöst wurde. (Rn. 36 – 41) (redaktioneller Leitsatz)
2. Die zentrale Funktion des personalisierten Sicherheitsmerkmals besteht darin, den Zahlungsdienstnutzer zu authentifizieren und damit als über das Zahlungsinstrument berechtigt Verfügenden auszuweisen. (Rn. 55) (redaktioneller Leitsatz)
3. Ein grob fahrlässiger Verstoß gegen die Pflicht, personalisierte Sicherheitsmerkmale nicht an Dritte weiterzugeben, liegt vor, falls sich der Zahlungsdienstnutzer beharrlich allen Hinweisen darauf verschließt, dass er nicht mit seinem Zahlungsdienstleister, sondern einem Dritten kommuniziert. (Rn. 65) (redaktioneller Leitsatz)

Schlagworte:

Zahlungsdiensterahmenvertrag, Online-Banking, TAN, PIN, Erstattungsanspruch, personalisierte Sicherheitsmerkmale, SecureGo-Verfahren, Zahlungsdienstleister, Mitverschulden

Vorinstanz:

LG Landshut, Endurteil vom 02.03.2023 – 24 O 2842/22

Fundstellen:

BKR 2023, 839
MMR 2024, 587
LSK 2023, 28101
BeckRS 2023, 28101

Tenor

I. Der Senat weist nach § 522 Abs. 2 S. 2 ZPO darauf hin, dass er beabsichtigt, die Berufung des Klägers zu 1) gegen das Endurteil des Landgerichts Landshut vom 02.03.2023, Az. 24 O 2842/22, gemäß § 522 Abs. 2 S. 1 ZPO zurückzuweisen.

II. Hierzu besteht Gelegenheit zur Stellungnahme binnen drei Wochen nach Zustellung dieses Beschlusses.

Entscheidungsgründe

I.

1
Die Parteien streiten um wechselseitige Ansprüche aus einem zwischen ihnen bestehenden Zahlungsdiensterahmenvertrag.

2
Der Kläger zu 1) ist auch Vorstandsmitglied des – am Berufungsverfahrens nicht mehr beteiligten – Klägers zu 2), eines eingetragenen Vereins.

3
Die Beklagte ist ein in der Rechtsform einer Genossenschaft organisiertes Kreditinstitut.

4
Der Kläger zu 1) unterhielt bei der Beklagten ein Girokonto mit der Kontonummer …. Außerdem war der Kläger zu 1) in seiner Funktion als Vorstandsmitglied des Klägers zu 2) auch verfügungsberechtigt über dessen Girokonto mit der Kontonummer … bei der Beklagten. Beide Konten verfügten über einen gemeinsamen Online-Banking-Zugang, der vom Kläger zu 1) seit vielen Jahren, jedenfalls seit 2004/2005, genutzt wurde.

5
Mittlerweile wurde das Konto des Klägers zu 1) mit der Kontonummer … aufgelöst.

6
In der jeweiligen „Vereinbarung über die Nutzung des Online-Banking – PIN-/TAN-Verfahren; Telefon“ zwischen den Klägern und der Beklagten (Anlagen B 1, B 2) ist gemäß Ziffer 4 unter anderem vereinbart:

„Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten.“

7
In den „Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ der Beklagten (ebenfalls Anlage B 1) ist unter Ziffer 7 Abs. 1 neben anderem bestimmt:

„Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und der TAN erlangt. Jede Person, die die PIN und – falls erforderlich – die TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z.B. Aufträge zulasten des Kontos/Depots erteilen.“

8
In den „Sonderbedingungen für das Online-Banking“ der Beklagten (Anlage B 3) ist unter Ziffer 7.1 Abs. 1 geregelt:

„Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (…).“

9
Nach Ziffer 2 Abs. 3 der „Sonderbedingungen für das Online-Banking“ sind „Authentifizierungselemente“ unter anderem „Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer [PIN] oder der Nutzungscode für die elektronische Signatur“.

10
In Ziffer 7.1 Abs. 2 lit. a ist vereinbart:

„Wissenselemente, wie z.B. die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,

(…)“

11
In Ziffer 10.2.1 Abs. 3 der „Sonderbedingungen für das Online-Banking“ ist bestimmt:

„Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer (…) seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen (…) grob fahrlässig verletzt, trägt der Kunde (…) den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er einer seiner Sorgfaltspflichten nach

- Nummer 7.1 Abs. 2

(…) dieser Bedingungen verletzt hat.“

12
Ziffer 7.2 regelt zudem:

„Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.“

13
Die Beklagte warnte auf ihrer Website (s. Anlage B 4) im Jahr 2021 mehrfach – jedenfalls zwischen dem 20.01.2021 und dem 23.07.2021 viermal – davor, dass es zu Telefonanrufen angeblicher Bankmitarbeiter komme, bei denen die Kunden dazu aufgefordert werden, Zugangsdaten und personenbezogene Informationen telefonisch preiszugeben.

14
Am 31.08.2021 wurde unter Angabe des richtigen VR-Netkey – eine personenbezogene Kennung für das Online-Banking bei Volksbanken und Raiffeisenbanken in Deutschland – sowie der korrekten Onlinebanking-Zugangs-PIN der Kläger durch unbekannte Dritte, welche an diese Informationen unstreitig dadurch gelangten, dass sie den Computer des Klägers zu 1) hackten, in betrügerischer Absicht für dessen Onlinebanking die Freischaltung des SecureGo-Verfahrens bei der Beklagten beantragt. Dabei handelt es sich um ein Verfahren, um Transaktionsnummern (TAN), mithin Einmalkennworte für Online-Banking-Transaktionen, direkt in der App der Beklagten auf einem mobilen Endgerät (z.B. einem Smartphone oder Tablet) zu erhalten. Die Freischaltung ist gerätebunden, d.h. für die Freischaltung der SecureGo-App auf jedem mobilen Endgerät ist jeweils ein separater Freischaltcode erforderlich.

15
Seit November 2020 hatte der Kläger zu 1) aber bereits eine Freischaltung für das SecureGo-Verfahren und nutzte dieses vielfach zur TAN-Generierung.

16
Daraufhin erhielt der Kläger zu 1) ein von der Beklagten stammendes – nicht mehr vorhandenes – Schreiben vom 01.09.2021 (s. Anlage B 5), das inhaltlich im Kern mit der Anlage K 1 vergleichbar ist. Mit diesem erhielt sie in einem separaten Sicherheitsumschlag zum Aufreißen – in Form eines zweidimensionalen QR-Codes und eines alphanumerischen Codes – den Freischaltcode zur Nutzung des aktualisierten SecureGo-Verfahrens. In dem Schreiben ist angegeben, dass zur Freischaltung des SecureGo-Verfahrens die SecureGo-App auf einem mobilen Endgerät zu öffnen sei. Dann sei der QR-Code in der SecureGo-App einzuscannen oder der alphanumerische Code per Hand einzugeben. Danach könne die SecureGo-App für die Durchführung TAN-pflichtiger Transaktionen im Online-Banking verwendet werden.

17
In den beigelegten „Informationen zum SecureGo-Verfahren“ wurde nochmals klargestellt:

„Die SecureGo-App ist an einen VR-NetKey gebunden und kann nur auf einem Gerät installiert werden.“

18
Dem Kläger zu 1) war bewusst, dass er die Zusendung eines erneuten Freischaltcodes nicht beantragt hatte.

19
Im Jahr 2021 proklamierten die Volks- und Raiffeisenbanken die Umstellung des bisherigen SecureGo- auf das aktualisierte SecureGo plus-System mit angeblich höheres Sicherheitsniveau.

20
Am 03.09.2021 erhielt der Kläger zu 1) einen Anruf eines Unbekannten unter der anzeigten Rufnummer „…“ (s. Anlage K 2). Der Anrufer gab sich als Mitarbeiter der Beklagten aus und teilte mit, dass das Aktualisierungsverfahren bald ausgeführt werden müsse. Da der Kläger zu 1) an diesem Tage jedoch keine Zeit hatte, vereinbarte man einen Rückruf eine Woche später. Eine der Stammnummer der Beklagten „…“ nachfolgende Durchwahl „…“ existiert bei ihr nicht.

21
Am 10.09.2021 erfolgte der vereinbarte Rückruf durch den vermeintlichen Mitarbeiter der Beklagten (s. Anlage K 3). Der Kläger zu 1) befolgte die Anweisungen des Anrufers und teilte telefonisch den per Brief erhaltenen Freischaltcode mit. Der Kläger kam der Aufforderung zur Mitteilung des Freischaltcodes nach, da er der Meinung war, dass die Weitergabe des Freischaltcodes zum Zwecke der Aktualisierung des SecureGo-Verfahrens erforderlich sei.

22

Unstreitig telefonierte der Kläger zu 1) zwar in der Vergangenheit mit Mitarbeitern der Beklagten, wurde von diesen aber nie nach Codes oder Authentifizierungselementen gefragt.

23
Durch Eingabe des Freischaltcodes in die SecureGo-App waren die unbekannten Täter, welche bereits über den VR-Netkey und die Onlinebanking-Zugangs-PIN der Kläger verfügten, nun in der Lage, ein eigenes mobiles Endgerät zwecks Nutzung des SecureGo-Verfahrens freizuschalten und in der Folge TAN für Transaktionen bezüglich der Konten der Kläger zu erzeugen.

24
Daraufhin überwiesen die unbekannten Täter

- am 14.09.2021 einen Betrag von 1.683,97 € vom Konto des Klägers zu 1) und

- am 15.09.2021 einen Betrag von 12.300 € vom Konto des Klägers zu 2)

auf andere Konten weiter.

25
Nachdem der Kläger zu 1) am 16.09.2021 bei der Beklagten monierte, dass die streitgegenständlichen Abbuchungen nicht von ihm autorisiert worden seien, veranlasste die Beklagte sofort die Sperrung der Konten der Kläger. Auch wurden unverzüglich Überweisungsrückrufe veranlasst, die allerdings nicht zu Rückzahlungen führten.

26
Nachfolgende strafrechtliche Ermittlungen der Staatsanwaltschaft … verliefen erfolglos (s. Anlage K 4).

27
Beide Kläger begehrten erstinstanzlich von der Beklagten die Zahlung dieser Beträge, da die Kontoverfügungen von ihnen nicht autorisiert worden seien. Beim Freischaltcode für das Secure-Go-Verfahren handele es sich nicht um ein personalisiertes Sicherheitsmerkmal, so dass bereits deswegen dessen Weitergabe durch den Kläger zu 1) an die unbekannten Täter auch keine Gegenansprüche der Beklagten wegen eines Sorgfaltspflichtverstoßes begründen könne.

28
Die Beklagte rechnete mit Schadensersatzansprüchen nach § 675 v Abs. 3 Nr. 2 lit. a), b) BGB je in Höhe der Klageforderungen gegen die jeweiligen Ansprüche der Kläger auf. Die Kläger hätten den unbekannten Tätern grob fahrlässig und pflichtwidrig den Zugriff auf ihre Konten ermöglicht und es zugelassen, dass diese TAN generieren konnten, die zur Autorisierung von Überweisungen mittels Online-Banking erforderlich waren. Die Beklagte sei dafür nicht verantwortlich. Der Freischaltcode für das SecureGo-Verfahren sei ein personalisiertes Sicherheitsmerkmal und habe Dritten nicht offenbart werden dürfen.

29
Das Landgericht hat die Klage mit dem angefochtenen Urteil vom 02.03.2022 (Bl. 65 ff. d. LG-eAkte), auf dessen tatsächliche Feststellungen (§ 522 Abs. 2 S. 4 ZPO) und Entscheidungsgründe Bezug genommen wird, abgewiesen. Die auf Zahlung gerichteten Klageanträge gingen ins Leere, da die Kläger weiterhin über ihre Konten bei der Beklagten verfügten. Daher könnten sie allenfalls die Gutschrift der begehrten Beträge verlangen. Dessen ungeachtet seien die streitgegenständlichen Zahlungsvorgänge zwar nicht autorisiert gewesen. Jedoch habe die Beklagte die von ihr geltend gemachten Gegenansprüche auf Schadensersatz in gleicher Höhe gegen die Kläger, mit welchen sie wirksam aufgerechnet habe.

30
Dagegen richtet sich die mit Schriftsatz vom 31.03.2023 (Bl. 1 f. d. OLG-eAkte) eingelegte und mit Schriftsatz vom 29.06.2023 (Bl. 11 ff. d. OLG-eAkte) begründete Berufung des Klägers zu 1). Er beantragt, das Urteil des Landgerichts abzuändern und zu erkennen wie folgt:

1. Die Beklagte wird verurteilt, dem Kläger zu 1) einen Betrag in Höhe von 1.683,97 € nebst Zinsen hieraus i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 11.12.2021 zu bezahlen.

2. Die Beklagte wird verurteilt, an den Kläger zu 1) außergerichtliche Rechtsverfolgungskosten in Höhe von 280,60 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 08.02.2022 zu bezahlen.

31
Die Beklagte beantragt,

die Berufung zurückzuweisen.

32
Wegen der Einzelheiten des Parteivortrages wird auf die Berufungsbegründung vom 29.06.2023 (Bl. 11 ff. d. OLG-eAkte), die Berufungserwiderung vom 21.08.2023 (Bl. 18 ff. d. OLG-eAkte) sowie die weiteren Schriftsätze der Parteien verwiesen.

II.

33
Der Senat ist einstimmig der Auffassung, dass die Berufung offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache auch keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist.

34
Die angefochtene Entscheidung des Landgerichts ist richtig. Dessen Urteil beruht nicht auf einer Rechtsverletzung (§§ 513 Abs. 1, 546 ZPO). Vielmehr rechtfertigen die Tatsachen, die der Senat im Rahmen des durch § 529 ZPO festgelegten Prüfungsumfangs der Beurteilung des Streitstoffes zugrunde zu legen hat, keine andere Entscheidung. Die Ausführungen der Klagepartei in der Berufungsinstanz vermögen dem Rechtsmittel nicht zum Erfolg zu verhelfen, da sie das Ersturteil, auf das Bezug genommen wird, nicht erschüttern.

35
1. Der Kläger zu 1) hat keinen Anspruch aus §§ 675 u S. 2, 675 f BGB auf Erstattung von 1.683,97 € gegenüber der Beklagten.

36
a) Ein derartiger Anspruch des Klägers zu 1) ist zwar zunächst entstanden.

§ 675 u S. 2 BGB begründet, in Verbindung mit dem zwischen den Parteien unstreitig bestehenden Kontovertrag i.S. eines Zahlungsdiensterahmenvertrages (§ 675 f Abs. 2 BGB), vorliegend einen Anspruch des Klägers zu 1) auf Auszahlung des Betrages, mit dem sein Konto zu Unrecht belastet worden ist.

37
aa) Als Rechtsfolge gewährt § 675 u S. 2 BGB einen Erstattungsanspruch. „Erstattung“ ist der Oberbegriff für die Auszahlung und die Stornobuchung, d.h. die Wertstellung in Höhe der nicht autorisierten Zahlung.

38
Der Anspruch ist in der Regel auf Wertstellung in Höhe der nicht autorisierten Zahlung gerichtet (Schulte-Nölke in: Schulze, BGB, 11. Aufl., § 675 u Rz. 2).

39
Auszahlung ist geboten, wenn der Nutzer beim Dienstleister kein Zahlungskonto unterhält (Zetzsche in: Münchener Kommentar zum BGB, 9. Aufl., § 675 u Rz. 19), insbesondere falls die Kontobeziehung zwischenzeitlich aufgelöst wurde (OLG Celle, Beschluss v. 17.11.2020, Az. 3 U 122/20, juris Rz. 19; OLG Frankfurt a.M., Urteil v. 11.05.2017, Az. 1 U 224/15, juris Rz. 14; LG Darmstadt, Urteil v. 28.08.2014, Az. 28 O 36/14, juris Rz. 26; Zimmermann in: beck-online.GROSSKOMMENTAR, Stand: 01.06.2023, § 675u BGB Rz. 25; Schmalenbach in: BeckOK BGB, 67. Ed., Stand: 01.08.2023, § 675u Rz. 5; Sprau in: Grüneberg, BGB, 82. Aufl., § 675u Rz. 5).

40
Damit war die Ansicht des Landgerichts, die geltend gemachten Zahlungsansprüche bestünden schon nicht, weil der Anspruch aus § 675u S. 2 BGB grundsätzlich nicht auf Zahlung, sondern auf Gutschrift des

belasteten Betrages gerichtet sei, zum Zeitpunkt des Schlusses der mündlichen Verhandlung erster Instanz rechtsfehlerfrei.

41
Mittlerweile wurde das verfahrensgegenständliche Konto des Klägers zu 1) bei der Beklagten aber unstreitig aufgelöst. Somit kann der Kläger jetzt nicht mehr die zunächst richtigerweise geschuldete Stornobuchung, sondern nur noch – wie von ihm beantragt – die Auszahlung des streitigen Betrages verlangen.

42
bb) Unstreitig kam es zu einer Überweisung von 1.683,97 € vom Konto des Klägers zu 1) bei der Beklagten auf ein von den unbekannten Täter hierfür genutztes Konto.

43
cc) Die streitgegenständliche Überweisung vom Konto des Klägers zu 1) war von diesem nicht autorisiert.

44
aaa) Nach der Legaldefinition des § 675j Abs. 1 S. 1 BGB ist die Autorisierung die wirksame Zustimmung des Zahlers zum Zahlungsvorgang, welche nach § 675j Abs. 1 S. 2 BGB als Einwilligung oder, sofern zwischen dem Zahler und seinem Zahlungsdienstleister zuvor vereinbart, auch als Genehmigung erteilt werden kann.

45
bbb) Selbst eine Stellvertretung insoweit ist grundsätzlich möglich (Jungmann in: Münchener Kommentar zum BGB, 9. Aufl., § 675 j Rz. 148; Berger in: Jauernig, BGB, 18. Aufl., § 675 j Rz. 1; differenzierend Köndgen in: beck-online.GROSSKOMMENTAR, Stand: 01.03.2023, § 675 j BGB Rz. 17 ff.; Schmalenbach in: BeckOK BGB, 67. Ed., Stand: 01.08.2023, § 675 j Rz. 3).

46
Die vereinzelt vertretene Ansicht, dass in Fällen, in denen der Nutzer seine Zugangsdaten leichtfertig an Dritte weitergibt und somit eine manipulierte Autorisierung im Onlinebanking ermöglicht, das Einverständnis des Nutzers zu den durch den Angreifer sodann durchgeführten Zahlungsvorgängen nach den Grundsätzen der Rechtscheinsvollmacht zuzurechnen sei (z.B. LG Darmstadt, Urteil v. 28.08.2014, Az. 28 O 36/14, juris Rz. 37 ff.), ist abzulehnen. Die Grundsätze über die Duldungs- und Anscheinsvollmacht finden in Bezug auf die Zustimmung i.S.v. § 675 j BGB richtigerweise keine Anwendung (BGH, Urteil v. 26.01.2016, Az. XI ZR 91/14, Rz. 55 ff.; Urteil v. 16.06.2015, Az. XI ZR 243/13, Rz. 22 ff.; OLG Dresden, Urteil v. 06.04.2023, Az. 8 U 578/22, juris Rz. 73; Köndgen in: beck-online.GROSSKOMMENTAR, Stand: 01.03.2023, § 675 j BGB Rz. 20; Schulte-Nölke in: Schulze, BGB, 11. Aufl., § 675 j Rz. 2; Köbrich, VuR 2015, 9 [12 f.]).

47
ccc) Der Kläger zu 1) trägt vor, dass er die streitgegenständliche Überweisung nicht veranlasste, sondern unbekannte Dritte ohne sein Wissen und Wollen. Dies wird von der Beklagten nicht hinreichend bestritten, so dass es auf die Frage der Darlegungs- und Beweislast für die (Nicht-)Autorisierung der Überweisungen – welche im Übrigen gemäß § 675 w S. 1 BGB bei der Beklagten läge – vorliegend nicht ankommt.

48
b) Der Anspruch des Klägers zu 1) nach § 675 u S. 2 BGB ist aber – was das Landgericht richtigerweise bejaht hat – durch wirksame Aufrechnung der Beklagten wieder erloschen, § 389 BGB.

aa) Die Beklagte hat bereits in der Klageerwiderung vom 12.12.2022 (S. 15 = Bl. 39 ff. d. LG-eAkte) die Aufrechnung erklärt, § 388 BGB.

bb) Die Beklagte hat nach § 675 v Abs. 3 Nr. 2 lit. a), b) BGB einen Gegenanspruch auf Schadensersatz gegen den Kläger zu 1) in Höhe dessen Erstattungsanspruchs gemäß § 675 u S. 2 BGB.

49
aaa) Der Kläger zu 1) hat grob fahrlässig Pflichten gemäß § 675 l Abs. 1 S. 1 BGB verletzt, § 675 v Abs. 3 Nr. 2 lit. a) BGB

50

a) Nach § 675 l Abs. 1 S. 1 BGB ist der Zahler verpflichtet, unmittelbar nach Erhalt eines Zahlungsauthentifizierungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

51
Die vom Zahlungsdienstnutzer danach geschuldeten Sicherheitsmaßnahmen beziehen sich auf die Geheimhaltung der personalisierten Sicherheitsmerkmale (v. Westphalen in: Erman, BGB, 17. Aufl., § 675 l BGB Rz. 3). Die Pflicht dient der Minimierung der Gefahr nicht autorisierter Nutzung bzw. missbräuchlicher Verwendung von Zahlungsinstrumenten und somit in der Schadensprävention (Jungmann in: Münchener Kommentar zum BGB, 9. Aufl., § 675 l Rz. 7).

52
aa) Beim Freischaltcode für das SecureGo-Verfahren handelt es sich – entgegen Klageansicht – um ein personalisiertes Sicherheitsmerkmal in diesem Sinne.

53
Personalisierte Sicherheitsmerkmale sind gemäß § 1 Abs. 25 ZAG personalisierte Merkmale, die der Zahlungsdienstleister einem Zahlungsdienstnutzer zum Zwecke der Authentifizierung bereitstellt.

54
Darunter sind Datenschlüssel, Zeichenabfolgen oder Codewörter zu fassen, die dem Zahlungsdienstnutzer durch den Zahlungsdienstleister exklusiv zur Kenntnis gebracht werden, sodass das Innehaben dieser Informationen gegenüber dem Zahlungsdienstleister oder anderen Zahlungsinstituten die Berechtigung indiziert (Jungmann in: Münchener Kommentar zum BGB, 9. Aufl., § 675 j Rz. 70; Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l BGB Rz. 36.1; Casper/Terlau, ZAG, 3. Aufl., § 1 Rz. 529; Scheibengruber, BKR 2010, 15 [17]; ähnlich Köndgen in: beck-online.GROSSKOMMENTAR, Stand: 01.03.2023, § 675 j BGB Rz. 70).

55
Zentrale Funktion des personalisierten Sicherheitsmerkmals darin besteht, den Zahlungsdienstnutzer zu authentifizieren und damit als über das Zahlungsinstrument berechtigt Verfügenden auszuweisen (vgl. BT-Drs. 16/11643, S. 106; s. auch Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l BGB Rz. 36; Schmalenbach in: BeckOK BGB, 67. Ed., Stand: 01.08.2023, § 675 l Rz. 3; Schwintowski in: jurisPK-BGB, 10. Aufl., Stand: 03.05.2023, § 675 l Rz. 5).

56
Offen für Dritte ersichtliche Daten sind nicht darunter zu fassen (Omlor in: Staudinger, BGB, Neubearb. 2020, Updatestand: 15.03.2023, § 675 l Rz. 4).

57
Folglich sind darunter zweifelsohne TAN zu verstehen, welche einmal für die Autorisierung einer ganz bestimmten Transaktion eingesetzt werden können, dem Zahlungsdienstnutzer erst im Zusammenhang mit der jeweiligen Transaktion übermittelt werden und nur für eine kurze Zeit gültig sind (vgl. BT-Drs. 16/11643, S. 106; s. auch BGH, Urteil v. 25.7.2017, Az. XI ZR 260/15, Rz. 29; Sprau in: Grüneberg, 82. Aufl., § 675 j Rz. 7; Berger in: Jauernig, BGB, 18. Aufl., §§ 675 k-675 m, Rz. 2; Hofmann, BKR 2014, 105 [107]; Scheibengruber, BKR 2010, 15 [17]; Casper/Terlau, ZAG, 3. Aufl., § 1 Rz. 438).

58
Richtigerweise ist darunter – gleichsam als „Vorstufe“ – aber auch der Freischaltcode für das SecureGo-Verfahren zu fassen (s. bereits Senatsbeschluss v. 22.09.2022, Az. 19 U 2204/22, juris Rz. 86; zustimmend Schmalenbach in: BeckOK BGB, 67. Ed., Stand: 01.08.2023, § 675 l Rz. 3), gleich ob in Form des zweidimensionalen QR-Codes und des alphanumerischen Codes. Er wurde postalisch in einem separaten Sicherheitsumschlag zur ausschließlichen Kenntnis des Klägers zu 1) an diesen übersandt. Er ermöglicht mit seiner Eingabe in die SecureGo-App die Legitimation gegenüber der Beklagten, die Freischaltung der App auf einem mobilen Endgerät und in der Folge die Erzeugung und Erlangung von TAN.

59
Wenn der Kläger zu 1) einwendet, ein rechtsrelevanter Unterschied zwischen Freischaltcode und TAN sei, dass ersterer einmalig verwendet würden, letztere dafür regelmäßig, verkennt er die technischen Gegebenheiten. Selbstredend werden TAN ebenfalls nur für eine einzige Transaktion vergeben, nicht zum

dauerhaften Gebrauch wie beispielsweise ein PIN. Außerdem würde dieser Umstand für die rechtliche Einordnung als personalisiertes Sicherheitsmerkmal keinen Unterschied machen (vgl. hierzu Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l Rz. 36), denn auch eine PIN ist als solches einzustufen (so z.B. BGH, Urteil v. 25.7.2017, Az. XI ZR 260/15, Rz. 29).

60
Dass die Weitergabe des Freischaltcodes für den Kläger zu 1) gegebenenfalls mit einer Aktualisierung oder einem Update des SecureGo-Verfahrens verbunden gewesen sei, ändert an dieser Einschätzung entgegen Klageauffassung ebenso nichts.

61
ββ) Unbefugt ist namentlich jede Verwendung, die ohne oder gegen den Willen des Inhabers des Zahlungsinstruments erfolgt und dementsprechend auf die Auslösung eines nicht autorisierten Zahlungsvorgangs gerichtet ist (Jungmann in: Münchener Kommentar zum BGB, 9. Aufl., § 675 l Rz. 23; Herresthal in: Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., § 675 l BGB Rz. 4).

62
Der Kläger hatte allgemein dafür Sorge zu tragen, dass nicht dritte Personen die unkontrollierte Zugriffsmöglichkeit auf sein Online-Bankung oder die Banking-App mittels Zugangsdaten und TAN bekommen und so ohne sein Wissen und Wollen eine Transaktion von seinem Konto bei der Beklagten durchführen können (generell zum Sorgfaltsmaßstab beim Online-Banking und beim Mobile Banking ausführlich: Jungmann in: Münchener Kommentar zum BGB, 9. Aufl., § 675 l Rz. 49 ff.; s. auch Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l Rz. 85 ff.).

63
Die vom Zahlungsdienstnutzer geschuldeten Sorgfaltspflichten sind außerdem nach der Art des konkreten Angriffs zu bestimmen (Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l BGB Rz. 96).

64
Wenn sich jedem Zahlungsdienstnutzer in der entsprechenden Situation sowie dem betroffenen Zahlungsdienstnutzer ganz individuell geradezu aufdrängen musste, dass es sich nicht um einen regulären Vorgang handeln kann, ist von grober Fahrlässigkeit auszugehen (Hofmann in: beck-online.GROSSKOMMENTAR, Stand: 01.09.2022, § 675 l BGB Rz. 96).

65
Ein grob fahrlässiger Verstoß gegen die Pflicht, personalisierte Sicherheitsmerkmale nicht an Dritte weiterzugeben, liegt jedenfalls dann vor, falls sich der Zahlungsdienstnutzer beharrlich allen Hinweisen darauf verschließt, dass er nicht mit seinem Zahlungsdienstleister, sondern einem Dritten kommuniziert (Senatsbeschluss v. 22.09.2022, Az. 19 U 2204/22, juris Rz. 95; zustimmend Schwintowski in: jurisPK-BGB, 10. Aufl., Stand: 03.05.2023, § 675 l Rz. 19.1, § 675 v Rz. 37.1; s. auch LG Köln, Urteil v. 10.09.2019, Az. 21 O 116/19, juris Rz. 22 ff.).

66
β) Gegen die Pflicht nach § 675 l Abs. 1 S. 1 BGB, personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen, hat der Kläger zu 1) vorliegend grob fahrlässig verstoßen.

67
αα) Grob fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt in besonders schwerem Maße verletzt, einfachste und nahe liegende Überlegungen nicht anstellt und in der konkreten Situation das nicht beachtet, was sich jedem aufdrängt (stRspr., z.B. BGH, Urteil v. 13.12.2004, Az. II ZR 17/03; Urteil v. 17.10.2000, Az. XI ZR 42/00 [NJW 2001, 286]; Urteil v. 29.09.1992, Az. XI ZR 265/91 [NJW 1992, 3235]; Urteil v. 05.12.1983, Az. II ZR 252/82 [NJW 1984, 789]; Urteil v. 11.05.1953, Az. IV ZR 170/52 [NJW 1953, 1139]).

68
Dabei bestimmt sich die im Verkehr erforderliche Sorgfalt daran, was von einem durchschnittlichen Angehörigen der jeweiligen Verkehrskreise in der jeweiligen Situation erwartet werden kann, also vorliegend die Sorgfalt eines durchschnittlichen Verwenders von Onlinebanking, bei dem unterstellt werden kann, dass er über einigermaßen gesicherte Grundkenntnisse der Funktionsweise des Internets einschließlich des E-

Mail-Verkehrs verfügt und die Berichterstattung über Onlinebanking in groben Zügen verfolgt (Häuser in: Münchener Kommentar zum HGB, 4. Aufl., Bd. 6, Teil 1, Kap. B, Rz. 355; LG Essen, Urteil v. 04.12.2014, Az. 6 O 339/14, juris Rz. 22).

69
Im Rahmen der missbräuchlichen Nutzung von TAN durch Dritte im Rahmen des Onlinebankings besteht indes kein Anscheinsbeweis für eine grobe Fahrlässigkeit des Kontoinhabers (BGH, Urteil v. 26.01.2016, Az. XI ZR 91/14, Rz. 70 ff.).

70
ββ) Unter Berücksichtigung aller Umstände des hiesigen Einzelfalls ist das Verhalten des Klägers zu 1) als grob fahrlässig einzustufen, indem er einer ihm unbekannten Person am Telefon den Freischaltcode zur Nutzung des aktualisierten SecureGo-Verfahrens weitergab.

71
Dahinstehen kann, ob die Beklagte durch die Warnhinweise auf ihrer Online-Banking-Seite hinreichend vor derartigen Phishing-Attacken gewarnt hat und der Kläger zu 1) gemäß Ziffer 7.2 der „Sonderbedingungen für das Online-Banking“ dazu verpflichtet war, diese regelmäßig einzusehen. Aufgrund der in den letzten Jahren vielfach durch verschiedene Medien bekannt gewordenen Fälle ist die Erkenntnis, dass Kunden durch betrügerische Anrufe vorgeblicher Bankmitarbeiter zur Preisgabe von Zugangsdaten zum Online-Banking veranlasst werden sollen, als allgemeines Wissen vorauszusetzen (s. auch Senatsbeschluss v. 22.09.2022, Az. 19 U 2204/22, juris Rz. 99). Der Wandel im Bewusstsein des allgemeinen Rechtsverkehrs durch die regelmäßigen Berichte über derartige Angriffe in den Medien und der Umstand, dass die Banken mit ihren Kunden nicht in dieser Weise in Kontakt treten, müssen bei der Konkretisierung des Sorgfaltsmaßstabes berücksichtigt werden (Herresthal in: Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., § 675 v BGB Rz. 64). Der Kläger zu 1) musste daher von der Möglichkeit solcher betrügerischen Vorgänge, wenn auch in unterschiedlicher Ausgestaltung, jedenfalls allgemeine Kenntnis haben. Falls nicht, wäre zumindest dies als grob fahrlässige Unkenntnis einzustufen (vgl. auch LG Zweibrücken, Urteil v. 23.01.2023, Az. 2 O 130/22, BeckRS 2023, 2293, Rz. 51). Darüber hinaus – mag der Kläger zu 1) auch technischer Laie in Computerangelegenheiten sein – ist er nach eigenem Vorbringen mit dem Online-Banking vertraut.

72
Bei der Weitergabe von personalisierten Sicherheitsmerkmalen in einem Telefongespräch an einen unbekannten Dritten liegt stets ein Sorgfaltspflichtverstoß vor und der Vorwurf einer groben Fahrlässigkeit regelmäßig nahe (OLG Köln, Urteil v. 20.10.2021, Az. 13 U 18/21, juris Rz. 3; LG Zweibrücken, Urteil v. 23.01.2023, Az. 2 O 130/22, BeckRS 2023, 2293, Rz. 47; LG Saarbrücken, Urteil v. 09.12.2022, Az. 1 O 181/20, juris, Rz. 34; Urteil v. 10.06.2022, Az. 1 O 394/21, juris Rz. 26; LG Frankfurt a.M., Urteil v. 12.04.2022, Az. 2-12 O 202/21, juris Rz. 22 ff.; LG Bonn, Urteil v. 13.01.2021, Az. 2 O 204/20, juris Rz. 18; LG Köln, Urteil v. 10.09.2019, Az. 21 O 116/19, juris Rz. 23 ff.; AG München, Urteil v. 05.01.2017, Az. 132 C 49/15, juris Rz. 36; Häuser in: Münchener Kommentar zum HGB, 4. Aufl., Bd. 6, Teil 1, Kap. B, Rz. 355; Linardatos in: Münchener Kommentar zum HGB, 4. Aufl., Bd. 6, Teil 1, Kap. K, Rz. 213; Schwintowski in: Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 9. Aufl., Stand: 08.09.2022, § 675v Rz. 34.1; Maihold in: Ellenberger/Bunte, Bankrechts-Handbuch, 6. Aufl., § 33 Rz. 298).

73
Dessen ungeachtet muss das Handeln des Klägers zu 1) allerdings auch im Rahmen einer vorzunehmenden Gesamtschau der Umstände des vorliegenden Einzelfalls als grob fahrlässig bewertet werden. Es musste sich ihm geradezu aufdrängen, dass hier (möglicherweise) betrügerische Anrufe vorlagen und er hätte keinesfalls den von der Beklagten übersandten Freischaltcode für das SecureGo-Verfahren ohne Weiteres einem ihm unbekannten Anrufer mitteilen dürfen. Damit wurde leichtfertig den unbekannten Tätern die Möglichkeit zur Generierung einer TAN auf einem mobilen Endgerät eröffnet, um so die streitgegenständliche Überweisung zu Lasten des Klägers zu 1) vorzunehmen.

74
Auch wenn nicht übersehen werden kann, dass die Volks- und Raiffeisenbanken im Jahr 2021 die Umstellung des bisherigen SecureGo- auf das aktualisierte SecureGo plus-System proklamierten, musste es den Kläger zu 1) bereits stutzig machen, dass er einen Brief der Beklagten zur Freischaltung des SecureGo-Verfahrens erhielt, obwohl er dies nicht beantragt hatte und dieses Verfahren seit geraumer Zeit

bereits nutzte. Unstreitig war in diesem Schreiben nicht lediglich von einer Aktualisierung oder einem Update der App die Rede. Eine (erneute) Freischaltung war für ihn unnötig. Umso mehr musste dies seinen Argwohn erregen, als das SecureGo-Verfahren einen neuerlichen Freischaltcode nur für ein weiteres mobiles Endgerät erfordert. Zudem verschloss der Kläger die Augen davor, dass im Schreiben der Beklagten vom 01.09.2021 erläutert wurde, dass zur Freischaltung des SecureGo-Verfahrens die SecureGo-App auf einem mobilen Endgerät zu öffnen und dann der QR-Code in der SecureGo-App einzuscannen oder der alphanumerische Code per Hand einzugeben sei. Der Kläger zu 1) gab selbst an, das Schreiben vor dem ersten betrügerischen Anruf gelesen zu haben. Danach bestand keinerlei Anlass für die Mitwirkung eines Bankmitarbeiters. Auch als ein angeblicher Mitarbeiter der Beklagten ihn am 03.09.2021 anrief und angab, dass das Aktualisierungsverfahren bald ausgeführt werden müsse, sah sich der Kläger zu 1) zu keinerlei Nachfragen bei diesem oder in der Folgezeit bei der Beklagten veranlasst. Schließlich teilte der Kläger zu 1) beim zweiten Anruf des Unbekannten vom 10.09.2021 diesem völlig abweichend von der beschriebenen Vorgehensweise den Freischaltcode telefonisch mit. Dass das Schreiben und der beigelegte Flyer für den Kläger laut eigenem Vorbringen zu diesem Zeitpunkt nicht mehr relevant gewesen seien, entlastet ihn keineswegs, sondern untermauert seinen Sorgfaltspflichtverstoß. Selbst wenn die anzeigte Rufnummer „…“ Anrufe der Beklagten suggerierte, musste dem Kläger auffallen, dass er zwar in der Vergangenheit mehrfach mit Mitarbeitern der Beklagten telefonierte, von diesen aber niemals nach Codes oder Authentifizierungselementen gefragt wurde. Onlinebanking-Nutzern sollte generell bekannt sein, dass echte Bankmitarbeiter sie niemals nach Zugangsdaten fragen, schon gar nicht am Telefon (Zahrte, BKR 2016, 315 [318]). Dazu kommt, dass dieses Vorgehen auch keinerlei Sinnhaftigkeit aufweist. Weshalb sollte die Beklagten dem Kläger zu 1) per Post persönlich in einem separaten verschlossenen Sicherheitsumschlag einen ersichtlich nur zur seiner Kenntnis bestimmten Freischaltcode zusenden, um in dann wiederum von ihm telefonisch zu erfragen.

75
Bei Gesamtbetrachtung sämtlicher Umstände des hiesigen Falles stellt sich das Handeln des Klägers zu 1) somit als objektiv schwerwiegender und subjektiv nicht entschuldbarer Verstoß gegen die Anforderungen der im Verkehr erforderlichen Sorgfalt dar.

76
Der grob fahrlässige Pflichtenverstoß fußt ausschließlich im Verantwortungsbereich des Klägers zu 1) und ist in keiner Weise der Beklagten anzulasten.

77
bbb) Die Kläger haben daneben grob fahrlässig vereinbarte Bedingungen für die Ausgabe und Nutzung des Zahlungsauthentifizierungsinstrument verletzt, § 675v Abs. 3 Nr. 2 lit. b) BGB.

78
α) Gemäß Ziffer 7.1 Abs. 1, Abs. 2 lit. a der unbestritten in das Vertragsverhältnis einbezogenen „Sonderbedingungen für das Online-Banking“ hatte der Kläger seine Authentifizierungsinstrumente vor unbefugtem Zugriff zu schützen, insbesondere Wissenselemente nicht außerhalb des Online-Bankings weiterzugeben. Als solche i.S.v. Ziffer 2 Abs. 3 ist der Freischaltcode zur Nutzung des SecureGo-Verfahrens – sowohl in Form eines QR-Codes als auch alphanumerisch – einzustufen.

79
β) Auch gegen diese vertraglichen Bestimmungen verstieß der Kläger zu 1) grob fahrlässig, indem er den Freischaltcode leichtfertig in dem Telefongespräch vom 10.09.2021 preisgab und so den unbekannten Tätern die Möglichkeit zu Zugriff und Verfügung über sein Konto eröffnete. Insoweit wird auf die vorstehenden Ausführungen Bezug genommen.

80
ccc) Der Anspruch besteht jedenfalls in der Höhe des klageweise geltend gemachte Erstattungsansprüche nach § 675u S. 2 BGB.

81
α) Ein Verstoß im Sinne des § 675v Abs. 3 BGB löst eine der Höhe nach unbeschränkte Haftung des Zahlers gegenüber seinem Zahlungsdienstleister für den gesamten entstandenen Schaden aus; es gelten die allgemeinen Grundsätze aus §§ 249 ff. BGB (Zetzsche in: Münchener Kommentar zum BGB, 9. Aufl., §

675v Rz. 57; Berger in: Jauernig, BGB, 18. Aufl., §§ 675 u-675 w, Rz. 4; Herresthal in: Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., § 675 v BGB Rz. 70).

82
Die Kläger sind mithin zum Ersatz des durch die nicht autorisierten Zahlungsvorgänge entstandenen Schadens verpflichtet, insbesondere der dadurch an die unbekannten Täter überwiesenen Beträge (Sprau in: Grüneberg, BGB, 82. Aufl. § 675 v Rz. 4) – hier 1.683,97 €.

83
β) Ein gegebenenfalls anspruchsminderndes Mitverschulden der Beklagten nach § 254 BGB – was grundsätzlich zu berücksichtigen wäre (Herresthal in: Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., § 675 v BGB Rz. 71) – ist von Klageseite nicht schlüssig vorgetragen.

84
Beim Online-Banking kann ein Mitverschulden der Bank auch aus der mangelnden Systemsicherheit resultieren (s. Senatsbeschluss v. 22.09.2022, Az. 19 U 2204/22, juris Rz. 125; zustimmend Maier, VuR 2023, 163 [172]). Sie muss ein technisch sicheres System nach dem jeweils aktuellen Stand der Technik bereitstellen (Herresthal in: Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 3. Aufl., § 675 v BGB Rz. 72; Zetzsche in: Münchener Kommentar zum BGB, 9. Aufl., § 675 v Rz. 58; Köbrich, VuR 2015, 9 [13]). Hierzu ist von Klageseite nichts dargetan.

85
ddd) Ein Schadenersatzanspruch aus § 280 Abs. 1 BGB scheidet dagegen aus.

86
Ansprüche des Zahlungsdienstleisters gegen den Zahler im Falle von nicht autorisierten Zahlungsvorgängen sind nach § 675 v Abs. 1, 3 BGB in seinem Anwendungsbereich abschließend geregelt; für eine Anwendung von § 280 Abs. 1 BGB ist daneben kein Raum (OLG Karlsruhe, Urteil v. 12.04.2022, Az. 17 U 823/20, Rz. 112 ff.).

87
cc) Die übrigen Voraussetzungen einer Aufrechnungslage nach § 387 BGB sind ebenso gegeben wie kein Aufrechnungsausschluss, namentlich nach §§ 390 ff. BGB, greift.

88
2. Verzugszinsen und außergerichtliche Rechtsverfolgungskosten sind somit von der Beklagten demgemäß ebenso nicht zu ersetzen.

III.

89
Die Rechtssache hat keine grundsätzliche Bedeutung (§§ 522 Abs. 2 S. 1 Nr. 2, 543 Abs. 2 S. 1 Nr. 1 ZPO). Auch erfordern weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Senats als Berufungsgericht oder die Zulassung der Revision (§§ 522 Abs. 2 S. 1 Nr. 3, 543 Abs. 2 S. 1 Nr. 2 ZPO).

90
Wie dargestellt, liegen den vorstehenden Ausführungen die von der höchstrichterlichen Rechtsprechung entwickelten Leitlinien zugrunde.

91
Zudem handelt es sich hier um eine Einzelfallentscheidung (vgl. BGH, Beschluss v. 14.08.2013, Az. XII ZB 443/12, Rz. 6), über welche hinaus die Interessen der Allgemeinheit nicht nachhaltig berührt werden, weswegen eine höchstrichterliche Leitentscheidung notwendig wäre (s. dazu BGH, Beschluss v. 25.05.2003, Az. VI ZB 55/02, juris Rz. 8; Beschluss v. 29.05.2002, Az. V ZB 11/02, juris Rz. 10).

92
Dazu ist keine mündliche Verhandlung geboten (§ 522 Abs. 2 S. 1 Nr. 4 ZPO), da keine besonderen Gründe vorgetragen oder sonst ersichtlich sind, bei denen nur die Durchführung einer mündlichen Verhandlung der prozessualen Fairness entspräche.

IV.

93
Bei dieser Sachlage wird schon aus Kostengründen empfohlen, die Berufung zurückzunehmen, was eine Ermäßigung der Gebühren für das „Verfahren im Allgemeinen“ von 4,0 (Nr. 1220 GKG-KV) auf 2,0 (Nr. 1222 GKG-KV) mit sich brächte.

94
Zu diesen Hinweisen besteht Gelegenheit zur Stellungnahme binnen drei Wochen nach Zustellung dieses Beschlusses. Der Senat soll nach der gesetzlichen Regelung die Berufung unverzüglich durch Beschluss zurückweisen, falls sich Änderungen nicht ergeben. Mit einer einmaligen Verlängerung dieser Frist um maximal drei weitere Wochen ist daher nur bei Glaubhaftmachung konkreter, triftiger Gründe zu rechnen (vgl. OLG Rostock, Beschluss v. 27.05.2003, Az. 6 U 43/03, juris Rz. 7 ff.). Eine Fristverlängerung um insgesamt mehr als einen Monat ist daneben entsprechend § 520 Abs. 2 S. 3 ZPO nur mit Zustimmung des Gegners möglich.