BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

XI ZR 91/14

Verkündet am:
26. Januar 2016
Weber,
Justizamtsinspektorin
als Urkundsbeamtin
der Geschäftsstelle

in dem Rechtsstreit

Nachschlagewerk: ja
BGHZ: ja
BGHR: ja

BGB § 675w
BGB § 675v Abs. 2
BGB § 172

a) Bei dem Nachweis der Autorisierung eines Zahlungsvorgangs mittels eines Zahlungsauthentifizierungsinstruments ist nach § 675w Satz 3 BGB Voraussetzung einer Anwendung der Grundsätze des Anscheinsbeweises, dass auf Grundlage aktueller Erkenntnisse die allgemeine praktische Unüberwindbarkeit des eingesetzten Sicherungsverfahrens sowie dessen ordnungsgemäße Anwendung und fehlerfreie Funktion im konkreten Einzelfall feststehen.

b) Der Zahlungsdienstnutzer muss zur Erschütterung eines für die Autorisierung eines Zahlungsauftrags sprechenden Anscheinsbeweises keinen konkreten und erfolgreichen Angriff gegen das Authentifizierungsinstrument vortragen und beweisen, sondern kann sich auch auf außerhalb des Sicherheitssystems des Zahlungsdienstleisters liegende Umstände stützen, die für einen nicht autorisierten Zahlungsvorgang sprechen.

c) Es gibt keinen einen Anscheinsbeweis rechtfertigenden Erfahrungssatz, dass bei einem Missbrauch des Online-Bankings, wenn die Nutzung eines Zahlungsauthentifizierungsinstruments korrekt aufgezeichnet worden und die Prüfung der Authentifizierung beanstandungsfrei geblieben ist, eine konkrete grob fahrlässige Pflichtverletzung des Zahlungsdienstnutzers nach § 675v Abs. 2 BGB vorliegt.

d) Zur Anwendbarkeit der Grundsätze der Anscheinsvollmacht und eines Handelns unter fremdem Namen bei einem Missbrauch des Online-Bankings.

BGH, Urteil vom 26. Januar 2016 - XI ZR 91/14 - OLG Schleswig
LG Lübeck

ECLI:DE:BGH:2016:260116UXIZR91.14.0

Der XI. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 26. Januar 2016 durch den Vorsitzenden Richter Dr. Ellenberger, den Richter Maihold sowie die Richterinnen Dr. Menges, Dr. Derstadt und Dr. Dauber

für Recht erkannt:

Auf die Revision der Beklagten wird der Beschluss des 5. Zivilsenats des Schleswig-Holsteinischen Oberlandesgerichts in Schleswig vom 22. Januar 2014 aufgehoben.

Die Sache wird zur neuen Verhandlung und Entscheidung, auch über die Kosten des Revisionsverfahrens, an das Berufungsgericht zurückverwiesen.

Von Rechts wegen

Tatbestand:

1 Die klagende Sparkasse begehrt Ausgleich des Schlusssaldos eines Geschäftsgirokontos der Beklagten, die entgegenhält, der behauptete Fehlbetrag resultiere aus einer im Wege des Online-Bankings ausgelösten Überweisung auf ein Konto des Streithelfers, die von ihr nicht autorisiert worden sei.

2 Die Beklagte unterhielt bei der Klägerin u.a. ein Geschäftsgirokonto, mit dem sie seit März 2011 am Online-Banking teilnahm. Der Geschäftsführer der Beklagten M. B. erhielt dazu eine persönliche Identifikationsnummer

(PIN), mit der er online auch auf das genannte Geschäftsgirokonto zugreifen und durch zusätzliche Eingabe einer Transaktionsnummer (TAN) Zahlungsaufträge erteilen konnte. Weiter vereinbarten die Parteien zur Freigabe einzelner Transaktionen das smsTAN-Verfahren (Übermittlung der TAN durch SMS) über eine Mobilfunknummer, die einer SIM-Karte zugewiesen war, die nach Angaben der Beklagten in einem grundsätzlich im Gewahrsam ihres Geschäftsführers befindlichen Mobiltelefon betrieben wurde.

3 Im Zuge einer Umstellung der EDV der Klägerin kam es im Juli 2011 zu länger andauernden Störungen in deren Online-Banking-System, über die auch in der Tagespresse berichtet wurde. Einige Kunden - darunter auch die Beklagte - konnten eine Zeit lang auf ihr Konto nicht online zugreifen, einzelne Lastschriften wurden nicht ausgeführt und andere Buchungen doppelt. In diesem Zusammenhang wurden aus nicht geklärten Umständen am 15. Juli 2011 dem Geschäftskonto der Beklagten fehlerhaft Beträge von 47.498,95 € und 191.576,25 € gutgeschrieben. Die Klägerin veranlasste am 15. und 17. Juli 2011 entsprechende Stornierungen, die aufgrund des Wochenendes erst am Montag, dem 18. Juli 2011, ausgeführt wurden. Wegen der Fehlbuchungen wies das Geschäftskonto der Beklagten bis zu diesem Montagmorgen buchungstechnisch ein Guthaben von nahezu 238.000 € auf.

4 Am Freitag, dem 15. Juli 2011, um 23:25 Uhr wurden unter Verwendung der PIN des Geschäftsführers der Beklagten im Online-Banking die Kontostände aller Konten der Beklagten sowie die Umsätze auf deren Geschäftskonto abgefragt. Um 23:29 Uhr wurde eine Überweisung von 235.000 € mit dem Verwendungszweck "M. B. ", dem Namen des Geschäftsführers der Beklagten, zugunsten des Streithelfers der Klägerin in das Online-Banking-System der Klägerin eingegeben. Die erforderliche smsTAN wurde von der Klägerin zur vereinbarten Mobiltelefonnummer der Beklagten übermittelt und so-

dann für die Freigabe dieser Überweisung verwendet. Im Anschluss daran kam es zwischen 23:31 Uhr und 23:36 Uhr zu drei weiteren Umsatzabfragen und einer Statusabfrage. Die Überweisung wurde am Montagmorgen, dem 18. Juli 2011, mit dem ersten Buchungslauf ausgeführt. Da zeitgleich die fehlerhaften Gutschriften berichtigt wurden, ergab sich ein Sollbetrag auf dem Geschäftskonto der Beklagten.

5 Nachdem die Klägerin die Beklagte erfolglos zum Ausgleich des Kontos aufgefordert hatte, kündigte sie die Geschäftsbeziehung fristlos und fordert mit der vorliegenden Klage Ausgleich des negativen Schlusssaldos von 236.422,14 € nebst Zinsen.

6 Die Klägerin hat behauptet, bei dem streitigen Zahlungsvorgang hätten keine Unregelmäßigkeiten vorgelegen. Der technische Ablauf sei ordnungsgemäß aufgezeichnet worden. Anhand der Darlegungen der Beklagten könne nicht nachvollzogen werden, wie es zu einem Missbrauch hätte kommen können.

7 Die Beklagte hat vorgetragen, sie bzw. ihr Geschäftsführer hätte die Überweisung nicht veranlasst und auch nicht veranlassen können, weil ihr Geschäftsführer zum maßgeblichen Zeitpunkt im Urlaub gewesen sei und sich das Geschäftshandy bei ihrem Mitarbeiter Ma. befunden habe, der die Überweisung ebenfalls nicht autorisiert, sondern die SMS, mit der eine TAN übermittelt worden sei, für Spam gehalten und "weggedrückt" habe.

8 Der Streithelfer der Klägerin hat behauptet, ihm habe eine schriftliche Weisung des Geschäftsführers der Beklagten vorgelegen, aufgrund der er den erhaltenen Betrag auf ein ihm mitgeteiltes Konto weitergeleitet habe. Im Übrigen hat er sich auf seine Schweigepflicht als Rechtsanwalt berufen.

9 Das Landgericht hat der Klage ohne Beweisaufnahme stattgegeben. Die Berufung der Beklagten ist vom Berufungsgericht durch Beschluss nach § 522 Abs. 2 ZPO zurückgewiesen worden. Mit der vom Senat zugelassenen Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter.

Entscheidungsgründe:

10 Die Revision ist begründet. Sie führt zur Aufhebung des Beschlusses des Berufungsgerichts und zur Zurückverweisung der Sache an das Berufungsgericht.

I.

11 Das Berufungsgericht hat unter umfassender Bezugnahme auf die Gründe des landgerichtlichen Urteils zur Begründung seiner Entscheidung im Wesentlichen ausgeführt:

12 Die Beklagte schulde der Klägerin Aufwendungsersatz nach §§ 675c, 670 BGB, da die Klägerin nach § 675w Satz 1 BGB den Nachweis einer Authentifizierung der streitigen Überweisung durch die Beklagte geführt habe. Die Beklagte habe den aus der Verwendung der richtigen PIN und TAN folgenden gegen sie sprechenden Anschein einer ordnungsgemäßen Nutzung des Online-Bankings nicht erschüttert. Umstände, welche die Benutzung des Zahlungsauthentifizierungsinstruments durch einen Unberechtigten plausibel erklären könnten, habe die Beklagte nicht aufgezeigt. Von der Beklagten angebotenen Zeugenbeweis habe das Landgericht zu Recht nicht erhoben, da kein substantiierter Tatsachenvortrag zu einem konkreten Missbrauch gehalten worden sei.

Auch im Berufungsverfahren erhelle die Beklagte nicht, wie es zu einer nicht autorisierten Überweisung habe kommen können. Es fehle substantiierter Vortrag dazu, dass das Firmenhandy mit einem Schadprogramm infiziert gewesen sei. Das Handy sei zu keiner Zeit von einem Computerspezialisten überprüft worden. Überdies bleibe unklar, wie ein unbefugter Dritter an die Zugangsdaten hätte gelangen können. Die vom Streithelfer behauptete schriftliche Zahlungsanweisung habe das Landgericht als Indiz würdigen dürfen, ohne die anwaltlich vertretene Beklagte hierzu auf die Möglichkeit eines Beweisantrags hinweisen zu müssen.

II.

13 Die Entscheidung des Berufungsgerichts hält revisionsrechtlicher Nachprüfung nicht stand. Die vom Berufungsgericht getroffenen Feststellungen rechtfertigen keinen Aufwendungsersatzanspruch der Klägerin gegen die Beklagte aus § 675c Abs. 1, § 675 i.V.m. § 670 BGB. Das Berufungsgericht hat bei Prüfung der dafür nach § 675j Abs. 1 BGB erforderlichen Autorisierung der streitgegenständlichen Überweisung durch die Beklagte die Voraussetzungen eines Anscheinsbeweises im Falle der Verwendung eines Zahlungsauthentifizierungsinstruments nach § 675j Abs. 1 Satz 4 BGB im Online-Banking verkannt sowie die Anforderungen an eine Erschütterung des Anscheinsbeweises überspannt.

14 1. Zutreffend geht das Berufungsgericht davon aus, dass ein Aufwendungsersatzanspruch der Klägerin gegen die Beklagte nach § 675c Abs. 1, § 675 i.V.m. § 670 BGB auf Zahlung des nach Kündigung des Geschäftsgirovertrages vorhandenen Sollsaldos den von der Klägerin zu erbringenden Nachweis einer Zustimmung des Zahlers (Autorisierung) zu der streitigen

Überweisung nach § 675j Abs. 1 Satz 1 BGB voraussetzt. Gemäß § 675j Abs. 1 Satz 3 BGB ist die Art und Weise der Zustimmung zwischen dem Zahler und dem Zahlungsdienstleister zu vereinbaren. Dabei kann nach § 675j Abs. 1 Satz 4 BGB festgelegt werden, dass die Zustimmung mittels eines Zahlungsauthentifizierungsinstruments im Sinne des § 1 Abs. 5 ZAG erteilt werden kann. Danach haben vorliegend die Parteien für die Autorisierung im Online-Banking die Nutzung des von der Beklagten angebotenen smsTAN-Verfahrens vereinbart, bei dem ein Zahlungsvorgang durch die Eingabe von PIN und TAN autorisiert wird, wobei die TAN mittels einer SMS-Nachricht an eine vereinbarte Mobilfunknummer des Bankkunden gesendet wird.

15 2. Weiter hat das Berufungsgericht nach § 559 Abs. 2 ZPO für die Revisionsinstanz bindend und insoweit von der Revision unangegriffen festgestellt, dass die Klägerin den Nachweis der Authentifizierung des streitigen Zahlungsvorgangs sowie von dessen ordnungsgemäßer Verbuchung, Aufzeichnung und Störungsfreiheit geführt hat.

16 Ist - wie hier - die Autorisierung eines Zahlungsvorgangs streitig, hat der Zahlungsdienstleister nach § 675w Satz 1 BGB zunächst die Authentifizierung sowie die ordnungsgemäße Aufzeichnung, Verbuchung und störungsfreie, keine Auffälligkeiten aufweisende technische Abwicklung des Zahlungsvorgangs nachzuweisen. Eine Authentifizierung ist nach § 675w Satz 2 BGB erfolgt, wenn der Zahlungsdienstleister die Nutzung des vereinbarten Zahlungsauthentifizierungsinstruments, einschließlich seiner personalisierten Sicherheitsmerkmale, mithilfe eines Verfahrens überprüft hat. Sind diese Voraussetzungen nicht erfüllt, ist der Nachweis einer Autorisierung mithilfe des betroffenen Zahlungsauthentifizierungsinstruments gescheitert (Palandt/Sprau, BGB, 75. Aufl., § 675w Rn. 2; MünchKommBGB/Casper, 6. Aufl., § 675w Rn. 4; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 72 f.;

Staudinger/Omlor, BGB, Neubearb. 2012, § 675w Rn. 4 f.; Nobbe in Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2. Aufl., § 675w BGB Rn. 16).

17 Vorliegend hat das Landgericht, dem das Berufungsgericht insoweit gefolgt ist, die erfolgreiche Überprüfung der streitigen Überweisung durch die Beklagte anhand des vorgelegten Transaktionsprotokolls und damit - insoweit von der Revision nicht angegriffen - den Nachweis der Authentifizierung dieses Zahlungsvorgangs sowie den Nachweis der Verbuchung, Aufzeichnung und Störungsfreiheit festgestellt.

18 3. Zutreffend geht das Berufungsgericht davon aus, dass nach § 675w Satz 3 Nr. 1 BGB die Authentifizierung und die Aufzeichnung der Nutzung des Zahlungsauthentifizierungsinstruments einschließlich der personalisierten Sicherheitsmerkmale aber nicht notwendigerweise ausreichen, den dem Zahlungsdienstleister - hier der Klägerin - obliegenden Nachweis einer Autorisierung des Zahlungsvorgangs zu führen. Hierzu von der Klägerin angebotene Beweise, insbesondere die Einvernahme des Streithelfers der Klägerin als Zeugen und die Einholung eines Sachverständigengutachtens, haben - von ihrem Rechtsstandpunkt zur Anwendung der Grundsätze des Anscheinsbeweises folgerichtig - jedoch weder das Landgericht noch das Berufungsgericht erhoben.

19 4. Weiter rechtsfehlerfrei geht das Berufungsgericht davon aus, dass sich ein Zahlungsdienstleister statt dessen gegenüber dem Zahler unter bestimmten Voraussetzungen zum Nachweis der strittigen Autorisierung auf einen Beweis des ersten Anscheins berufen kann, der allerdings bei Nutzung eines Zahlungsauthentifizierungsinstruments den besonderen Anforderungen des § 675w Satz 3 BGB genügen muss. Danach ist Voraussetzung eines Anscheinsbeweises bei Nutzung eines Zahlungsauthentifizierungsinstruments ein Sicherheits-

system, das allgemein praktisch nicht zu überwinden war, im konkreten Einzelfall ordnungsgemäß angewendet worden ist und fehlerfrei funktioniert hat.

20 a) In Rechtsprechung und Literatur ist streitig, ob die Beweisregeln in § 675w Satz 3 BGB, mit dem Art. 59 Abs. 2 der Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt (Zahlungsdiensterichtlinie) umgesetzt worden ist, einer Anwendung der Grundsätze des Anscheinsbeweises zugunsten des Zahlungsdienstleisters gestützt auf die Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments entgegenstehen.

21 aa) Eine Meinung in der Literatur (Franck/Massari, WM 2009, 1117, 1126; Jungmann in Jahrbuch junger Zivilrechtswissenschaftler Bd. 2007, 2008, S. 329, 356; Scheibengruber, BKR 2010, 15, 21; kritisch auch: Erman/Graf von Westphalen, BGB, 14. Aufl., § 675w Rn. 16 ff.), der sich vereinzelt Gerichte angeschlossen haben (z.B. AG Berlin-Mitte, NJW-RR 2010, 407, 408), geht davon aus, § 675w Satz 3 BGB verbiete im Zahlungsdiensterecht bei Einsatz eines Authentifizierungsinstruments die Anwendung des Anscheinsbeweises, da das dadurch entstehende Regel-Ausnahme-Verhältnis Sinn und Zweck des § 675w Satz 3 BGB widerspreche.

22 bb) Demgegenüber nimmt die h.M. an, § 675w Satz 3 BGB hindere eine Anwendung des Anscheinsbeweises im Zahlungsdiensterecht grundsätzlich nicht (OLG Düsseldorf, ZIP 2012, 2244, 2245; OLG Dresden, ZIP 2014, 766, 768; Beesch in Dauner-Lieb/Langen, BGB, 2. Aufl., § 675w Rn. 37; Beesch/Willershausen, juris-PR-BKR 9/2012 Anm. 1; Bunte, ABG-Banken und Sonderbedingungen, 4. Aufl., 4. Teil Rn. 31; MünchKommBGB/Casper, 6. Aufl., § 675w Rn. 13; Herresthal in Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 2013, § 675w Rn. 13; Hofmann, BKR 2014, 105, 112; Lohmann/Koch, WM 2008, 57, 63; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-

Handbuch, 4. Aufl., § 55 Rn. 80; Meckel, jurisPR-BKR 2/2010 Anm. 1; Nobbe, WM 2011, 961, 968; ders. in Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2. Aufl., § 675w Rn. 27; Staudinger/Omlor, BGB, Neubearb. 2012, § 675w Rn. 7; Schmalenbach in Bamberger/Roth, BGB, 3. Aufl., § 675w Rn. 12; Palandt/Sprau, BGB, 75. Aufl., § 675w Rn. 4; Werner in Kümpel/Wittig, Bank- und Kapitalmarktrecht, 4. Aufl., Rn. 7.774). Der Wortlaut des § 675w Satz 3 BGB verbiete mit der Formulierung "allein nicht notwendigerweise" lediglich zwingende Beweisregeln, nicht aber widerlegbare Beweiserleichterungen wie den Anscheinsbeweis.

23 b) Der Senat entscheidet diesen Streit anknüpfend an die h.M. dahin, dass § 675w Satz 3 BGB einer Anwendung des Anscheinsbeweises nicht entgegensteht, sondern vielmehr besondere Anforderungen an dessen Ausgestaltung stellt.

24 aa) Die Grundsätze des Anscheinsbeweises stehen nicht in Widerspruch zum Wortlaut des § 675w Satz 3 BGB, da dieser erst dann berührt wäre, wenn die Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments einschließlich der Authentifizierung durch den Zahlungsdienstleister den vollen Beweis für die in § 675w Satz 3 Nr. 1 bis Nr. 3 BGB genannten Tatsachen erbringen würde. Die Grundsätze des Anscheinsbeweises begründen hingegen weder eine zwingende Beweisregel noch eine Beweisvermutung und auch keine Beweislastumkehr zulasten einer Partei (st. Rspr. BGH, z.B. Urteile vom 5. Februar 1987 - I ZR 210/84, BGHZ 100, 31, 34 und vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 319). Ein Anscheinsbeweis wird vielmehr bereits dadurch erschüttert, dass der Prozessgegner atypische Umstände des Einzelfalles darlegt und im Falle des Bestreitens Tatsachen nachweist, die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache

nahelegen (BGH, Urteile vom 3. Juli 1990 - VI ZR 239/89, NJW 1991, 230, 231 mwN und vom 17. Januar 1995 - X ZR 82/93, VersR 1995, 723, 724).

25 Dies wird durch die Entstehungsgeschichte der Vorschrift gestützt. Der Zusatz "nicht notwendigerweise" ist in den Entwurf der Zahlungsdiensterichtlinie erst später eingefügt worden (MünchKommBGB/Casper, 6. Aufl., § 675w Rn. 12; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 80; siehe auch Burgard, WM 2006, 2065, 2069), um klarzustellen, dass eine umfassende Beweiswürdigung nach den Grundsätzen des nationalen Prozessrechts möglich bleiben soll (Erwägungsgrund 33 der Zahlungsdiensterichtlinie). Deswegen geht auch die Regierungsbegründung zum Entwurf des § 675w Satz 3 BGB davon aus, dass die nationalen Beweisgrundsätze und damit auch diejenigen über den Anscheinsbeweis weiterhin zulässig bleiben (BT-Drucks. 16/11643, S. 115).

26 bb) Der in § 675w Satz 3 BGB festgelegten Beweisregel ist aber auch bei Anwendung des Anscheinsbeweises praktische Geltung zu verschaffen. § 675w Satz 3 BGB begrenzt den Beweiswert einer schlichten Dokumentation des technischen Authentifizierungsvorgangs, um den Zahlungsdienstnutzer, der weder den Authentifizierungsvorgang technisch gestalten noch dessen korrekte Funktion im Einzelfall überblicken kann, nicht über § 675v Abs. 1 BGB hinaus mit den Risiken eines Missbrauchs technischer Authentifizierungsinstrumente zu belasten. Deswegen dürfen im Zahlungsdiensterecht beim Einsatz technischer Authentifizierungsinstrumente die Grundsätze des Anscheinsbeweises nicht so gehandhabt werden, dass sie bei Vorliegen allein der in § 675w Satz 3 BGB genannten technischen Merkmale aus praktischer Sicht einer Beweislastumkehr gleichkommen (vgl. Hofmann, BKR 2014, 105, 112; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 81; siehe

auch Staudinger/Omlor, BGB, Neubearb. 2012, Vorbemerkungen zu §§ 675c - 676c Rn. 203 aE).

27 Für eine Anwendung der Grundsätze des Anscheinsbeweises im Zahlungsdiensterecht bei dem Nachweis einer Autorisierung durch ein vereinbartes Zahlungsauthentifizierungsinstrument reicht danach allein die korrekte Aufzeichnung der Nutzung dieses Zahlungsauthentifizierungsinstruments nicht aus. Vielmehr müssen dessen allgemeine praktische Sicherheit und die Einhaltung des Sicherheitsverfahrens im konkreten Einzelfall feststehen. Zudem bedarf die Erschütterung des Anscheinsbeweises nicht zwingend der Behauptung und ggf. des Nachweises technischer Fehler des dokumentierten Authentifizierungsverfahrens.

28 (1) Der Anscheinsbeweis für eine Autorisierung durch den Zahlungsdienstnutzer darf nicht ohne Rücksicht auf das technische Schutzniveau des verwendeten Sicherheitssystems allein an die ordnungsgemäß aufgezeichnete Nutzung eines Zahlungsauthentifizierungsinstruments einschließlich seiner personalisierten Sicherheitsmerkmale anknüpfen (vgl. Staudinger/Omlor, BGB, Neubearb. 2012, Vorbemerkungen zu §§ 675c - 676c Rn. 203 aE; siehe dazu auch Schinkels in Gebauer/Wiedmann, Zivilrecht unter europäischem Einfluss, 2. Aufl., Kap. 16 Rn. 56). Die korrekte Aufzeichnung der Nutzung eines nicht ausreichend sicheren Zahlungsauthentifizierungsinstruments kann nämlich für sich keine Beweiserleichterung für den Zahlungsdienstleister rechtfertigen, da andernfalls der Zahlungsdienstnutzer entgegen der Wertung des § 675w Satz 3 Nr. 1 BGB das Risiko von Defiziten des von ihm nicht zu verantwortenden Authentifizierungsvorgangs tragen würde. Vielmehr ist ein allgemein praktisch nicht zu überwindendes und im konkreten Einzelfall ordnungsgemäß angewendetes und fehlerfrei funktionierendes Sicherheitssystem Voraussetzung für die Anwendung der Grundsätze des Anscheinsbeweises.

29 (2) Darüber hinaus darf vom Zahlungsdienstnutzer zur Erschütterung des Anscheinsbeweises nicht Vortrag und ggf. Nachweis verlangt werden, auf welche Weise die Schutzvorkehrungen des Authentifizierungsverfahrens überwunden worden oder weshalb sie wirkungslos geblieben sind. Das käme in der praktischen Wirkung ebenfalls einer gegen § 675w Satz 3 BGB verstoßenden unwiderleglichen Beweislastumkehr gleich (vgl. Erfurth, WM 2006, 2198, 2206), da der Zahlungsdienstnutzer im Allgemeinen über keine Kenntnisse zu dem eingesetzten Sicherungssystem und dessen Beachtung im Einzelfall verfügen wird. Vielmehr kann zur Erschütterung des Anscheinsbeweises die Darlegung und ggf. der Nachweis aller und damit auch außerhalb des technischen Zahlungsvorgangs liegender Tatsachen genügen, die die ernsthafte Möglichkeit eines Missbrauchs nahelegen (vgl. dazu BGH, Urteile vom 3. Juli 1990 - VI ZR 239/89, NJW 1991, 230, 231 mwN und vom 17. Januar 1995 - X ZR 82/93, VersR 1995, 723, 724).

30 5. Nach diesen Maßstäben hat das Berufungsgericht sowohl die Voraussetzungen für eine Anwendung der Grundsätze des Anscheinsbeweises im Online-Banking verkannt und deswegen erforderliche Feststellungen nicht getroffen als auch rechtsfehlerhaft die Anforderungen an ein Erschüttern des von ihm angenommenen Anscheinsbeweises durch die Beklagte als Zahlungsdienstnutzer überspannt.

31 a) Die Frage, ob im Einzelfall die Grundsätze eines Anscheinsbeweises anzuwenden sind, unterliegt der Prüfung durch das Revisionsgericht (BGH, Urteile vom 5. Februar 1987 - I ZR 210/84, BGHZ 100, 31, 33, vom 17. Februar 1988 - IVa ZR 277/86, NJW-RR 1988, 789, 790, vom 6. März 1991 - IV ZR 82/90, VersR 1991, 460, vom 23. Januar 1997 - I ZR 29/94, WM 1997, 1493, 1496 und vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 313).

32 b) Entgegen der Ansicht der Revisionsbegründung ist eine Anwendung der Grundsätze eines Anscheinsbeweises im Online-Banking nicht allgemein ausgeschlossen. Die allseits bekannte Gefahr des Ausspähens und Verfälschens von Daten, die über das Internet übermittelt werden, steht einer gesicherten Lebenserfahrung zur Verlässlichkeit einer Online-Autorisierung nämlich dann nicht entgegen, wenn auf Grundlage aktueller Erkenntnisse die allgemeine praktische Unüberwindbarkeit eines konkret eingesetzten Sicherungsverfahrens und dessen Beachtung im konkreten Einzelfall feststehen.

33 aa) Ob der Beweis des ersten Anscheins für die Autorisierung eines Zahlungsvorgangs im Online-Banking allgemein oder für bestimmte Authentifizierungsverfahren ausgeschlossen ist, ist in Literatur und Rechtsprechung umstritten (einen Anscheinsbeweis wohl generell verneinend: Casper/Pfeiffle, WM 2009, 2343, 2348; Kind/Werner, CR 2006, 353, 359; Erman/Graf von Westphalen, BGB, 14. Aufl., § 675w Rn. 21; Wiesgickl, WM 2000, 1039, 1047; einen Anscheinsbeweis bei Nutzung des einfachen PIN/TAN-Verfahrens ablehnend: AG Wiesloch, WM 2008, 1648, 1650; AG Krefeld, MMR 2013, 164, 165; Bunte, ABG-Banken und Sonderbedingungen, 4. Aufl., 4. Teil Rn. 26; Dienstbach/Mühlenbrock, K&R 2008, 151, 154; Erfurth, WM 2006, 2198, 2205; Nobbe in Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2. Aufl., § 675w Rn. 51; Spindler in Festschrift Nobbe, 2009, S. 215, 232; auch für das iTAN-Verfahren zweifelnd MünchKommBGB/Casper, 6. Aufl., § 675w Rn. 20; Staudinger/Omlor, BGB, Neubearb. 2012, § 675w Rn. 10; einen Anscheinsbeweis bei Nutzung des mTAN-(=smsTAN)Verfahrens bejahend: LG Köln, WM 2014, 2372 f.; Borges in Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, 2. Aufl., Rn. 157; ders., BKR 2009, 85; MünchKommBGB/Casper, 6. Aufl., § 675w Rn. 20; einen Anscheinsbeweis bei Verwendung des einfachen PIN/TAN- oder iTAN-Verfahrens ablehnend, jedoch für das mTAN-, Sm@rtTAN plus- und Sm@rtTAN optic-Verfahren bejahend:

Köbrich, VuR 2015, 9, 12; einen Anscheinsbeweis nur für optimierte eTAN bzw. chipTAN-Verfahren annehmend Hoeren/Kairies, ZBB 2015, 35, 37; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 85, 87; generell für das Eingreifen eines Anscheinsbeweises bei Nutzung der richtigen PIN und TAN unabhängig vom konkret verwendeten System: Bock in Neumann/Bock, Zahlungsverkehr im Internet, 2004, Rn. 180; Borges, NJW 2005, 3313, 3317; van Gelder in Festschrift Nobbe, 2009, S. 55, 67; Größmann/ Bredenkamp in Festschrift Nobbe, 2009, S. 93, 111; Karper, DuD 2006, 215, 218; Weber, Recht des Zahlungsverkehrs, 4. Aufl., S. 304; Werner, MMR 1998, 232, 235; Werner in Kümpel/Wittig, Bank- und Kapitalmarktrecht, 4. Aufl., Rn. 7.774).

34 bb) Der Senat entscheidet diese Streitfrage dahin, dass die Anwendung des Anscheinsbeweises für eine Autorisierung durch den Zahler im Online-Banking unter den oben genannten Voraussetzungen rechtlich zulässig und nicht generell ausgeschlossen ist.

35 Gegenwärtig werden nämlich Authentifizierungsverfahren im Online-Banking dann noch allgemein als praktisch unüberwindbar angesehen, wenn diese von einer Kompromittierung der eingesetzten Geräte nicht berührt werden, ein Zugriff Unberechtigter auf den Übertragungsweg ausgeschlossen ist, die - dynamische - TAN an den konkreten Zahlungsvorgang gebunden ist und das Verfahren dem Zahlungsdienstnutzer vor einer Freigabe die Überprüfung des vollständigen, unverfälschten Zahlungsauftrags ermöglicht (siehe Hoeren/ Kairies, ZBB 2015, 35, 36 f. und WM 2015, 549, 552 zum chipTAN-Verfahren; vgl. dazu auch Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 19, 85). Bislang sind noch keine praktisch erfolgreichen Angriffe auf ein derart ausgestaltetes System in der Öffentlichkeit bekannt geworden. Eine die Anwendung des Anscheinsbeweises rechtfertigende Typik muss

somit nicht von vornherein an der allgemeinen Unsicherheit einer Datenübertragung über das Internet scheitern.

36 c) Das Berufungsgericht hat aber rechtsfehlerhaft ohne Prüfung der praktischen Unüberwindbarkeit des eingesetzten Sicherungssystems einen Erfahrungssatz angenommen, nach Nutzung der zutreffenden PIN und smsTAN für einen Zahlungsauftrag im Online-Banking spreche der Anschein für dessen Autorisierung durch den Kontoinhaber. In diesem Zusammenhang hat es weiter zu Unrecht von dem Zahlungsdienstnutzer - hier der Beklagten - Darlegung und ggf. Nachweis dafür verlangt, dass die Nutzung des Authentifizierungsinstruments durch Unberechtigte technisch möglich gewesen sei.

37 aa) Der Beweis des ersten Anscheins erfordert die Feststellung eines allgemeinen Erfahrungssatzes als einer aus allgemeinen Umständen gezogenen tatsächlichen Schlussfolgerung, die auf den vorliegenden konkreten Sachverhalt angewendet werden kann (BGH, Urteile vom 4. Oktober 1983 - VI ZR 98/82, VersR 1984, 40 und vom 6. März 1991 - IV ZR 82/90, VersR 1991, 460, 461). Dieser Sachverhalt, der grundsätzlich von der beweisbelasteten Partei darzulegen und zu beweisen ist (BGH, Urteil vom 14. September 2005 - VIII ZR 369/04, NJW 2006, 300 Rn. 11), muss einer Typik entsprechen, also nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder auf einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolges hinweisen (BGH, Urteile vom 27. Mai 1957 - II ZR 132/56, BGHZ 24, 308, 312, vom 5. Februar 1987 - I ZR 210/84, BGHZ 100, 31, 33, vom 6. März 1991 - IV ZR 82/90, VersR 1991, 460, 461, vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 313 und vom 14. September 2005 - VIII ZR 369/04, NJW 2006, 300 Rn. 9 f.).

38 Voraussetzungen eines Anscheinsbeweises, der für die Autorisierung des Zahlungsvorgangs durch den Zahlungsdienstnutzer im Online-Banking spricht, sind danach - wie oben dargestellt - nicht nur die in § 675w Satz 1 BGB genannten Umstände, die lediglich die Dokumentation des Authentifizierungsvorgangs betreffen, sondern es bedarf zusätzlich der Feststellung eines allgemein praktisch nicht zu überwindenden, im konkreten Einzelfall ordnungsgemäß angewendeten und fehlerfrei funktionierenden Sicherheitssystems.

39 bb) Dazu hat das Berufungsgericht keine Feststellungen getroffen, sondern die rechtsfehlerhafte Auffassung des Landgerichts bestätigt, bereits die korrekte Aufzeichnung im Transaktionsprotokoll begründe den "Anschein einer ordnungsgemäßen Nutzung des Online-Banking".

40 (1) Funktionsweise und allgemeine praktische Unüberwindbarkeit des hier verwendeten smsTAN-Verfahrens sind weder substantiiert dargelegt noch sind dazu Beweise erhoben worden. Die isolierte Feststellung, die für einen Zahlungsvorgang erforderliche TAN sei an die bei der Bank hinterlegte Rufnummer der SIM-Karte des Geschäftsführers der Beklagten übermittelt und mit dieser TAN sei die Überweisung freigegeben worden, liefert keine Information zum Sicherheitsniveau des konkret eingesetzten Verfahrens.

41 (2) Weiter fehlt die notwendige Klärung, ob das von dem Zahlungsdienstleister konkret genutzte Sicherheitssystem im Zeitpunkt der Vornahme des strittigen Zahlungsvorganges ein ausreichendes Sicherheitsniveau für die Anwendung des Anscheinsbeweises geboten hat (vgl. dazu Senatsurteile vom 14. November 2006 - XI ZR 294/05, BGHZ 170, 18 Rn. 31 und vom 29. November 2011 - XI ZR 370/10, WM 2012, 164 Rn. 37; Senatsbeschluss vom 6. Juli 2010 - XI ZR 224/09, WM 2011, 924 Rn. 12). Diese Prüfung muss auf Grundlage des neuesten Stands der Erfahrung erfolgen (vgl. dazu Laumen in Baumgärtel/

Laumen/Prütting, Handbuch der Beweislast, 3. Aufl., Kap. 17 Rn. 26). Gerade im Online-Banking, in dem Sicherungssysteme und Angriffsszenarien laufenden und kurzfristigen Änderungen unterworfen sind, reichen älterer Rechtsprechung zugrunde liegende Erkenntnisse oder Ansichten von Stimmen in der Literatur nicht aus. Vielmehr wird regelmäßig Anlass bestehen, das eingesetzte Sicherungssystem und den konkreten technischen Ablauf, die dem streitigen Zahlungsvorgang zugrunde lagen, einer die aktuellen Erkenntnisse auswertenden sachverständigen Begutachtung zu unterziehen, um den neuesten Stand der Erfahrung zu erfassen (vgl. dazu auch Senatsbeschluss vom 6. Juli 2010 - XI ZR 224/09, WM 2011, 924 Rn. 12 und Senatsurteil vom 29. November 2011 - XI ZR 370/10, WM 2012, 164 Rn. 37).

42 (a) Da zu dem hier eingesetzten smsTAN-Verfahren zahlreiche bekannt gewordene erfolgreiche Attacken die Frage aufwerfen, ob es allgemein als praktisch unüberwindbar gelten und damit einen Anscheinsbeweis für die Autorisierung der Zahlung durch den Zahlungsdienstnutzer bei Verwendung der richtigen PIN und TAN rechtfertigen kann, hätte das Berufungsgericht hierzu Feststellungen treffen müssen. So sind zum Online-Banking eingesetzte Computer zugleich mit dem zum Empfang der TAN eingesetzten Smartphone infiziert worden (vgl. Bundesamt für Sicherheit in der Informationstechnik, Pressemeldung vom 4. März 2011, Neue Schadsoftware liest mTAN-Nummern mit), sodass Zahlungsvorgänge in Echtzeit manipuliert werden konnten (siehe Bundeskriminalamt, Bundeslagebericht 2013 - Cybercrime, S. 8). Weiter waren mittels eines Trojaners durchgeführte sog. Man-In-The-Middle/Man-In-The-Browser-Attacken erfolgreich (Bundeskriminalamt, Bundeslagebericht 2014 - Cybercrime, S. 7 f. und Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2014, S. 30; siehe dazu auch Köbrich, VuR 2015, 9, 10; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 85, 87; Nobbe in Ellenberger/Findeisen/Nobbe,

Kommentar zum Zahlungsverkehrsrecht, 2. Aufl., § 675w Rn. 53; Staudinger/ Omlor, BGB, Neubearb. 2012, § 675w Rn. 10). Danach ist aufgrund öffentlich zugänglicher Quellen fraglich, ob das smsTAN-Verfahren allgemein einen Sicherheitsstandard aufweist, der die Anwendung der Regeln des Anscheinsbeweises rechtfertigt.

43 (b) Weiter hat das Berufungsgericht die Klärung rechtsfehlerhaft unterlassen, ob mögliche Sicherheitsdefizite des smsTAN-Verfahrens dessen Einordnung als allgemein praktisch unüberwindbar bereits im Zeitpunkt der streitigen Autorisierung hinderten. Denn inzwischen bekannt gewordene Schwächen des smsTAN-Verfahrens, die jedoch im Zeitpunkt der Erteilung des hier streitigen Zahlungsauftrags noch nicht bekannt oder praktisch nicht nutzbar waren, können einer Anwendung der Grundsätze des Anscheinsbeweises nicht entgegenstehen.

44 (3) Unabhängig davon war vor einer Anwendung der Grundsätze des Anscheinsbeweises die Einhaltung des Sicherheitsniveaus des smsTAN-Verfahrens im Online-Banking-System der Klägerin bei Erteilung des konkreten Zahlungsauftrags zu überprüfen.

45 Dazu bestand im vorliegenden Fall besonderer Anlass, da unstreitig wegen einer EDV-Umstellung bei der Klägerin über längere Zeit erhebliche Softwareprobleme auch im Online-Banking auftraten, die etwa zu unberechtigten Gutschriften in sechsstelliger Höhe führten. Davon war auch das Geschäftsgirokonto der Beklagten betroffen. Eine die Anwendung des Anscheinsbeweises rechtfertigende Typizität setzt mithin vorliegend die konkrete Darlegung und ggf. den Nachweis voraus, dass sich solche Probleme nicht auf das Sicherheitssystem des smsTAN-Verfahrens ausgewirkt haben.

46 (4) In diesem Zusammenhang hat das Berufungsgericht im Anschluss an das Landgericht weiter rechtsfehlerhaft angenommen, dass Voraussetzung einer Beweisaufnahme über die Sicherheit des eingesetzten Authentifizierungssystems substantiierter Vortrag der Beklagten als Zahlungsdienstnutzer zu konkreten Defiziten im Sicherheitssystem des Online-Bankings der Klägerin sei. Da grundsätzlich die beweisbelastete Partei die Darlegungs- und Beweislast auch für die Tatsachen trägt, die der Anwendung eines Anscheinsbeweises zugrunde liegen (BGH, Urteil vom 14. September 2005 - VIII ZR 369/04, NJW 2006, 300 Rn. 11), hat vielmehr der Zahlungsdienstleister - hier die Klägerin - die konkrete Ausgestaltung des von ihm eingesetzten Authentifizierungssystems und dessen Sicherheitsniveau darzulegen und im Falle des Bestreitens zu beweisen.

47 d) Das Berufungsgericht hat weiter rechtsfehlerhaft die Anforderungen an ein Erschüttern des von ihm angenommenen Anscheinsbeweises überspannt und deswegen von seinem Rechtsstandpunkt aus zu Unrecht die dazu von der Beklagten angebotenen Zeugen nicht vernommen bzw. den Geschäftsführer der Beklagten nicht zumindest angehört.

48 aa) Ein Anscheinsbeweis ist erschüttert, wenn der Beweisgegner Tatsachen darlegt und gegebenenfalls zur vollen Überzeugung des erkennenden Gerichts beweist (BGH, Urteil vom 18. Dezember 1952 - VI ZR 54/52, BGHZ 8, 239, 240), die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache nahelegen (BGH, Urteile vom 3. Juli 1990 - VI ZR 239/89, NJW 1991, 230, 231 mwN und vom 17. Januar 1995 - X ZR 82/93, VersR 1995, 723, 724). Danach muss der Zahlungsdienstnutzer zur Erschütterung des Anscheinsbeweises keinen konkreten und erfolgreichen Angriff gegen das Authentifizierungsinstrument beweisen, sondern nur solche Umstände, die gegen die Autorisierung durch ihn und für ein missbräuchliches Eingreifen eines Dritten sprechen. Diese Anforderungen kann der Zahler auch dadurch erfüllen, dass er

außerhalb des Sicherheitssystems des Zahlungsdienstleisters liegende Indizien, die für einen nicht autorisierten Zahlungsvorgang sprechen, substantiiert darlegt und bei Bestreiten nachweist.

49 bb) Entgegen der Ansicht des Berufungsgerichts hat die Beklagte zu solchen, zur Erschütterung des Anscheinsbeweises geeigneten Umständen hinreichend vorgetragen.

50 (1) Sie hat behauptet und unter Beweis gestellt, dass der Geschäftsführer der Beklagten den Überweisungsempfänger nicht kenne und er diesem auch keine schriftliche Zahlungsanweisung erteilt habe. Sofern eine solche mit seiner Unterschrift vorliegen sollte, sei die Unterschrift gefälscht. Weiter sei er zum Zeitpunkt der Überweisung in Urlaub gewesen und habe keine Möglichkeit gehabt, Buchungen im Wege des Online-Bankings vorzunehmen. Das Mobiltelefon, in dem sich die SIM-Karte zu der bei der Klägerin für das smsTAN-Verfahren hinterlegten Telefonnummer befunden habe, habe sich im Gewahrsam eines Mitarbeiters befunden, der ebenfalls keinen Überweisungsauftrag erteilt habe. Die TAN sei zwar über SMS auf dem Mobiltelefon eingegangen, der Mitarbeiter habe diese SMS aber für Spam gehalten und "weggedrückt" sowie die TAN nicht verwendet.

51 (2) Träfe diese Sachdarstellung zu, hätte der Geschäftsführer der Beklagten im Zeitpunkt der Erteilung eines Überweisungsauftrags keinen Zugriff auf die erforderliche TAN gehabt und der als Zeuge benannte Mitarbeiter hätte mangels PIN keinen Zahlungsauftrag erteilen können sowie die TAN nicht genutzt. Zudem wäre der Zahlungsempfänger dem Geschäftsführer der Beklagten unbekannt gewesen. Könnte die Beklagte diese Behauptungen zur Überzeugung der Tatsachengerichte nachweisen, wäre ein Anscheinsbeweis ersichtlich erschüttert. Die Anträge auf Vernehmung des Mitarbeiters Ma. und weite-

rer Zeugen sowie ggf. auf Anhörung des Geschäftsführers der Beklagten durften deswegen nicht zurückgewiesen werden. Das gilt auch für die Vernehmung des Streithelfers, die - was vom Berufungsgericht übersehen worden ist - bereits in der Klageerwiderung beantragt worden ist.

52 cc) Entgegen der Ansicht des Berufungsgerichts musste die Beklagte als Voraussetzung einer Erhebung dieser Beweise nicht darlegen, dass das von der Beklagten eingesetzte Mobiltelefon mit einem Schadprogramm infiziert gewesen ist, nicht von sich aus einen Computerexperten mit der Untersuchung des Mobiltelefons beauftragen und auch nicht erklären, auf welche Weise ein unbefugter Dritter an die Zugangsdaten gelangt ist. Die Erschütterung eines Anscheinsbeweises verlangt nämlich nicht die Aufklärung des unsicheren Geschehensablaufs, sondern lediglich den Nachweis der ernsthaften, ebenfalls in Betracht kommenden Möglichkeit einer anderen Ursache.

53 e) Die Revision beanstandet schließlich zu Recht, das Berufungsgericht habe in diesem Zusammenhang rechtsfehlerhaft die für die Klägerin günstige Indiztatsache, dem Streithelfer sei von der Beklagten ein Auftrag zur Weiterleitung des zu Unrecht überwiesenen Betrags erteilt worden, als festgestellt zugrunde gelegt. Dazu ist nämlich von der Klägerin und ihrem Streithelfer nur Vortrag gehalten worden, den die Beklagte bestritten hat, sodass es bei der Beweislast der Klägerin verblieben ist. Deswegen kommt es - anders als das Berufungsgericht meint - zunächst nicht auf einen Antrag der Beklagten zur Führung des Gegenbeweises an. Das Berufungsgericht hätte vielmehr den von der Klägerin angetretenen Hauptbeweis zu der ihr günstigen Behauptung erheben müssen, die Beklagte habe dem Streithelfer einen entsprechenden Auftrag erteilt. Da sich auch die Beklagte bereits in der Klageerwiderung - gegenbeweislich - auf die Vernehmung des Streithelfers als Zeugen berufen hat, dürfte dessen Vernehmung die anwaltliche Schweigepflicht aus einem möglichen An-

waltsvertrag mit der Beklagten nicht entgegenstehen (§ 385 Abs. 2, § 383 Abs. 1 Nr. 6 ZPO).

III.

54 Die Entscheidung des Berufungsgerichts stellt sich auch nicht aus anderen Gründen als richtig dar (§ 561 ZPO).

55 1. Die Überweisung des streitigen Betrags vom Konto der Beklagten auf ein Konto des Streithelfers wirkt nicht nach den Grundsätzen der Anscheinsvollmacht oder eines Handelns unter fremdem Namen zulasten der Beklagten.

56 a) In Rechtsprechung und Literatur ist umstritten, ob von Dritten unter Nutzung eines Zahlungsauthentifizierungsinstruments einschließlich seiner personalisierten Sicherheitsmerkmale veranlasste Zahlungsvorgänge dem Zahler nach den Grundsätzen der Anscheinsvollmacht zugerechnet werden können (für eine generelle Anwendbarkeit der Grundsätze der Anscheinsvollmacht: Größmann in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 3. Aufl., § 55 Rn. 26; Größmann/Bredenkamp in Festschrift Nobbe, 2009, S. 93, 102 ff.; eine Anscheinsvollmacht im Falle eines Man-in-the-Middle-Angriffs bei Verwendung des Smart-TAN-plus-Verfahrens bejahend: LG Darmstadt, ZIP 2014, 1972, 1974; die Anwendbarkeit von Rechtsscheingrundsätzen ablehnend: KG, WM 2011, 493, 494; LG Berlin, Urteil vom 11. August 2009 - 37 O 4/09, juris Rn. 15; Borges, NJW 2005, 3313, 3314; Dienstbach/Mühlenbrock, K&R 2008, 151, 154; Köbrich, VuR 2015, 9, 12; Linardatos, BKR 2015, 96, 98; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 68; Omlor, ZfRV 2013, 80, 86; Spindler in Festschrift Nobbe, 2009, S. 215, 218 ff.; Erman/Graf von Westphalen, BGB, 14. Aufl., § 675w Rn. 22).

57 b) Der Senat hat erhebliche Zweifel, ob die Grundsätze einer Anscheinsvollmacht bzw. eines Handelns unter fremdem Namen im Recht der Zahlungsdienste neben den Spezialvorschriften der § 675j Abs. 1 Satz 4, §§ 675u, 675v BGB angewendet werden können.

58 Die Auffassung, ein Kontoinhaber müsse Zahlungsaufträge, die ein Dritter unter missbräuchlicher Verwendung eines Authentifizierungsinstruments erteilt hat, nach diesen Rechtsscheingrundsätzen gegen sich gelten lassen, wenn ihm das Handeln des Nichtberechtigten bekannt war oder er es hätte erkennen können (vgl. OLG Schleswig-Holstein, CR 2011, 52; KG Berlin, WM 2012, 493, 494; LG Darmstadt, ZIP 2014, 1972, 1974 f.; Fischer/Klanten/Koch, Bankrecht, 4. Aufl., Rn. 10.475 f.; MünchKommHGB/Häuser/Haertlein, 3. Aufl., Bd. 6, Bankkartenverfahren, Rn. E 37; Herresthal in Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 2013, § 675u Rn. 7), ist mit den nach § 675e Abs. 1 BGB im Grundsatz abschließenden (vgl. auch Senatsurteil vom 16. Juni 2015 - XI ZR 243/13, WM 2015, 1631 Rn. 23) Regelungen in § 675j Abs. 1 Satz 4, § 675u Satz 1 BGB nicht zu vereinbaren (Linardatos, BKR 2015, 96, 98; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 68; siehe auch MünchKommBGB/Schubert, 7. Aufl., § 167 Rn. 126 und Stöber JR 2012, 225, 231). Denn nach dem zwischen Bank und Kunde geschlossenen Vertrag ist bei Nutzung eines personalisierten Zahlungsauthentifizierungsinstruments, das ohnehin nach § 675l BGB geheim zu halten ist, eine Bevollmächtigung Dritter ausnahmslos ausgeschlossen. Das Handeln eines Dritten bei der förmlichen Authentifizierung nach § 675j Abs. 1 Satz 4 BGB mit den personalisierten Sicherheitsmerkmalen des Kontoinhabers ist damit unwirksam und kann auch dann einen Zahlungsauftrag mittels des betreffenden Authentifizierungsverfahrens nicht autorisieren, wenn die persönlichen Sicherheitsmerkmale vom Dritten mit Zustimmung des Kontoinhabers eingesetzt worden sein sollten. Zudem ist der in § 675v Abs. 2 BGB festgelegte Grundsatz,

dass der Kontoinhaber für einen nicht autorisierten Zahlungsvorgang nur bei Vorsatz oder grober Fahrlässigkeit einzustehen hat, berührt, wenn daneben dessen Haftung nach den Regeln eines Handelns unter fremdem Namen auch für einfache Fahrlässigkeit in Betracht käme (Linardatos, BKR 2015, 96, 98; Köbrich, VuR 2015, 9, 12; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 68; vgl. auch Stöber, JR 2012, 225, 231).

59 Soll ein entsprechend Bevollmächtigter das Recht erhalten, für den Kontoinhaber mit einem Zahlungsauthentifizierungsinstrument Zahlungsvorgänge zu autorisieren, muss ihm ein eigenes personalisiertes Authentifizierungsinstrument einschließlich gesonderter personalisierter Sicherheitsmerkmale zugewiesen werden.

60 c) Dies bedarf im vorliegenden Fall jedoch keiner abschließenden Entscheidung, da die Voraussetzungen einer Anscheinsvollmacht oder eines Handelns unter fremdem Namen bei der - hier zu unterstellenden - missbräuchlichen Nutzung von PIN und TAN im Online-Banking nicht vorliegen.

61 aa) Eine Anscheinsvollmacht setzt voraus, dass der Vertretene das Handeln des Scheinvertreters nicht kennt, er es aber bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können, und der Geschäftspartner annehmen durfte, der Vertretene kenne und billige das Handeln des Vertreters (st. Rspr., vgl. BGH, Urteile vom 10. Januar 2007 - VIII ZR 380/04, NJW 2007, 987 Rn. 25, vom 16. März 2006 - III ZR 152/05, BGHZ 166, 369 Rn. 17 und vom 11. Mai 2011 - VIII ZR 289/09, BGHZ 189, 346 Rn. 16 jeweils mwN). Zudem ist im Grundsatz erforderlich, dass das Verhalten des Geschäftsherrn, aus dem der Geschäftsgegner auf die Bevollmächtigung des Dritten schließt, von einer gewissen Dauer und Häufigkeit ist (st. Rspr., vgl. BGH, Urteile vom 10. Januar 2007 - VIII ZR 380/04, NJW 2007, 987 Rn. 25, vom 16. März 2006 - III ZR

152/05, BGHZ 166, 369 Rn. 17 und vom 11. Mai 2011 - VIII ZR 289/09, BGHZ 189, 346 Rn. 16 jeweils mwN).

62 Diese Voraussetzungen sind vorliegend nicht erfüllt. Die Klägerin hat - nach dem hier zugrunde zu legenden Sachverhalt - nicht erkannt, dass ein Dritter und nicht der Kunde gehandelt hat. Zudem kommt lediglich ein einmaliger Missbrauch des Online-Bankings und kein Handeln von gewisser Dauer und Häufigkeit in Betracht.

63 bb) Die Beklagte haftet auch nicht wegen eines Handelns des unbekannten Dritten unter ihrem Namen in entsprechender Anwendung der für Anscheinsvollmachten geltenden Grundsätze.

64 Erweckt das verdeckte Handeln unter fremdem Namen bei dem Geschäftspartner den Eindruck, tatsächlich werde die Erklärung vom Namensträger abgegeben, und wird dadurch eine falsche Vorstellung von der Identität des Handelnden hervorgerufen, können die Grundsätze der Anscheinsvollmacht entsprechend anzuwenden sein (vgl. BGH, Urteil vom 3. März 1966 - II ZR 18/64, BGHZ 45, 193, 195 f. und vom 11. Mai 2011 - VIII ZR 289/09, BGHZ 189, 346 Rn. 12). Dies kann auch für Geschäfte gelten, die - vergleichbar der vorliegenden Konstellation - über das Internet abgewickelt werden (vgl. BGH, Urteil vom 11. Mai 2011, aaO Rn. 12; Palandt/Ellenberger, BGB, 75. Aufl., § 172 Rn. 18).

65 Der Geschäftsherr wird aber auch in diesem Fall nur verpflichtet, wenn er das Handeln des Scheinvertreters bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können und dieses Handeln von einer gewissen Dauer und Häufigkeit war (vgl. BGH, Urteil vom 11. Mai 2011 - VIII ZR 289/09, BGHZ 189, 346 Rn. 16). Beide Voraussetzungen sind nicht erfüllt, wenn lediglich ein einmaliger missbräuchlicher Kontozugriff in Betracht kommt, der - entsprechend dem

auch hier zugrunde zu legenden Sachverhalt - von dem Zahlungsdienstnutzer erst im Nachhinein erkannt wurde.

66 2. Die Klage ist entgegen der Ansicht der Revisionserwiderung auch nicht nach § 675v Abs. 2 BGB als Schadensersatzanspruch begründet.

67 a) Tatsachen, die eine betrügerische Absicht oder ein grob fahrlässiges Verhalten der Beklagten belegen würden, sind von der Klägerin nicht vorgetragen und vom Berufungsgericht nicht festgestellt worden.

68 b) Es gibt auch keinen Erfahrungssatz, wonach bei einem Missbrauch des Online-Bankings bereits die korrekte Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die beanstandungsfreie Prüfung der Authentifizierung für eine grob fahrlässige Pflichtverletzung des Zahlungsdienstnutzers sprechen, sodass sich der Zahlungsdienstleister für den ihm im Rahmen von § 675v Abs. 2 BGB obliegenden Nachweis auch nicht auf den Beweis des ersten Anscheins stützen kann.

69 aa) In Literatur und Rechtsprechung ist umstritten, ob bei missbräuchlicher Verwendung von PIN und TAN durch einen Dritten im Online-Banking ein Anscheinsbeweis für eine grob fahrlässige Pflichtverletzung des Zahlers in Anspruch genommen werden kann (mangels Typizität einen Anscheinsbeweis generell bezweifelnd: Erman/Graf von Westphalen, BGB, 14. Aufl., § 675w Rn. 21; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 166; Staudinger/Omlor, BGB, Neubearb. 2012, § 675w Rn. 10; Schulte am Hülse/Klabunde, MMR 2010, 84, 87; Spindler in Festschrift Nobbe, 2009, S. 215, 232; einen Anscheinsbeweis für einfache Fahrlässigkeit bejahend, für grobe Fahrlässigkeit verneinend: Grundmann, WM 2009, 1157, 1163; kein Anscheinsbeweis für eine grob fahrlässige Sorgfaltspflichtverletzung bei Anwendung des klassischen PIN/TAN-Verfahrens: LG Mannheim, WM 2008, 2015;

Borges, BKR 2009, 85, 87; Dienstbach/Mühlenbrock, K&R 2008, 151, 154; Erfurth, WM 2006, 2198, 2206; Kind/Werner, CR 2006, 353, 359; Nobbe in Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2. Aufl., § 675w Rn. 52; Herresthal in Langenbucher/Bliesener/Spindler, Bankrechts-Kommentar, 2013, § 675w Rn. 15, der jedoch für das iTAN-, eTAN- und mTAN-Verfahren einen Anscheinsbeweis für grobe Fahrlässigkeit annimmt; kein Anscheinsbeweis bei Verwendung des mTAN-Verfahrens: LG Köln, WM 2014, 2372; einen Anscheinsbeweis allgemein bejahend: Bender, WM 2008, 2049, 2058; Bock in Neumann/Bock, Zahlungsverkehr im Internet, 2004, Rn. 183; Borges, BKR 2009, 85; van Gelder in Festschrift Nobbe, 2009, S. 55, 67; Gößmann/Bredenkamp in Festschrift Nobbe, 2009, S. 93, 110; Werner in Hoeren/Sieber/Holznagel, Hdb. Multimedia-Recht, Teil 13.5, Stand Juli 2013 Rn. 63; Wiesgickl, WM 2000, 1039, 1050).

70 bb) Der Senat entscheidet diesen Streit dahingehend, dass bei missbräuchlicher Verwendung von PIN und TAN im Online-Banking allein die Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die Prüfung der Authentifizierung im Sinne von § 675w Satz 3 Nr. 4 BGB die Anwendung der Grundsätze des Anscheinsbeweises für eine grob fahrlässige Pflichtverletzung des Zahlers nicht rechtfertigen. Auch ein Anscheinsbeweis auf alternativer Grundlage, der Zahlungsdienstnutzer habe entweder den Zahlungsvorgang autorisiert oder aber grob fahrlässig gegen seine Pflichten aus § 675l BGB verstoßen, kommt deswegen nicht in Betracht.

71 (1) Grobe Fahrlässigkeit erfordert einen in objektiver Hinsicht schweren und in subjektiver Hinsicht schlechthin unentschuldbaren Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt (BGH, Urteile vom 30. Januar 2001 - VI ZR 49/00, NJW 2001, 2092, 2093, vom 11. Juli 2007 - XII ZR 197/05, NJW 2007, 2988 Rn. 15 und vom 10. Oktober 2013 - III ZR 345/12, BGHZ 198,

265 Rn. 26 mwN). Selbst ein objektiv grober Pflichtenverstoß rechtfertigt für sich noch keinen zwingenden Schluss auf ein entsprechend gesteigertes personales Verschulden (BGH, Urteile vom 30. Januar 2001 - VI ZR 49/00, NJW 2001, 2092, 2093 und vom 10. Oktober 2013 - III ZR 345/12, BGHZ 198, 265 Rn. 28).

72 (2) Es gibt keine die Grundsätze des Anscheinsbeweises stützende Erfahrungssätze, dass bei Aufzeichnung der fehlerfreien Nutzung eines Authentifizierungsinstruments ein Missbrauch des Online-Bankings auf einer solchen subjektiv unentschuldbaren Verletzung von Sorgfaltspflichten in besonders schwerem Maße durch den Zahlungsdienstnutzer beruhen würde oder dass in einem solchen Fall jedenfalls ein tatsächliches Verhalten des Zahlungsdienstnutzers belegt wäre, das als grob fahrlässig bewertet werden könnte.

73 (a) Die Regeln des Anscheinsbeweises sind auf den Nachweis der subjektiven Voraussetzungen grober Fahrlässigkeit grundsätzlich dann nicht anwendbar, wenn es sich - wie hier - um ein individuelles Versagen handelt (vgl. BGH, Urteile vom 21. April 1970 - VI ZR 226/68, VersR 1970, 568, vom 7. Mai 1974 - VI ZR 138/72, VersR 1974, 853, vom 29. Januar 2003 - IV ZR 173/01, NJW 2003, 1118, 1119 und vom 21. März 2007 - I ZR 166/04, NJW-RR 2007, 1630 Rn. 20; Bacher in BeckOK ZPO, Stand: 1. September 2015, § 284 ZPO Rn. 96; Staudinger/Georg Caspers, BGB, Neubearb. 2014, § 276 Rn. 97; Palandt/Grüneberg, BGB, 75. Aufl., § 277 Rn. 7; Leipold in Stein/Jonas, ZPO, 22. Aufl., § 286 Rn. 142; Saenger/Saenger, ZPO, 6. Aufl., § 286 Rn. 43). Dieser Grundsatz gilt auch, wenn der Missbrauch des Online-Bankings auf einem Umstand aus der Sphäre des Zahlungsdienstnutzers beruht. Denn ein objektiv grober Pflichtenverstoß rechtfertigt für sich allein noch nicht den Schluss auf ein gesteigertes personales Fehlverhalten, selbst wenn dieses in vergleichbaren Fällen häufig vorliegen sollte (vgl. dazu BGH, Urteile vom 12. Januar 1988

- VI ZR 158/87, NJW 1988, 1265, 1266 und vom 30. Januar 2001 - VI ZR 49/00, NJW 2001, 2092, 2093).

74 (b) Die Regeln des Anscheinsbeweises können aber auch nicht zum Nachweis der objektiven Voraussetzungen grober Fahrlässigkeit des Zahlungsdienstnutzers im Online-Banking herangezogen werden. Zwar ist der Anscheinsbeweis zum Nachweis grober Fahrlässigkeit grundsätzlich zulässig, wenn damit lediglich die Annahme eines bestimmten tatsächlichen Verhaltens gestützt werden soll und dieses erst in einem weiteren Schritt rechtlich als grob fahrlässig bewertet wird (vgl. Senatsurteil vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 319).

75 Im Falle eines Missbrauchs des Online-Bankings gibt es aber keine Erfahrungssätze, die auf ein bestimmtes typisches Fehlverhalten des Zahlungsdienstnutzers hinweisen würden. Die Vielzahl von Authentifizierungsverfahren, die sich zum Teil erheblich im Sicherungskonzept und in dessen Ausgestaltung unterscheiden (vgl. Hoeren/Kairies, ZBB 2015, 35; Maihold in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl., § 55 Rn. 7 ff.), können jeweils auf unterschiedliche Weise angegriffen werden, wozu wiederum verschiedene Pflichtverletzungen des Zahlungsdienstnutzers beitragen können, sodass - anders als bei Nutzung von Zahlungskarten an Geldautomaten (Senatsurteile vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 317 f. und vom 29. November 2011 - XI ZR 370/10, WM 2012, 164 Rn. 16; Senatsbeschluss vom 6. Juli 2010 - XI ZR 224/09, WM 2010, 924 Rn. 10) - ein Missbrauch des Online-Bankings nicht auf ein bestimmtes Verhalten des Zahlungsdienstnutzers hinweist, das sodann als grob fahrlässig eingeordnet werden könnte.

IV.

76 Einer Vorlage an den Europäischen Gerichtshof zur Klärung der Frage, ob eine Anwendung der Regeln des Anscheinsbeweises bei Einsatz eines Zahlungsauthentifizierungsinstruments mit der Zahlungsdiensterichtlinie zu vereinbaren ist, bedarf es nicht, da nach den oben dargestellten Grundsätzen der Anscheinsbeweis im Online-Banking in Übereinstimmung mit Art. 59 Abs. 2 der Zahlungsdiensterichtlinie nicht ausschließlich an die genannte Dokumentation der Nutzung des Authentifizierungsverfahrens anknüpft und zudem keine zwingende Beweisregel zur Folge hat. Im Übrigen obliegt die Beweiswürdigung, zu der auch die Grundsätze des Anscheinsbeweises gehören, nach Erwägungsgrund 33 der Zahlungsdiensterichtlinie den Gerichten nach nationalem Recht.

V.

77 Der Zurückweisungsbeschluss ist deshalb aufzuheben (§ 562 Abs. 1 ZPO). Da die Sache nicht zur Endentscheidung reif ist, ist sie zur neuen Verhandlung und Entscheidung an das Berufungsgericht zurückzuverweisen (§ 563 Abs. 1 Satz 1 ZPO).

78 1. Dieses wird, wenn es die Grundsätze des Anscheinsbeweises anwenden will, ggf. nach Ergänzung des Vortrags der Klägerin zum verwendeten Sicherheitssystem mit sachverständiger Hilfe festzustellen haben, ob dieses nach heutigem Kenntnisstand im Zeitpunkt der Autorisierung des streitigen Zahlungsvorgangs im Allgemeinen praktisch unüberwindbar war und dieses Sicherheitsniveau auch im vorliegenden Fall bei Vornahme der strittigen Überweisung trotz der technischen Schwierigkeiten im EDV-System der Klägerin gewahrt worden ist.

79 a) Sollte das Ergebnis dieser Beweiserhebung nach Auffassung des Berufungsgerichts eine Anwendung des Anscheinsbeweises für die Autorisierung der Überweisung durch die Beklagte rechtfertigen, werden die von der Beklagten zu dessen Erschütterung angebotenen Beweise zu erheben sein. Dabei kann nach den Grundsätzen der sekundären Darlegungslast der Zahlungsdienstleister - hier die Klägerin - im Rahmen des Zumutbaren (Senatsurteil vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 320) gehalten sein, das verwendete Sicherheitssystem und eventuell bestehende weitere Sicherheitsvorkehrungen darzustellen, soweit dies nicht bereits im Rahmen der Begründung des Anscheinsbeweises geschehen ist. Dadurch soll der Zahler in die Lage versetzt werden, Beweis für von ihm vermutete konkrete Sicherheitsmängel antreten zu können (vgl. BGH, Urteile vom 15. Mai 2003 - III ZR 7/02, juris Rn. 15 und vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 320). Der Zahlungsdienstleister wird weiter auf Grundlage des Girovertrags in seinem Besitz befindliche technische Aufzeichnungen, die die streitigen sowie im selben Zeitraum ausgeführte Zahlungsvorgänge betreffen oder hierüber Aufschluss geben können, bis zur Klärung der Angelegenheit aufzuheben und sie dem Zahler gegebenenfalls zugänglich zu machen haben (Senatsurteil vom 5. Oktober 2004 - XI ZR 210/03, BGHZ 160, 308, 320 mwN).

80 b) Dem steht ein allgemeines Interesse der Kreditwirtschaft an der Geheimhaltung von Sicherungssystemen nicht entgegen. Einem im konkreten Einzelfall bestehenden berechtigten Geheimhaltungsinteresse des betroffenen Kreditinstituts an den technischen Grundlagen des von ihm eingesetzten Sicherungssystems kann in einem gerichtlichen Verfahren dadurch Rechnung getragen werden, dass nach § 172 Nr. 2 GVG die Öffentlichkeit ausgeschlossen wird und nach § 174 Abs. 3 GVG die Verfahrensbeteiligten zur Verschwiegenheit verpflichtet werden (vgl. dazu BGH, Urteil vom 9. Dezember 2015 - IV ZR 272/15, juris Rn. 9 ff.).

81 2. Stattdessen bzw. bei einem Scheitern eines Anscheinsbeweises kann der Zahlungsdienstleister - hier die Klägerin - eine Autorisierung des Zahlungsauftrags durch den Zahler im Wege des Vollbeweises nachweisen. Insoweit hat die Klägerin auch Beweis angeboten. In diesem Fall wird der Zahlungsdienstnutzer nach den Grundsätzen der sekundären Darlegungslast zu allen ihm bekannten Umständen, die den streitigen Zahlungsvorgang und dessen Autorisierung betreffen, insbesondere zu den Sicherheitsvorkehrungen auf dem für das Online-Banking genutzten Rechner und dem Mobiltelefon sowie zur Notierung, Speicherung oder Weitergabe der PIN substantiiert vorzutragen haben.

Ellenberger Maihold Menges

Derstadt Dauber

Vorinstanzen:
LG Lübeck, Entscheidung vom 07.06.2013 - 3 O 418/12 -
OLG Schleswig, Entscheidung vom 22.01.2014 - 5 U 87/13 -