

Anmerkung zu:	OLG Schleswig 5. Zivilsenat, Beschluss vom 29.10.2018 - 5 U 290/18
Autoren:	Dr. Franz Schnauder, RiOLG a.D., Dr. Anna-Maria Beesch, RA'in und FA'in für Bank -und Kapitalmarktrecht
Erscheinungsdatum:	09.04.2019
Quelle:	
Normen:	§ 432 ZPO, § 676c BGB, § 675 BGB, § 675I BGB, § 286 ZPO ... mehr
Fundstelle:	jurisPR-BKR 4/2019 Anm. 4
Herausgeber:	Prof. Dr. Stephan Meder, Universität Hannover Dr. Anna-Maria Beesch, RA'in und FA'in für Bank- und Kapitalmarktrecht
Zitiervorschlag:	Schnauder/Beesch, jurisPR-BKR 4/2019 Anm. 4

Zur Verteilung des Haftungsrisikos beim Online-Banking

Orientierungssätze

- 1. Grundsätzlich genügt ein Antrag auf Beiziehung von Akten nach § 432 ZPO nicht den gesetzlichen Erfordernissen, wenn die Partei nicht näher bezeichnet, welche Urkunden oder Aktenteile sie für erheblich hält (BGH, Urt. v. 09.06.1994 - IX ZR 125/93). Der Tatrichter ist nicht verpflichtet, von sich aus die Akten daraufhin zu überprüfen, ob sie Tatsachen enthalten, die einer Partei günstig sind; andernfalls betriebe er unzulässige Beweisermittlung.**
- 2. Bei § 675u BGB a.F. handelt es sich um eine verschuldensunabhängige Haftung. Damit obliegt es dem Zahlungsdienstleister, darzulegen und zu beweisen, dass es sich um ein außerhalb seines Einflussbereichs liegendes und auch bei Anwendung der gebotenen Sorgfalt nicht vermeidbares Ereignis handelte, welches zu der Durchführung der nicht autorisierten Überweisung führte.**
- 3. Bei missbräuchlicher Verwendung von PIN und TAN im Online-Banking rechtfertigen allein die Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die Prüfung der Authentifizierung i.S.v. § 675w Satz 3 Nr. 4 BGB die Anwendung der Grundsätze des Anscheinsbeweises für eine grob fahrlässige Pflichtverletzung des Zahlers nicht. Auch ein Anscheinsbeweis auf alternativer Grundlage, der Zahlungsdienstnutzer habe entweder den Zahlungsvorgang autorisiert oder aber grob fahrlässig gegen seine Pflichten aus § 675I Satz 1 BGB verstoßen, kommt deswegen nicht in Betracht (BGH, Urt. v. 26.01.2016 - XI ZR 91/14).**

A. Problemstellung

Das Haftungsregime des Zahlungsdiensterechts, das von dem Regelungs-dreieck der §§ 675u, 675v und 675w BGB bestimmt wird, geht von dem Grundsatz aus, dass dem Zahlungsdienstleister die Verantwortung obliegt, die Zahlungssysteme so sicher wie nur technisch möglich zu machen. Dies gilt gerade auch für Online-Banking-Systeme, die in besonderer Weise Missbrauchsrisiken ausgesetzt sind. Denn die Verwendung des Zahlungsauthentifizierungsinstruments (PSD 1) oder - wie es jetzt (PSD 2) heißt - des Zahlungsinstruments, erfolgt im Distanzgeschäft aus-

schließlich in der Sphäre und im Verantwortungsbereich des Zahlungsdienstnutzers, die außerhalb des Kontroll- und Einflussbereichs des Zahlungsdienstleisters liegen. Der Einsatz des Zahlungsinstruments und die Autorisierung des Zahlungsvorgangs durch den Zahler können daher vom Zahlungsdienstleister im Streitfall so gut wie niemals durch Vollbeweis nachgewiesen werden. Diesem Dilemma der Zahlungsdienstleister hat der BGH jedenfalls bei streitiger Autorisierung der Online-Überweisung unter engen Voraussetzungen durch das prozessrechtliche Institut des Anscheinsbeweises im Rahmen des § 286 ZPO abgeholfen. Der Besprechungsfall betrifft demgegenüber die (verschuldensabhängige) Missbrauchshaftung des Zahlungsdienstnutzers für unautorisierte Überweisungen. Dabei stellen sich Fragen nach dem möglichen Haftungstatbestand und dem Nachweis der Haftungsvoraussetzungen einschließlich möglicher Beweiserleichterungen.

B. Inhalt und Gegenstand der Entscheidung

Der Kläger, ein Einzelkaufmann, unterhielt bei der Beklagten ein Geschäftskonto, mit dem er seit 2011 am Online-Banking im smsTAN-Verfahren (auch sog. mobileTAN- oder mTAN-Verfahren) teilnahm. Er erhielt dazu eine persönliche Geheimzahl (PIN) und über die vereinbarte Mobilfunknummer die jeweils zur Freigabe einzelner Zahlungsanweisungen erforderliche Transaktionsnummer (TAN) per SMS.

Die der Mobilfunknummer des Klägers zugewiesene SIM-Karte funktionierte am Morgen des 30.08.2017 nicht mehr, was der Kläger sofort seinem Mobilfunkanbieter – dem späteren Streithelfer des Klägers –, nicht jedoch der beklagten Bank mitteilte. Tags darauf, am 31.08.2017, wurden vom Konto des Klägers in kurzen Abständen zwei Online-Überweisungen (um 11:36 Uhr in Höhe von 11.270 Euro und um 11:40 Uhr weitere 16.900 Euro) im smsTAN-Verfahren unter nicht näher geklärten Umständen an unbekannte Empfänger vorgenommen. Ungewöhnlich und bemerkenswert zugleich ist, dass der Kläger dies selbst sofort („noch am Vormittag“ des 31.08.2017) bemerkte und bei der Beklagten anzeigte. Diese konnte jedoch das Geld nicht wieder zurückerlangen, weil darüber bereits – ebenfalls sofort – nach Eingang beim Empfänger verfügt worden war. Nach dem Vortrag des Klägers hat er noch am 31.08.2017 die funktionsunfähige SIM-Karte auf Empfehlung seines Mobilfunkbetreibers vernichtet und gegen eine Zweitkarte ausgetauscht; die Originalkarte des Klägers wurde gesperrt. Die Beklagte behauptete, dass am 31.08.2017 um 11:29 Uhr, mithin sieben Minuten vor der ersten Missbrauchsverfügung, eine Ersatz-SIM-Karte auf den Namen des Klägers unter Verwendung von dessen Zugangsdaten durch den Mobilfunkanbieter aktiviert worden sei, die dieser jedoch nicht versandt habe. Nach Freischaltung seien die an die Rufnummer des Klägers gesendeten SMS mit den TANs von Unbekannten abgefangen und umgeleitet worden.

Da die unautorisierte Kontobelastung außer Streit stand, hat das LG Kiel dem Klagebegehren auf Erstattung des Überweisungsbetrags von insgesamt 28.170 Euro gemäß § 675u Satz 2 BGB a.F. stattgegeben (LG Kiel, Urt. v. 22.06.2018 - 12 O 562/17). Der zur Aufrechnung gestellte Schadensersatzanspruch der Beklagten sei unter keinem rechtlichen Gesichtspunkt gegeben, denn für die streitigen Zahlungsvorgänge greife keiner der Haftungstatbestände des § 675v BGB a.F. ein.

Die rechtliche Prüfung des Landgerichts setzte bei der verschuldensunabhängigen, auf 150 Euro beschränkten Basishaftung des Zahlungsdienstnutzers gemäß § 675v Abs. 1 Satz 1 BGB a.F. an. Diese Haftung scheide schon deswegen aus, weil die Beklagte nicht geltend mache (und auch nicht geltend machen könne), dass dem Kläger ein Zahlungsauthentifizierungsinstrument abhandengekommen sei. Lediglich die SIM-Karte des Mobiltelefons des Klägers habe nicht mehr funktioniert. Mögliche Pflichtverstöße des Mobilfunkanbieters im Zusammenhang mit der vertragswidrigen Freischaltung der Ersatz-SIM-Karte müsse sich der Kläger gemäß § 278 BGB nicht zurechnen lassen. Ebenso wenig liege ein Haftungsfall nach § 675v Abs. 1 Satz 2 BGB a.F. vor. Dem Kläger

sei nicht der Vorwurf fahrlässigen Umgangs mit personalisierten Sicherheitsmerkmalen zu machen. Dass der Kläger die PIN unsicher aufbewahrt habe, könne nach seiner Schilderung im Rahmen der sekundären Darlegungslast nicht festgestellt werden. Die TAN selbst sei weder vom Kläger noch vom Mobilfunkanbieter „aufbewahrt“ worden.

Insbesondere sei auch eine uneingeschränkte Haftung des Klägers wegen grob fahrlässiger Verletzung seiner Pflichten aus § 675I Satz 1 BGB a.F. nicht gegeben, § 675v Abs. 2 Nr. 1 BGB a.F. Es fehle schon am Nachweis, dass der Kläger zumutbare Vorkehrungen zum Schutz von PIN und TAN unterlassen habe und dass ihm insoweit der Vorwurf eines qualifizierten Verschuldens gemacht werden könne. Die Beklagte könne sich hierfür nicht auf den Beweis des ersten Anscheins stützen, vielmehr obliege ihr der Nachweis einer schuldhaften Pflichtverletzung des Klägers. Dies folge auch aus § 675w Satz 4 BGB a.F. (!), der „unterstützende Beweismittel“ für den Nachweis des Verschuldens verlange.

Ebenso wenig sei eine grob fahrlässige Pflichtverletzung in Bezug auf die Pflicht zur unverzüglichen Anzeige der missbräuchlichen Verwendung eines Zahlungsinstrumentes gegeben, § 675v Abs. 2 Nr. 1 i.V.m. § 675I Satz 2 BGB a.F. Insoweit fehle es schon an der Kenntnis des Klägers von einer missbräuchlichen Verwendung oder der nicht autorisierten Nutzung eines Zahlungsinstrumentes. Die Behauptung des Klägers, er sei nur von einer technischen Störung der SIM-Karte ausgegangen, sei nicht widerlegt. Schließlich könne die Beklagte Schadensersatz wegen Verstoßes gegen ihre vertraglichen Bedingungen zur Nutzung des Online-Banking nicht beanspruchen, weil die AGB der Beklagten nicht Vertragsinhalt geworden seien.

Mit ihrer Berufung verfolgte die Beklagte ihr Prozessziel auf Klageabweisung weiter. Sie rügte, der Einzelrichter des Landgerichts habe einen Gehörsverstoß begangen, weil er ihrem Begehren auf Beiziehung der strafrechtlichen Ermittlungsakte nicht nachgekommen sei. Im Übrigen seien die Ansprüche des Klägers schon nach § 676c Nr. 1 BGB a.F. ausgeschlossen.

Die Berufung der Beklagten hatte vor dem OLG Schleswig keinen Erfolg.

Das Oberlandesgericht erkannte weder einen Verfahrensverstoß noch einen materiell-rechtlichen Fehler des angegriffenen Urteils und hat daher mit ausführlicher Begründung im wesentlichen unter Wiederholung der vom Landgericht erwogenen Gesichtspunkte die Berufung als offensichtlich unbegründet zurückgewiesen.

C. Kontext der Entscheidung

Die Angriffe von Betrügern auf das Online-Banking sind vielfältig und werden technisch immer weiter verfeinert. Wenn Manipulationen am PC des Kontoinhabers und an seinem Mobiltelefon erfolgen, hängt die Schadensverteilung zwischen Zahlungsdienstleister und Zahler maßgeblich davon ab, ob der Zahlungsdienstleister einen aufrechenbaren Schadensersatzanspruch aus § 675v BGB gegen den Zahler hat (I.). Die immer ausgefeilteren Methoden des Missbrauchs von Zahlungsinstrumenten führen gerade bei dem im Streitfall unternommenen Angriff auf das Zahlungssystem mittels einer Ersatz-SIM-Karte häufig dazu, dass den Zahlungsdienstnutzern der Vorwurf der haftungsbegründenden Verletzung einer verhaltensbezogenen Sorgfaltspflicht nicht gemacht werden kann, so dass eine Missbrauchshaftung ausscheidet (II.).

I. Das Haftungskonzept des Zahlungsdienstrechts

Die im Zahlungsdienstrecht aufgestellten (und von PSD 2 modifizierten) Haftungsregeln begrenzen tendenziell den Rückgriffsanspruch des Zahlungsdienstleisters im Fall einer durch Missbrauch des Zahlungsinstrumentes verursachten Belastung des Kundenkontos (1.). Darüber hinaus obliegt es dem Zahlungsdienstleister, die Voraussetzungen des in Betracht kommenden Haftungstatbe-

standes darzutun und nachzuweisen, was gerade bei Online-Überweisungen auf große Schwierigkeiten stößt (2.).

1. Haftungstatbestände

Ist ein Zahlungsvorgang aufgrund eines betrügerischen Angriffs auf das Authentifizierungsverfahren erfolgt und daher vom Zahler nicht autorisiert, haftet ihm der Zahlungsdienstleister dafür nach § 675u BGB. Ausgleich für den aufgewendeten Zahlbetrag kann der Dienstleister vom Zahlungsdienstnutzer nur im Wege eines Schadensersatzanspruchs gemäß § 675v BGB erlangen. Danach besteht lediglich eine auf 150 Euro begrenzte (und seit 13.01.2018 auf 50 Euro reduzierte) Basishaftung des Zahlungsdienstnutzers, § 675v Abs. 1 BGB. Eine unbegrenzte Haftung (freilich innerhalb des Verfügungsrahmens des Zahlungsinstruments) sieht das Gesetz in § 675v Abs. 2 BGB a.F. (= § 675v Abs. 3 BGB n.F.) nur bei qualifiziertem Verschulden des Zahlungsdienstnutzers vor.

Dieses nach Maßgabe des § 675e Abs. 1 BGB abschließende Haftungskonzept zur Verteilung des Risikos bei nicht autorisierten Zahlungen unter Einsatz eines Zahlungsinstruments beruht zum großen Teil auf den früher für Zahlungskarten geltenden vertraglichen Regeln, die das Zahlungsdienstrecht auf alle Zahlungsinstrumente ungeachtet ihrer Heterogenität ausgedehnt hat. Die tatbestandlichen Voraussetzungen der (bislang verschuldensunabhängigen) Basishaftung nach § 675v Abs. 1 Satz 1 BGB a.F. orientieren sich an dem Einsatz von Zahlungskarten (körperliche Gegenstände), die verloren gehen oder abhanden kommen können. Beim Online-Banking konnte bisher nur der sorgfaltswidrige Verlust von personalisierten Sicherheitsmerkmalen die betraglich begrenzte Missbrauchshaftung des Zahlungsdienstnutzers begründen, § 675v Abs. 1 Satz 2 BGB a.F. Dieser Haftungstatbestand ist de lege lata (PSD 2) entfallen, nachdem die Basishaftung nunmehr generell einen speziellen Verschuldensvorwurf gemäß § 675 Abs. 2 Nr. 1 BGB n.F. voraussetzt. Ob allerdings mit dem auf die symbolische Schadenssumme begrenzten Schadensersatzanspruch des Zahlungsdienstleisters ein nennenswerter Anreiz für den Zahlungsdienstnutzer zum sorgsamem Umgang mit seinem Zahlungsinstrument erreicht wird (zum Gesetzeszweck vgl. Hofmann, BKR 2018, 62, 64), mag mit Fug und Recht bezweifelt werden. Das gilt nun umso mehr, als der ersatzfähige Schaden „zum Schutz der Zahler“ (BT-Drs. 18/11495, S. 165) auf 50 Euro reduziert wurde. Diese vom europäischen und deutschen Gesetzgeber detailliert geregelte Basishaftung spielt im Schadensrecht praktisch keine Rolle. Die beklagte Bank machte im Besprechungsfall (vgl. Rn. 51) diese Haftung auch ausdrücklich nicht (mehr) geltend.

Im Fall der Nichtautorisierung des Zahlungsvorgangs ist vielmehr die unbegrenzte und vorrangige (Beesch in: NK-BGB, 3. Aufl. 2016, §§ 675v, 675w Rn. 4; Omlor in: Staudinger, BGB, Neubarb. 2012, Stand: 20.11.2017, § 675v Rn. 18: „lex specialis“) Missbrauchshaftung des Zahlungsdienstnutzers gemäß § 675v Abs. 2 BGB a.F. (= § 675v Abs. 3 BGB n.F.) von prozessentscheidender Bedeutung. Diese Einstandspflicht setzt allerdings voraus, dass der Zahlungsdienstnutzer den Schaden in betrügerischer Absicht ermöglicht oder durch vorsätzliche oder grob fahrlässige Verletzung von Sorgfaltspflichten in Bezug auf Zahlungsinstrumente herbeigeführt hat. Haftungsbegründende Sorgfaltspflichten des Zahlers stellt das Gesetz in § 675l BGB auf, wonach der Zahler u.a. die personalisierten Sicherheitsmerkmale der ihm zugesandten Zahlungsinstrumente nach Erhalt vor unbefugtem Zugriff Dritter zu schützen hat. Weitere Pflichten des Zahlungsdienstnutzers können sich aus den AGB der Zahlungsdienstleister ergeben, die den sorgfältigen Umgang mit Zahlungsinstrumenten wie auch Bedingungen für die Ausgabe und Nutzung von Zahlungsinstrumenten zum Zwecke der Begrenzung des Missbrauchsrisikos regeln, § 675v Abs. 2 Nr. 2 BGB a.F. (= § 675v Abs. 3 Nr. 2 Buchst. b BGB n.F.).

Sichere Verwahrung i.S.d. § 675l BGB bedeutet zunächst einmal nach dem freilich nicht unumstrittenen weiten Normverständnis der h.M., dass der Zahlungsdienstnutzer beim Online-Banking

seinen Computer vor unberechtigten Zugriffen durch spezielle Computerprogramme und beim Mobile Banking durch entsprechende Sicherung des Smartphones schützen muss (Jungmann in: MünchKomm BGB, 7. Aufl. 2017, § 675I Rn. 28 ff.). Die personalisierten Sicherheitsmerkmale (PIN und TAN) unterliegen in jedem Fall mit Zugang beim Zahlungsdienstnutzer einer strikten Geheimhaltungspflicht. Darüber hinaus wird aus § 675I Satz 1 BGB a.F. (= § 675I Abs. 1 Satz 1 BGB n.F.) die spezifische Pflicht des Zahlungsdienstnutzers beim Mobile Banking hergeleitet, die zusammen mit der TAN per SMS gesendeten Rahmendaten des Zahlungsauftrags zu überprüfen und sich vor Erteilung des Auftrags am PC zu vergewissern, dass die Autorisierung mittels der TAN tatsächlich für den in der SMS-Nachricht angegebenen Zweck erfolgt (Jungmann, EWiR 2017, 745, 746; Jungmann in: MünchKomm BGB, § 675I Rn. 55; Sprau in: Palandt, BGB, 78. Aufl. 2019, § 675v Rn. 5 a.E.). Die Missachtung dieser konkreten Sorgfaltsanforderungen begründet die Haftung des Zahlungsdienstnutzers wegen grob fahrlässiger Pflichtverletzung (vgl. dazu z.B. OLG Oldenburg, Beschl.v. 21.08.2018 - 8 U 163/17; LG Köln, Urte. v. 26.08.2014 - 3 O 390/13 Rn. 23 - NJW 2014, 3735 = WM 2014, 2372; LG Darmstadt, Urte. v. 28.08.2014 - 28 O 36/14 Rn. 43 f.: zu Unrecht als Rechtscheinhaftung qualifiziert, wie Omlor, EWiR 2014, 701, 702 zutreffend bemerkt; a.A. Schwintowski in: jurisPK-BGB, 8. Aufl. 2017, § 675w, 1. Überarbeitung, Rn. 8; eine Haftung des Zahlers bejaht auch LG Oldenburg, Urte. v. 15.01.2016 - 8 O 1454/15; ebenso OLG Karlsruhe, Urte. v. 22.03.2016 - 17 U 97/15 n.v.).

2. Beweisanforderungen

Die schadensrechtliche Anspruchsgrundlage hilft dem nach § 675u BGB haftenden Zahlungsdienstleister jedoch nur, wenn er im Prozess die Anspruchsvoraussetzungen nachweisen kann. Dabei greift die Beweisregel des § 675w BGB ein, die Mindestanforderungen für die Beweislast beim Nachweis von Autorisierung und Pflichtverletzung des Zahlers normiert. Die weiteren Anforderungen an die Beweisführung sind Gegenstand eines lebhaften Streits, der seit Inkrafttreten des neuen Zahlungsdienstrechts geführt wird und nunmehr durch § 675w Satz 4 BGB n.F. neue Nahrung erhalten hat.

Nach der Grundnorm des § 675w Satz 1 BGB (a.F. und n.F.) hat der Zahlungsdienstleister zunächst die durchgeführte Authentifizierung und die ordnungsgemäße Aufzeichnung der Zahlungsvorgangs, die Verbuchung sowie den störungsfreien technischen Ablauf darzutun und durch entsprechende Protokolle zu belegen. Fehlt es bereits daran, ist vorbehaltlich einer gegenteiligen Beweisführung des Zahlungsdienstleisters (str., vgl. Zetzsche in: MünchKomm BGB, 7. Aufl. 2017, § 675w Rn. 5) von einer nicht autorisierten Zahlung auszugehen. Kann der Zahlungsdienstleister einen in technischer Hinsicht störungsfreien Zahlungsvorgang nachweisen, so spricht für die Autorisierung des Zahlungsdienstnutzers eine gewisse Vermutung (Beesch in: NK-BGB, §§ 675v, 675w Rn. 5, 23 ff., 29 ff.; Sprau in: Palandt, BGB, § 675w Rn. 4), die jedoch nach § 675w Satz 3 BGB „allein nicht notwendigerweise“ zum Nachweis der Autorisierung ausreicht. Diese kryptische Formulierung des europäischen Gesetzgebers soll nach allgemeiner Meinung zum Ausdruck bringen, dass an den bloßen Nachweis der Authentifizierung durch Verwendung von PIN und TAN nicht die unwiderlegliche Vermutung geknüpft werden darf, der Zahler habe selbst die Zahlung autorisiert oder für sie nach § 675v BGB einzustehen (Hofmann, BKR 2018, 62, 68 m.w.N.). Der § 675w Satz 3 BGB erfordert vielmehr die Berücksichtigung der Gesamtumstände des Einzelfalls bei der richterlichen Beweiswürdigung gemäß § 286 ZPO (Beesch in: NK-BGB, §§ 675v, 675w Rn. 39).

Der beweisrechtliche Vorbehalt des Gesetzes schließt daher, wie der BGH entschieden hat, die Anwendung der Grundsätze des Anscheinsbeweises auch beim Online-Banking nicht von vornherein aus, weil damit weder eine zwingende Beweisregel noch eine Beweisvermutung oder gar eine Beweislastumkehr begründet wird (BGH, Urte. v. 26.01.2016 - XI ZR 91/14 Rn. 24 - BGHZ 208, 331

= NJW 2016, 2024 m. Anm. Blissenbach, jurisPR-BKR 5/2017 Anm. 3). Diese Beweiserleichterung kommt dem Zahlungsdienstleister allerdings nur unter der zusätzlichen Voraussetzung zugute, dass er ein Zahlungssystem verwendet, das technisch so sicher wie möglich ist. Der Zahlungsdienstleister muss deshalb nachweisen, dass das von ihm verwendete Sicherheitssystem allgemein praktisch nicht überwindbar war, im konkreten Einzelfall ordnungsgemäß angewendet worden ist und fehlerfrei funktioniert hat (BGH, Urt. v. 26.01.2016 - XI ZR 91/14 Rn. 19 - BGHZ 208, 331 = NJW 2016, 2014; dazu kritisch Hoffmann/Hauptert/Freiling, ZHR 181, 780, 788 (2017) ff.).

Die Grundsätze des Anscheinsbeweises, die der XI. Zivilsenat des BGH schon vor Inkrafttreten des Zahlungsdienstrechts für kartengestützte Zahlungsvorgänge entwickelt hat (BGH, Urt. v. 05.10.2004 - XI ZR 210/03 - BGHZ 160, 308 = NJW 2004, 3623 m. Anm. Schott, jurisPR-BGHZivilR 51/2004 Anm. 2; bestätigt durch BGH, Urt. v. 14.11.2006 - XI ZR 294/05 Rn. 31 - BGHZ 170, 18 = NJW 2007, 593 m. Anm. Meder/Beesch, EWiR 2007, 135), sind von ihm mit den genannten Modifikationen auf das Online-Banking übertragen worden, bisher beschränkt auf das Vorliegen einer Autorisierung des Überweisungsvorgangs (BGH, Urt. v. 26.01.2016 - XI ZR 91/14 Rn. 32 ff. - BGHZ 208, 331 = NJW 2016, 2024). Gelingt es jedoch dem Zahlungsdienstnutzer, die Grundlagen des Anscheinsbeweises durch Darlegung eines atypischen Geschehensablaufes zu erschüttern, hat der Zahlungsdienstleister die Autorisierung nachzuweisen.

Dagegen hat der BGH - anders als bei unberechtigter Nutzung von Zahlungskarten oder Kreditkarten am Geldautomaten oder im Präsenzggeschäft, wo typischerweise auf ein bestimmtes Fehlverhalten des Zahlungsdienstnutzers geschlossen werden kann (BGH, Urt. v. 29.11.2011 - XI ZR 370/10 - NJW 2012, 1277 m. Anm. Beesch/Willershausen, jurisPR-BKR 9/2012 Anm. 1) - beim Online-Banking entschieden, dass der Beweis des ersten Anscheins zum Nachweis grob fahrlässiger Pflichtverletzungen des Zahlers zwar grundsätzlich zulässig ist, jedoch nicht beim Online-Banking im smsTAN-Verfahren (bei dem ein über eine Banking-App verfügendes Mehrzweckgerät = Smartphone verwendet wird; weiterführend vgl. Omlor, BKR 2019, 105, 109). Denn bei Online-Überweisungen bestehen wegen der ganz unterschiedlichen Angriffsmöglichkeiten auf die Sicherheitsstrukturen der einzelnen Authentifizierungsverfahren keine Erfahrungssätze, die es erlauben, ein bestimmtes tatsächliches Verhalten des Zahlungsdienstnutzers zugrunde zu legen und sodann als grob fahrlässig zu bewerten (BGH, Urt. v. 26.01.2016 - XI ZR 91/14 Rn. 74 f. - BGHZ 208, 331 = NJW 2016, 2024). Daher scheidet für den Nachweis der subjektiven Voraussetzungen eines Schadensersatzanspruchs nach § 675v BGB (gravierendes individuelles Versagen) der Anscheinsbeweis mangels Typizität des Kundenverhaltens und des Geschehensablaufs aus (kritisch Hoffmann/Hauptert/Freiling, ZHR 181, 780, 785 (2017) ff.; Herresthal, JZ 2017, 28). Allerdings lässt sich z.B. bei Verwendung des ChipTAN-Verfahrens derzeit ein Anscheinsbeweis grundsätzlich annehmen (Omlor, BKR 2019, 105, 109 m.w.N.).

Diese Rechtsprechungsgrundsätze legte auch das damalige Berufungsgericht (ebenfalls der 5. Zivilsenat des OLG Schleswig) nach Zurückverweisung durch den BGH (Urt. v. 26.01.2016 - XI ZR 91/14 - BGHZ 208, 331 = NJW 2016, 2024) zugrunde. Im wieder eröffneten Berufungsrechtszug entschied das OLG Schleswig nach Beweislastgrundsätzen, dass der Zahlungsdienstleister im Zweifel auch die Folgen von nicht weiter aufklärbaren kriminellen Machenschaften trägt, weil es eine hinreichende Überzeugung von der betrügerischen Absicht des Zahlers - die im dortigen Fall beinahe schon mit Händen zu greifen war - nicht gewinnen konnte (OLG Schleswig, Urt. v. 09.03.2017 - 5 U 87/13 Rn. 46 ff.).

An dieser Rechtslage hat die Umsetzung der Zweiten Zahlungsdienstrichtlinie (PSD 2) mit Wirkung vom 13.01.2018 nichts geändert. Der Anscheinsbeweis bei Drittmisbrauch ist weiterhin zulässig. Soweit Art. 72 Abs. 2 PSD 2 (umgesetzt in § 675w Satz 4 BGB n.F.) durch einen weiteren Satz ergänzt wurde, wonach der Zahlungsdienstleister „unterstützende Beweismittel vorlegen

muss, um Betrug, Vorsatz oder grobe Fahrlässigkeit des Zahlungsdienstnutzers nachzuweisen“, entspricht dies der bisherigen deutschen Rechtslage wie auch der höchstrichterlichen Rechtsprechung und ändert an der Beweislastverteilung nichts (so auch Omlor, BKR 2019, 105, 110 mit weitergehender Begründung; Linardatos, NJW 2017, 2145, 2150; Hofmann, BKR 2018, 62, 68 f; Zahrte, NJW 2018, 337, 340; Zetzsche in: MünchKomm BGB, § 675w Rn. 32). Unrichtigerweise hatte sich das LG Kiel in dem hier angegriffenen streitigen Urteil zur Begründung ausdrücklich auf die neue Vorschrift des § 675w Satz 4 BGB n.F. (nicht „a.F.“) gestützt, obwohl diese auf den Streitfall nicht einmal Anwendung fand (Art. 229 § 45 Abs. 2 EGBGB). Darauf ist das OLG Schleswig in dem vorliegend besprochenen Beschluss nicht eingegangen.

II. Missbrauchshaftung bei Angriff mittels einer Ersatz-SIM-Karte

Nach den unter I.2. dargestellten Vorgaben der BGH-Rechtsprechung ist im vorliegenden Fall, in dem das smsTAN-Verfahren genutzt wurde, nicht zu beanstanden, dass das OLG Schleswig, wie schon die Vorinstanz, mangels Typizität des Geschehensablaufs die Anscheinsbeweis-Grundsätze nicht angewendet und den Zahlungsdienstleister antragsgemäß verurteilt hat (1.). Allenfalls wäre eine Haftung aufgrund der Vertragsbedingungen in Betracht gekommen (2.).

1. Nachweislast des Zahlungsdienstleisters

Der Missbrauch des Zahlungsinstruments erfolgte im vorliegenden Fall durch eine relativ neue kriminelle Vorgehensweise, bei der sich der Angreifer nach Ausspähen der PIN durch Infektion des PC eine Ersatz-SIM-Karte beim Mobilfunkbetreiber des Kontoinhabers erschleicht, mittels derer er das personalisierte Sicherheitsmerkmal (TAN) abfängt (vgl. Hoffmann/Hauptert/Freiling, ZHR 181, 780, 798 (2017) ff.; Zahrte, NJW 2018, 337). Im zweiten, wie schon im erstinstanzlichen Rechtszug, konnten im vorliegenden Fall Herkunft und Verbleib der Ersatz-SIM-Karte, die nach dem Vortrag der Beklagten gerade einmal sieben Minuten vor der ersten missbräuchlichen Online-Überweisung vom Mobilfunkanbieter des Klägers aktiviert worden war, nicht geklärt werden.

Da der Kläger in der gegebenen Konstellation das personalisierte Sicherheitsmerkmal (TAN) bereits nicht auf sein Mobiltelefon erhalten hat, treffen ihn auch keine Sorgfaltspflichten in Bezug auf die Geheimhaltung und die Verwendung des Zahlungsinstruments. Vielmehr wurde die TAN in raffinierter, jedenfalls ungeklärter Weise auf eine externe SIM-Karte unbekannter Dritter geleitet, die für den Kläger nicht freigeschaltet und ihm daher auch nicht zugänglich war. Infolgedessen war anzunehmen, dass die streitige Überweisung von ihm auch nicht autorisiert war. Für einen Anscheinsbeweis ist hier nach Auffassung des BGH kein Raum, weil dem Zahlungsvorgang kein typischer Geschehensablauf zugrunde liegt, auf dessen Grundlage nach der Lebenserfahrung eine sehr hohe Wahrscheinlichkeit für eine grob fahrlässige Pflichtverletzung des Klägers besteht. Daran ändert nach Auffassung des BGH auch der Umstand nichts, dass der Missbrauch des Online-Banking auf einem Umstand aus der Sphäre des Zahlers beruht (BGH, Urt. v. 26.01.2016 - XI ZR 91/14 Rn. 73 - BGHZ 208, 331 = NJW 2016, 2024). Auch wenn man die Rechtslage differenzierter betrachtet, steht nach derzeitigem Rechtsprechungsstand dem Anscheinsbeweis im Streitfall zumindest der Umstand entgegen, dass das eingesetzte Sicherheitssystem bei dem smsTAN-Verfahren aus technischer Sicht nicht als „allgemein praktisch nicht zu überwinden“ erachtet wird (dazu Hoffmann/Hauptert/Freiling, ZHR 181, 780, 795, 798 (2017)).

Allerdings handelte der Streithelfer (Mobilfunkanbieter) durch die Ausgabe und Freischaltung einer Ersatz-SIM-Karte an einen unbekanntem Dritten im Rechtsverhältnis zu seinem Kunden grob vertragswidrig und schuldhaft (unverständlich daher Besprechungsentscheidung Rn. 57). Indes kann dieses grobe Verschulden dem Zahlungsdienstnutzer nicht gemäß § 278 BGB im Verhältnis zu seinem Zahlungsdienstleister zugerechnet werden. Der Mobilfunkanbieter wird nicht im Kreis der Sorgfaltspflichten des Zahlers gegenüber dem Zahlungsdienstleister tätig (Zahrte, NJW

2018, 337). Auch bei der (elektronischen) Übermittlung der SMS mit der TAN handelt der Zahlungsdienstleister auf eigenes Risiko, § 675m Abs. 2 BGB.

Danach traf den beklagten Zahlungsdienstleister im Streitfall die Darlegungs- und Beweislast für die objektiven und subjektiven Voraussetzungen des Schadensersatzanspruchs aus § 675v Abs. 2 BGB a.F. Dieser Vorgabe konnte die Beklagte nicht genügen. Der bloße Umstand, dass die richtige PIN und die jeweils dem Überweisungsvorgang zugeordnete TAN benutzt worden waren, half der Beklagten bei der Begründung des geltend gemachten Schadensersatzanspruchs nicht.

Allerdings ist der Rechtsschutz der Beklagten damit nicht erschöpft. Die Beklagte ist nicht schutzlos; sie kann sich nach Erstattung des Abbuchungsbetrages gemäß § 675u Satz 2 BGB an den Kläger bei dem Streithelfer (Mobilfunkanbieter) im Wege der Drittschadensliquidation schadlos halten (näher dazu Zahrtte, NJW 2018, 337).

2. Verletzung von Vertragsbedingungen

Im Streitfall hat sich die beklagte Bank auch (allerdings ausdrücklich offenbar nur vor dem Landgericht) darauf berufen, dass den Kläger nach ihren AGB die Pflicht treffe, bereits die bloße Gefahr einer missbräuchlichen Nutzung des Online-Banking anzuzeigen, wie sie etwa bei einer technischen Störung der SIM-Karte gegeben sei. Darüber hinaus sei in den Bedingungen für das Online-Banking insbesondere eine Haftung schon für einfache Fahrlässigkeit für den Fall vorgesehen, dass der Kunde – was hier zutrefte – kein Verbraucher sei.

Es besteht Streit darüber, ob § 675e Abs. 4 BGB gestattet, die in § 675v BGB geregelte Missbrauchshaftung des unternehmerischen Zahlungsdienstnutzers formularvertraglich unter der Schwelle der groben Fahrlässigkeit eintreten zu lassen (dazu Omlor, BKR 2019, 105, 106; Omlor in: Staudinger, BGB, 2012, Stand: 20.11.2017, § 675e Rn. 10; Zetzsche in: MünchKomm BGB, § 675v Rn. 8). Das Landgericht hatte (rechtlich bedenklich) eine Haftung des Klägers jedenfalls mit der Begründung scheitern lassen, die Einbeziehung der AGB in den Zahlungsdienstvertrag sei nicht gemäß § 305 Abs. 2 BGB nachgewiesen. Die rechtsgeschäftliche Einbeziehung von AGB gegenüber einem Unternehmer setzt das Erfordernis des § 305 Abs. 2 BGB nicht voraus, § 310 Abs. 1 Satz 1 BGB. Im Ergebnis aber hatte das Landgericht einen Verweis der Beklagten auf ihre AGB nicht festzustellen vermocht, weil die Beklagte insoweit beweisfällig blieb. Damit schied eine Haftung des Klägers wegen Verletzung seiner etwaigen vertraglichen Sorgfaltspflichten im Online-Banking von vornherein aus. Dieser Teil des Urteils ist von der Berufung offenbar nicht angegriffen worden.

D. Auswirkungen für die Praxis

Der Zurückweisungsbeschluss des OLG Schleswig, wie auch das erstinstanzliche Urteil des LG Kiel, befinden sich im Einklang mit der BGH-Rechtsprechung. Art. 72 Abs. 2 Satz 2 PSD 2, den § 675w Satz 4 BGB n.F. abbildet, begründet eine Obliegenheit für den Zahlungsdienstleister, zum Nachweis von Betrug, Vorsatz oder grober Fahrlässigkeit des Zahlungsdienstnutzers „unterstützende Beweismittel“ vorzulegen. An der bisherigen Rechtslage, insbesondere zur Zulässigkeit eines Anscheinsbeweises bei Drittmissbrauch, ändert sich dadurch nichts.

Ebenso wie bereits der Satz 3 des § 675w BGB hat auch die in Umsetzung der PSD 2 erfolgte Einfügung des neuen § 675w Satz 4 BGB erneut allgemeine Verunsicherung in der Rechtspraxis verursacht. In der Literatur hat das Rätselraten über die ratio legis des § 675w Satz 4 BGB schon begonnen (vgl. etwa Linartados, NJW 2017, 2145, 2149 f.: „unsinnige Vorgabe“; Werner, WM 2018, 449, 453: „offen“, „unklar“; Hofmann, BKR 2018, 62, 69; Zahrtte, NJW 2018, 337: „Klarstellung“). Allgemein ist man jedoch der Auffassung, dass der in § 675w BGB eingefügte Satz 4 lediglich die Vorgabe von Satz 3 konkretisieren soll, so dass die vom BGH zusätzlich aufgestellten Anforderungen für das Eingreifen des Anscheinsbeweises den gesetzlichen Beweisanforderungen ohne wei-

teres genügen. In der Literatur wird jedoch die Beschränkung der Nachweisregel auf die subjektiven Voraussetzungen des Schadensersatzanspruchs des § 675v Abs. 3 BGB n.F. kritisiert (vgl. nur Linartados, NJW 2017, 2145, 2147: „widersinnig“; Zetsche in: MünchKomm BGB, § 675w Rn. 32; Hoffmann/Hauptert/Freiling, ZHR 181, 780, 786 f.). Um die (gewünschte) Weitergeltung des Anscheinsbeweises zu sichern, konstruiert etwa Linartados einen „kollektiven Motivirrtum“ des Gesetzgebers, der es rechtfertige, § 675w Satz 4 BGB n.F. ohne Rücksicht auf seinen Wortlaut auch für den Nachweis der Autorisierung anzuwenden (Linartados, NJW 2017, 2145, 2150).

Demgegenüber wird man am Gesetzeswortlaut und an den üblichen Auslegungsmethoden nicht vorbeikommen. Der Zweck des § 675w Satz 4 BGB n.F. besteht ersichtlich darin zu verhindern, dass die vom Gesetz aufgestellte hohe Schwelle des qualifizierten Verschuldens bei der Missbrauchshaftung des Zahlungsdienstnutzers durch großzügige Beweiserleichterungen ohne Rücksicht auf die Besonderheiten des Einzelfalles unterlaufen wird (so richtig Linartados, NJW 2017, 2145, 2149). Dem Gesetzgeber ging es offensichtlich allein darum, einem Haftungsautomatismus zulasten des Zahlungsdienstnutzers entgegenzuwirken. Diesem Ziel wird die BGH-Rechtsprechung jedoch schon mit der falldifferenzierten Anwendung des Anscheinsbeweises gerecht, die unter Berücksichtigung des Umstandes, dass die unterschiedlichen Zahlungsinstrumente nicht das gleiche Sicherheitsniveau aufweisen, das jeweilige Verhalten des Zahlungsdienstnutzers in den Blick nimmt. Die BGH-Rechtsprechung beugt damit gerade der vom Gesetzgeber inkriminierten schematischen Beweislastverteilung vor. Sie fordert nämlich unterstützende Nachweise für die Annahme des Anscheinsbeweises bezüglich der Sicherheit und Funktionsfähigkeit des Sicherheitssystems. Nur bei Ausfall oder Erschütterung des Anscheinsbeweises muss der Zahlungsdienstleister „unterstützende Beweismittel vorlegen“. Letzteres kann sich allerdings naturgemäß nur auf dem Zahlungsdienstleister erreichbare Nachweise beziehen (wie z.B. Dokumente mit widersprüchlichen Angaben des Zahlungsdienstnutzers in Zusammenhang mit den streitigen Transaktionen, Dokumente zu dessen krimineller Vergangenheit, Strafanzeigen oder Auszüge aus den Strafakten, etc.). Hier bleibt es notwendig, zwischen den Sphären und Verantwortungsbereichen des Zahlungsdienstleisters und des Zahlungsdienstnutzers zu unterscheiden und die „unterstützenden Beweismittel“ auf diejenigen zu beschränken, die der Zahlungsdienstleister aus seiner Sphäre und seinem Verantwortungsbereich zu erlangen in der Lage ist.

In dem nach Einfügung des Satzes 4 in § 675w BGB neuerlich drohenden Streit um die Fortgeltung des Anscheinsbeweises sprechen daher gute Gründe für die Beibehaltung der bisherigen ausgewogenen Rechtsprechung (Hofmann, BKR 2018, 62, 69; Omlor, BKR 2019, 105, 110). Dafür kann nicht zuletzt auch der Erwägungsgrund 72 Satz 2 PSD 2 angeführt werden: „Ob und in welchem Maße fahrlässig gehandelt wurde, sollte nach nationalem Recht beurteilt werden“.

In der Praxis zeigt sich, dass die Trennlinie zwischen einem tatsächlich haftungsbegründenden fahrlässigen Fehlverhalten eines Zahlungsdienstnutzers und einem Ausnutzen der Haftungslage etwa auch durch kollusives Zusammenwirken mit unbefugten Dritten schwer zu ziehen ist und ggf. enormen prozessualen Aufwand erfordert – wie auch die vorliegende Fallkonstellation zeigt. Zahlungsdienstleister sollten daher im Prozess den vom Zahlungsdienstnutzer behaupteten Mangel der Autorisierung nicht vorschnell zugestehen, weil ihnen hier (im Rahmen des § 675u Satz 1 BGB) auf jeden Fall der Anscheinsbeweis zugute kommt.