WM WERTPAPIER-MITTEILUNGEN Zeitschrift für Wirtschafts- und Bankrecht
12
21. März 2015
69. Jahrgang
Seiten 549-596

Der Anscheinsbeweis im Bankenbereich – aktuelle Entwicklungen

Von Univ.-Prof. Dr. Thomas Hoeren und wiss. Mitarbeiterin Maria Kairies, Münster

A. Einführung

Die Banken sehen sich seit Jahren mit der Frage konfrontiert, wie man angesichts der heutigen Phishing-Risiken die Darlegungs- und Beweislast für die missbräuchliche Nutzung von chipTAN-Verfahren regeln soll. § 675w Satz 3 BGB schreibt vor, dass der Einsatz eines Zahlungsauthentifizierungsinstruments „allein nicht notwendigerweise" den Nachweis der Autorisierung erbringt. Diese Vorschrift wurde wegen des besonderen Zusatzes „allein nicht notwendigerweise" von einzelnen Gerichten dahingehend ausgelegt, dass die Verwendung der korrekten Daten (PIN und TAN) des Kontoinhabers keinen Beweis des ersten Anscheins für die Berechtigung des Kontoinhabers erbringt.[1] Letztlich entscheidet sich an der Autorisierung eines Zahlungsvorgangs, ob der Zahlungsdienstleister Aufwendungsersatz verlangen (§ 675u BGB) oder auf eventuelle Schadensersatzansprüche verwiesen wird (§ 675v BGB). § 675w BGB entscheidet über die Verteilung der Beweislast zwischen den über die erfolgte Autorisierung streitenden Parteien. Nach dem Gesetzeswortlaut reicht im Streitfall der Nachweis der Nutzung des richtigen Authentifizierungsinstruments bei Auslösung des Vorgangs allein nicht *notwendigerweise* aus, um eine Pflichtverletzung oder Verschulden des Kunden nachzuweisen. Im Umkehrschluss könnte diese aber auch heißen: Der Nachweis kann durchaus ausreichen (Anscheinsbeweis). Bislang haben die Gerichte bei Missbrauchsfällen im Online-Banking einen Anscheinsbeweis für eine Autorisierung durch den beklagten Kunden nicht ausdrücklich bejaht. Dies führt letztlich dazu, dass den betroffenen Banken, unabhängig von dem verwendeten Authentifizierungsinstrument, nur der Weg über Schadensersatzansprüche bleibt. Diese sind durch den Gesetzgeber grundsätzlich auf maximal 150 EUR begrenzt (Ausnahme: durch die Bank nachweisbarer Betrug, Vorsatz oder grobe Fahrlässigkeit durch den Kunden).

B. Die aktuelle Rechtsprechung insbesondere zu chipTAN-Verfahren

Das AG Berlin-Mitte vertrat die Auffassung, dass man angesichts der gestiegenen Anzahl von Skimming- und Phishing-Fällen nicht mehr davon ausgehen könne, dass der Karteninhaber die PIN auf der Karte notiert oder in Kartennähe aufbewahrt habe.[2] Das Gericht schloss aus, dass ein Kartenmissbrauch unter der Verwendung der richtigen PIN nach der allgemeinen Lebenserfahrung eindeutig auf ein sorgfaltswidriges Handeln des Karteninhabers hinweise.[3] Das LG Berlin vertrat in der Berufungsentscheidung jedoch die Ansicht, dass Skimming und Phishing für den Missbrauch der Originalkarte nicht zur Erschütterung eines Anscheinsbeweis führten, da in diesen Fällen die abgefangenen Daten zur Erstellung einer Kartendublette benutzt würden.[4] Das LG verweist dabei unter anderem auf die Ansicht des BVerfG,[5] das ebenfalls bekräftigt, dass ein Anscheinsbeweis sowieso nur bei der Nutzung der Originalkarte in Frage komme. Anknüpfend an die Rechtsprechung des BGH entschieden das AG Hamburg[6] und das AG Frankfurt a.M.,[7] dass auch eine einmalige bzw. mehrmalige Fehleingabe der PIN beim Missbrauch der Karte nach der Lebenserfahrung nicht zu einer Erschütterung der Annahme führe, der Karteninhaber habe die PIN auf der Karte notiert oder mit der Karte aufbewahrt.

In seinem Urteil vom 29.11.2011 bestätigte der BGH sein Urteil aus dem Jahr 2004. Jedoch betonte er, dass die dort getroffenen Annahmen einen Anscheinsbeweis nur für den Missbrauch unter Verwendung der Originalkarte rechtfertigen, da es beim Missbrauch durch die Verwendung einer erstellten Kartendublette (z.B. durch Skimming) irrelevant sei, ob PIN und Karte zusammen aufbewahrt wurden.[8] Ebenso macht er deutlich, dass die Beweislast für die Verwendung der Originalkarte bei der Bank liegt, wenn diese sich auf die Geltung des Anscheinsbeweises beruft.[9] Allerdings betonte das AG München,[10] dass es außerhalb der Lebenswahrscheinlichkeit stehe, dass jemand eine Originalkarte erst stehle und dann mittels einer Kartendublette ohne Verwendung der gerade gestohlenen Originalkarte Abhebungen vornehme. Das AG München entschied daher, dass bei missbräuchlicher Abhebung an einem Geldautomaten unter Eingabe der richtigen PIN zeitnah nach dem Diebstahl der Beweis der ersten Anscheins dafür spreche, dass der Karteninhaber pflichtwidrig die PIN auf der Karte notiert oder gemeinsam mit dieser verwahrt habe.

Ein Anscheinsbeweis wurde bei der Verwendung einer Zahlungskarte mit richtiger PIN vom BGH bejaht.[11] Ein Anscheinsbeweis wurde ferner bei der Verwendung der richtigen PIN, des richtigen Kennwortes und einer richtigen TAN beim einfachen PIN-TAN-Verfahren zumindest nicht abgelehnt.[12]

Es bleibt die Frage, inwieweit die bisherige Rechtsprechung zum Anscheinsbeweis bei missbräuchlicher

---

1 So etwa LG Mannheim WM 2008, 2015; AG Wiesloch WM 2008, 1648 = WuB I D 1. - 1.09 *Ch. Escher-Weingart*; AG Krefeld BKR 2012, 480; u.v.a.
2 AG Berlin-Mitte NJW-RR 2010, 407, 408.
3 AG Berlin-Mitte NJW-RR 2010, 407, 408.
4 LG Berlin WM 2010, 2353 = WuB I D 5 b. - 1.11 *S. Werner*.
5 BVerfG WM 2010, 208, 209 = WuB I D 5 b. - 1.10 *M. Martinek/S. Omlor*.
6 AG Hamburg WM 2011, 498, 499 f. = WuB I D 5 b. - 2.11 *J. Richrath*.
7 AG Frankfurt a.M. WM 2011, 496, 497 = WuB I D 5 b. - 2.11 *J. Richrath*.
8 BGH WM 2012, 164, 166 = WuB I D 5 a. - 1.12 *L. Haertlein* = NJW 2012, 1277.
9 BGH WM 2012, 164, 166 = WuB I D 5 a. - 1.12 *L. Haertlein*.
10 AG München, Urteil vom 8.2.2013 – 121 C 10360/12.
11 Grundlegend BGHZ 160, 308 = WM 2004, 2309 = WuB I D 5 b. - 1.05 *W. Gößmann* = NJW 2004, 3623; ähnlich BGHZ 170, 18, 30 = WM 2007, 67 = WuB VIII D. Art. 1 3 RBerG 1.07 *A. Stadler* = NJW 2007, 593, 595; bestätigend dazu BVerfG WM 2010, 208, 210 = WuB I D 5 b. - 1.10 *M. Martinek/S. Omlor*.
12 LG Konstanz MMR 2002, 835, 836; LG Bonn CR 2004, 218, 220; LG Köln WM 2008, 354, 357 = WuB I D 1. - 2.08 *S. Werner*; *Werner*, MMR 1998, 232; *Borges*, NJW 2005, 3313; *Kind/Werner*, CR 2006, 353; *Franck/Massari*, WM 2009, 1117.

Verwendung der ec-Karte für das Online-Banking fruchtbar gemacht werden kann.

Vergleichbar ist das Online-Banking mit der Bezahlung mittels ec-Karte und PIN zumindest unter dem Aspekt, dass für die Autorisierung des Zahlungsvorgangs der Besitz eines Legitimationsmediums und die Eingabe einer PIN bzw. eines Passwortes erforderlich ist.[13] Von Teilen des Schrifttums wird ein Anscheinsbeweis daher auch für das Online-Banking befürwortet.[14]

Die Rechtsprechung ist im Bereich des Online-Bankings dagegen mehrheitlich gegen einen Anscheinsbeweis. Das LG Köln[15] nahm zwar 2007 einen Anscheinsbeweis im Online-Banking an. Allerdings galt dies einer anderen Frage: Sofern feststeht, dass die Kontodaten durch einen unbefugten Dritten ausgespäht wurden, spreche der Beweis des ersten Anscheins dafür, dass dies durch Ausspähen des Computers des Kontoinhabers geschehen ist und nicht durch Ausspähen des Zentralrechners der Bank. Dass die Daten beim Kunden ausgespäht werden, entspreche einem typischen Geschehensablaufs, da das Ausspähen von Zentralrechnern der Banken mit erheblichem Mehraufwand verbunden sei. Um diesen Beweis des ersten Anscheins zu widerlegen, reiche die Behauptung des Kontoinhabers, der Rechner der Bank sei ausgespäht worden, nicht aus. Auch wenn der Beweis dieser Tatsache dem Kontoinhaber erschwert ist, da er keine Einblicke in die Unternehmensstruktur hat, finde hier keine Umkehrung der Darlegungs- und Beweislast zu seinen Gunsten statt.

Das LG Mannheim[16] verneinte die Annahme eines Anscheinsbeweises für eine Pflichtverletzung des Bankkunden bei Verwendung des einfachen TAN-Verfahrens. Die vielzähligen Möglichkeiten durch unbemerktes Ausspähen die Legitimationsdaten des Bankkunden zu Missbrauchszwecken zu erlangen, stehe der Annahme eines Anscheinsbeweises entgegen. Aufgrund dieses Risikos könne bei einer unberechtigten Verfügung unter Verwendung von TAN und PIN nicht auf eine Pflichtverletzung des Bankkunden geschlossen werden.

Dagegen ließ das AG Wiesloch[17] offen, ob bei der Verwendung des einfachen TAN-Verfahrens ein Anscheinsbeweis besteht, da dieser im zugrunde liegenden Fall zumindest erschüttert war. Es stellte aber obiter dictum klar, dass es Zweifel daran hat, ob bei Verwendung des „einfachen TAN-Verfahrens" ohne zusätzliche Absicherung durch das iTAN-Verfahren oder andere Sicherheitsmechanismen ein Anscheinsbeweis zulasten des Kontoinhabers angenommen werden könne. Die Gefahren des Missbrauchs durch unbemerktes Abfangen oder Ausspähen von Daten seien zu hoch, um einen typischen Geschehensablauf zulasten des Kontoinhabers annehmen zu können. Ferner seien die Grundsätze der Rechtsprechung des BGH[18] zum ec-Karten-Missbrauch nicht ohne Weiteres auf das Online-Banking übertragbar. Im Gegensatz zu einem tatsächlich erfolgten Diebstahl der ec-Karte in Verbindung mit der Kenntniserlangung der PIN durch den unberechtigten Dritten könne im Online-Bereich nicht mit einer vergleichbar erforderlichen Sicherheit darauf geschlossen werden, dass der Kontoinhaber seine Bankdaten unsicher verwahrt hat.

Im Zusammenhang mit der Frage zum Anscheinsbeweis hat sich die Rechtsprechung zudem wiederholt mit der Frage nach einer Sorgfaltspflichtverletzung des Bankkunden auseinandergesetzt.

So ließ das LG Berlin[19] zwar die Frage nach einem Anscheinsbeweises für den Fall der Verwendung der korrekten Kontodaten durch unberechtigte Dritte offen. Es traf jedoch zwei weitere für den Anscheinsbeweis im Online-Banking maßgebliche Feststellungen, die in Bezug auf das iTAN-Verfahren getroffen worden sind: Das Gericht führte aus, dass in Fällen, in denen aufgrund einer Phishing-Attacke mehrere TANs verwendet werden, keine Anscheinsvollmacht für die anschließende missbräuchliche Überweisung angenommen werden könne. Gleichzeitig stellte das Gericht aber fest, dass der Kontoinhaber fahrlässig handle, wenn er aufgrund einer dahingehenden Aufforderung die PIN durch Eingabe von vier TANs bestätigt, da dies im Bereich des Online-Bankings hochgradig unüblich sei.[20]

Das AG Krefeld[21] schloss sich dieser Rechtsprechung an und sieht in der gleichzeitigen Eingabe mehrerer TANs einen Verstoß gegen die Pflichten des Kontoinhabers aus § 675l BGB. Im Weiteren verneinte das AG jedoch die Annahme eines Anscheinsbeweises für die Autorisierung der Online-Überweisung aus § 675w Satz 3 BGB. Selbst bei ordnungsgemäßer Aufzeichnung, Verbuchung und dem störungsfreien Ablauf des Zahlungsvorgangs könne kein typischer Geschehensablauf angenommen werden. Die Aufforderungen zur Dateneingabe mit kriminellem Hintergrund seien derart häufig, dass die Verwendung von korrekter PIN und TAN nicht den Rückschluss auf die Zustimmung des Berechtigten zulasse.

Das AG Köln[22] entschied im Zusammenhang mit dem chipTAN-Verfahren, dass es für einen Anscheinsbeweis nicht ausreichend sei, nur allgemein den Zahlungsvorgang beim Online-Banking mit einem TAN-Generator zu beschreiben, vielmehr müsse „zu dem konkreten Vorgang vorgetragen werden". Allerdings stehe der Bank ein Schadensersatzanspruch aus § 675v Abs. 2 BGB in Höhe der gezahlten Beträge aus der Banktransaktion zu. Abgestellt wurde hier auf die Sicherheitshinweise der Bank. Dazu zählte insbesondere Ziff. 4.3 der Bedingungen für das Online-Banking, wonach die Kunden verpflichtet seien, die Sicherheitshinweise zu beachten. Insofern hat das AG Köln darauf hingewiesen, dass konkrete Sicherheitshinweise auf der Website in den dortigen Sicherheitstipps zum Online-Banking erteilt worden seien. Dort sei auch darüber informiert worden, dass die TANs nur für persönliche Aufträge gelten und eine Bank den Kunden niemals auffordere, eine TAN für Gewinnspiele oder Sicherheitsupdates einzugeben. Schließlich stellte das Gericht auch fest, dass von einem durchschnittlichen Nutzer des Online-Bankings zumindest im Jahr 2013 eine allgemeine Kenntnis über verschiedene Betrugsformen beim Online-Banking als bekannt vorauszusetzen sei. Deshalb komme es noch nicht einmal auf die konkrete Kenntnis der Sicherheitshinweise der Beklagten an.[23]

Ähnlich äußerte sich das AG Bonn:[24] Das Gericht traf zwar keine Aussage dazu, ob es sich um eine autorisier-

---

[13] *Karper*, DuD 2006, 215, 218.

[14] *Werner*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 2014, Teil 13.5 Rdn. 63 ff.; *ders.*, MMR 1998, 232, 235; *Bunte*, AGB Banken, Nr. 6 (SB Online) Rdn. 126; *van Gelder*, Festschr. Nobbe, 2009, S. 55, 66 f.; *Karper*, DuD 2006, 215, 219; *Weber*, Recht des Zahlungsverkehrs, 4. Aufl. 2004, S. 304.

[15] LG Köln WM 2008, 354 = WuB I D 1. - 2.08 *S. Werner* = MMR 2008, 259.

[16] LG Mannheim WM 2008, 2015 = BKR 2009, 84.

[17] AG Wiesloch WM 2008, 1648 = WuB I D 1. - 1.09 *Ch. Escher-Weingart* = MMR 2008, 626.

[18] BGH WM 2004, 2309 = WuB I D 5 b. - 1.05 *W. Gößmann*.

[19] LG Berlin MMR 2010, 137.

[20] So nunmehr auch BGH WM 2012, 983 = WuB I D 1. - 3.12 *M. Geschwandtner/N. Breidenbach*.

[21] AG Krefeld BKR 2012, 480.

[22] AG Köln, Urteil vom 20.1.2014 – 142 C 406/13.

[23] Das Amtsgericht verweist auf ein Urteil des AG Krefeld vom 6.7.2012 - 7 C 605/11.

[24] AG Bonn, Urteil vom 15.4.2014 - 109 C 223/13.

te Zahlung handelte. Jedoch entschied es, dass es als grob fahrlässig zu bewerten sei, wenn der Bankkunde entgegen der Online-Sonderbedingungen nicht die Empfänger-Kontonummer, den Überweisungsbetrag und den Startcode abgleicht bevor er diese am TAN-Generator bestätigt. Bei dem vorzunehmenden Abgleich des Empfängerkontos handele es sich nach Ansicht der Gerichts um eine für jeden durchschnittliche Nutzer des Online-Bankings bekannte Grundregel, deren Nichtbeachtung ein Sicherheitsrisiko darstellt.

Das LG Darmstadt[25] setzt diese Rechtsprechung weiter fort. Anknüpfend an die dem Bankkunden obliegenden Pflichten wird aber anders als noch beim AG Bonn kein Schadensersatzanspruch der Bank bejaht, sondern dem Kunden bereits die Autorisierung des Zahlungsvorgangs nach den Grundsätzen der Rechtsscheinhaftung zugerechnet.

Im streitgegenständlichen Fall begehrte die Klägerin von ihrer Hausbank (Beklagte) Ersatz für zwei Online-Überweisungen. Zur Durchführung des Überweisungsauftrags bediente sich die Klägerin des chipTAN-Verfahrens,[26] bei dem für die Autorisierung der Transaktion mittels eines TAN-Generators eine transaktionsspezifische TAN generiert wird. Dabei werden dem Bankkunden die Transaktionsdaten auf dem Display des TAN-Generators angezeigt, die der Kunde durch Drücken der O.K.-Taste des TAN-Generators bestätigen muss. Anhand der an ihn übermittelten Daten errechnet der TAN-Generator eine auf die konkrete Transaktion bezogene TAN. Der Bankkunde löste zwar im Online-Banking Überweisungen aus, allerdings wurden diese Daten durch einen „Man-in-the-Middle-Angriff" manipuliert und mit einem anderen Zielkonto und einem anderen Zahlungsempfänger versehen. Das Gericht vertritt die Auffassung, dass die Klägerin ihr Einverständnis zu den Transaktionen zwar nicht selbst erteilte, ihr dieses jedoch nach den Grundsätzen der Anscheinsvollmacht zuzurechnen sei. Denn das chipTAN-Verfahren weise eine derart hohe Systemsicherheit auf, dass nach derzeitigem Stand der Technik so gut wie ausgeschlossen sei, dass die durchgeführte Transaktion nicht von dem Kunden selbst vorgenommen wurde. Die einzig in Betracht zu ziehende Manipulationsmöglichkeit des „Man-in-the-Middle-Angriffs" hätte die Klägerin verhindern können, wenn sie die auf dem Display angezeigten Transaktionsdaten auf ihre Übereinstimmung mit den für die Transaktion vorgesehenen Daten kontrolliert hätte, wie es Ziffer 7.4 der Allgemeinen Sonderbedingung für das Online-Banking bestimmt.

Noch weiter geht das LG Köln,[27] dass jüngst entschied, dass sich eine schematische Ablehnung des Anscheinsbeweises im Online-Banking schon angesichts des Wortlautes von § 675w Satz 3 BGB verbiete. Entscheidend für die Anwendung müsse vielmehr der Grad der Sicherheit des jeweils angewandten TAN-Verfahrens sein.

Insoweit sei die Anwendung des Anscheinsbeweises bei der Verwendung des mobilen TAN-Verfahrens gerechtfertigt, da bei diesem mittlerweile eine Sicherheitslage erreicht sei, die derjenigen der Nutzung von ec-Karten an Geld- oder Überweisungsautomaten entspricht.

C. ChipTAN und die Empfehlungen der Zentralbank

Der Beweiswert von chipTAN-Verfahren stellt sich nicht nur bankenvertragsrechtlich, sondern auch bankenaufsichtsrechtlich. Am 31.1.2013 veröffentlichte die Europäische Zentralbank verpflichtende Richtlinien,[28] die von allen Finanzdienstleistern innerhalb der Gruppe der Payment-Server-Provider eine „strong authentication" bis 1.2.2015 verlangt. Diese Richtlinien gelten für alle Fernverfahren, einschließlich des Online-Bankings.

I. Vorüberlegungen

Wichtig ist hier der Begriff der „strong authentication". Der Begriff ist nicht eindeutig und wird oft mit Begriffen vermengt wie der Zweifaktor-Authentifizierung oder Verschlüsselungstechniken. Juristisch versteht man im Anschluss an die Vorgaben der Europäischen Zentralbank den Begriff als Hinweis auf eine Fernauthentifizierung.

In den EZB Guidelines heißt es:

„Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data" (p.3)

Die EZB-Richtlinien gehen vom Zusammentreffen mindestens zweier Elemente aus. Das eine ist Wissen (knowledge), das zweite ist Besitz (possession). Diese beiden Elemente müssen unabhängig voneinander sein. Es muss also ein Informationselement dabei sein, das nur der Nutzer weiß, wie z.B. Passwörter, TAN oder PIN, und etwas, was nur der Nutzer besitzt (z.B. eine SmartCard). Mindestens eines der Elemente darf nicht wiederverwendbar oder kopierbar sein; es darf auch nicht übers Internet gestohlen werden können.

Dabei kann dahingestellt bleiben, ob biometrische Verfahren überhaupt nach geltendem Datenschutzrecht in solche Anwendungen integriert werden dürfen. Auch bringen solche Verfahren erhöhte Sicherheitsrisiken mit sich.[29] Größere Schwierigkeiten bestehen indes bei der Unterscheidung zwischen Wissen und Besitz. Das Bundesamt für Sicherheit in der Informationstechnik erkennt Wissen dann als Mittel zur Sicherung der Authentisierung an, wenn das Wissen ausschließlich dem berechtigten Inhaber bekannt ist.[30] Der Kunde selbst kann seine PIN aber an andere (z.B. Familienangehörige, Betreuer etc.) übermitteln, sodass mehr Men-

[25] LG Darmstadt WM 2014, 2323.

[26] Das Urteil spricht vom Smart-TAN-plus-Verfahren; dieses Verfahren entspricht dem chipTAN-Verfahren.

[27] LG Köln WM 2014, 2372.

[28] EZB, Recommendations for the security of internet payments, (zuletzt abgerufen am 2.3.2015) https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf.

[29] Vgl. *Amtul Fatima*, E-Banking Security Issues – Is There A Solution in Biometrics?Áøø, Journal of Internet Banking and Commerce, August 2011, Vol. 16, No. 2, 1 (7).

[30] BSI, TR-03107-1, Elektronische Identitäten und Vertrauensdienste im E-Government, S. 14, (zuletzt abgerufen am 2.3.2015) https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html.

schen etwas wissen. Auch im Falle von Hacking und sonstigen Sicherheitsangriffen erfährt der Angreifer die entsprechenden Passwörter. Es gibt eigentlich keine Information, die per se nur einer weiß.[31] Vielmehr ist Wissen eine relative Größe, die sich dynamisch verändert und unterschiedliche Kreise einbezieht. Im Übrigen ist das Element „and not capable of being surreptitiously stolen via the internet" unklar. Bezogen auf die Chipkarte kommt ein Diebstahl über das Internet nicht in Betracht. Bezogen auf PIN/TAN scheidet ein „Diebstahl/theft" denknotwendig aus, da Gegenstand eines Diebstahls immer eine bewegliche Sache, d.h. ein körperlicher Gegenstand ist. Im Übrigen kann aber ein „Diebstahl" der PIN/TAN über das Internet nicht 100%ig ausgeschlossen werden. Die Richtlinien der EZB sind ferner insofern eigenartig, als sie auch auf Besitz abstellen. Denn der Besitz als solches ist nur eine juristische Kategorie des Zivilrechts (siehe § 854 BGB). Entscheidend sind aber der Einsatz der entsprechenden Karte und deren Authentifizierung. Selbst wenn der Kunde keine unmittelbare Sachgewalt über die Karte hätte, wäre darauf abzustellen, dass die Nutzung dieser Karte unter seiner Kontrolle erfolgt. So könnte sich z.B. der Kunde des Besitzes an einer Chipkarte begeben und diese z.B. an einen Freund zur schnellen Transaktion ausleihen. Das deutsche Recht geht in diesem Fall davon aus, dass dann nicht mehr der unmittelbare Besitz vorliegt, sondern ein juristisch gestalteter, fiktiver mittelbarer Besitz.

Das Element des Besitzes könnte hier durch die Chipkarte mit TAN-Anwendung erfüllt sein.[32] Die Chipkarte selbst ist im Besitz des Karteninhabers. Zusätzlich zu der Chipkarte besitzt der Karteninhaber über eine vertrauenswürdige Quelle einen TAN-Generator. Für das Element des Wissens kann auch auf die TAN abgestellt werden. Denn der Kunde kennt als Einziger die TAN, die mithilfe des TAN-Generators und den jeweiligen Transaktionsdaten generiert wird. Dabei ist die Auswahl, ob eine TAN mit oder ohne Benutzer-PIN-Eingabe erzeugt werden soll, eine freie Entscheidung des Kunden. Wie sich aus den Empfehlungen der EZB zu ihren Richtlinien ergibt, kann durch diese Verknüpfung der Authentifizierung mit den jeweiligen Transaktionsdaten eine verstärkte Kundenauthentifizierung erreicht werden.[33]

Der TAN-Generator auf der einen Seite und die Online-Banking-Anmeldedaten kompromittieren sich nicht wechselseitig. Im Falle des Diebstahls der Chipkarte kann der Dieb nicht Zahlungsvorgänge auslösen, da ihm die Online-Banking-Anmeldedaten unbekannt sind. Umgekehrt hilft die Kenntnis der Online-Banking-Anmeldedaten seitens eines Unberechtigten nicht, um eine Banktransaktion durchzuführen. Die generierten TANs sind auch nicht wiederverwendbar; sie sind nur für die spezielle Transaktion gültig, für die sie generiert wurden. Die Übertragungswege zwischen dem PC des Kunden und der Bank sind in einer Art und Weise gestaltet worden, die ein Abfangen oder manipulieren der Daten ohne Zugriff auf den PC des Kunden unmöglich machen.

Entsprechend den EZB-Richtlinien kann man aber auch darauf abstellen, dass die Chipkarte in „possession (Besitz)" ist. Das Wissenskriterium würde dann auch unter Umständen durch die Online-Banking-Anmeldedaten gegeben sein, die zu Beginn der Online-Sitzung vom Kunden eingegeben werden. Diese Anmeldedaten sind nur ihm bekannt. Nicht einmal die Bank hat Kenntnis davon, da diese mit besonderen kryptographischen Verfahren so verschlüsselt werden, dass eine Bankkenntnis von den vollständigen Anmeldedaten nicht vorliegt. Das Kriterium der Non-Reusability wird dadurch erreicht, dass die Chipkarte als solche nicht durch Dritte verwendet werden kann. Sie ist daher nur für den Kunden selbst in Verbindung mit seinen Identifikationsdaten nutzbar. Die Chipkarte kann auch nicht über das Internet gestohlen werden.

II. Strong authentication in der 2. Zahlungsdiensterichtlinie

In diesem Zusammenhang ist zu beachten, dass die geplante 2. Zahlungsdiensterichtlinie, die bei allen Online-Bankgeschäften eine „strong authentication" im Einklang mit den EZB-Richtlinien verlangt, diesen Begriff anders definiert.

Die 2. Zahlungsdiensterichtlinie (Payment Service Directive II, PSD II)[34] ist auf Vorschlag der Europäischen Kommission am 24.7.2013 zur Überarbeitung der geltenden Richtlinie vorgelegt worden. Der Gesetzgebungsprozess wird voraussichtlich in der seit September 2014 laufenden Legislaturperiode des Europäischen Parlamentes abgeschlossen werden.

Art. 4 Nr. 22 der 2. Zahlungsdiensterichtlinie definiert „strong customer authentication" als „a procedure for the validation of the identification of a natural or legal person based on the use of two or more elements categorised as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data."

Hier wird auf das Element der Unmöglichkeit eines Diebstahls nicht mehr eingegangen. Vielmehr wirkt die Definition offener als die der EZB-Richtlinie.

Bislang in der Literatur noch nicht erörtert wurde der Zusammenhang von Anscheinsbeweis und „strong authentication". In der EZB-Richtlinie wird kurz betont:

„From the Forum's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction" (p.3).

Diese Aussage lässt im Umkehrschluss den Gedanken zu, dass die EZB im Falle einer „strong authentication" einen Anscheinsbeweis bejaht. Für eine solche Verbindung sprechen auch Hinweise im „ECB Assessment guide for the security of internet payments" (Februar 2014). Dort heißt es:[35]

„The authentication element (e.g. knowledge, ownership, inherence) produces a data string (e.g. password, OTP, biometric value) that is sent remotely to the authentication server, during the payment initiation phase. This data string, the „authenticator value", is transmitted via a protocol, to the authentication server *as a proof the user possesses and controls the „authentication element" and, consequently, as a proof of the user's identity.*" (Hervorhebung durch Verfasser)

In der 2. Zahlungsdiensterichtlinie heißt es hierzu in Art. 64:

„(1) Member States shall require that, where a payment service user denies having authorised an executed

---

[31] So im Ergebnis auch *Moncur/Leplâtre,* Digital Evidence and Electronic Signature Law Review Vol. 6, 2009, 116-122, die das mit der begrenzten Merkfähigkeit des Menschen begründen.

[32] Vgl. BSI, a.a.O. (Fn. 30), S. 38.

[33] EZB, a.a.O. (Fn. 28), S. 40.

[34] (Zuletzt abgerufen am 2.3.2015) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri =CELEX:52013PC0547&from=DE.

[35] EZB, a.a.O. (Fn. 28), S. 10 Fn. 23.

payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider and, if involved and as appropriate, the third party payment service provider, to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency under Article 61.

(2) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the third party payment service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligation."

Auffällig ist, dass Art. 64 Abs. 2 nur den bisherigen Wortlaut von § 675w BGB wiederholt und insofern den Stand der 1. Zahlungsdiensterichtlinie wiedergibt. Art. 64 Abs. 1 enthält hingegen sehr hohe Anforderungen an die Darlegungs- und Beweislast des Kreditinstituts, ohne aber auf die Besonderheiten einer „strong authentication" einzugehen.

Die „strong authentication" taucht in der 2. Zahlungsdiensterichtlinie erst in Art. 87 auf:

„Member States shall ensure that a payment service provider applies strong customer authentication when the payer initiates an electronic payment transaction unless EBA guidelines allow specific exemptions based on the risk involved in the provided payment service. This also applies to a third party payment service provider when initiating a payment transaction on behalf of the payer."

Danach sollen die Mitgliedstaaten sicherstellen, dass ein Zahlungsdienstleister eine verstärkte Kundenauthentifizierung verlangt, wenn der Zahler einen elektronischen Zahlungsvorgang auslöst. Die gewählte Formulierung der „elektronischen Zahlung" lässt zwar nicht hinreichend deutlich erkennen, welche Sachverhalte ihr unterfallen. Gemeint sein dürften aber Online-Banking-Überweisungen und kartengestützte Zahlungen unter Einsatz von Zahlungsinstrumenten (d.h. z.B. Online-Banking und PIN/TAN oder Debitkarte und PIN), während Lastschriften, die vom Zahlungsempfänger ausgelöst werden, ausgenommen sind.[36] Die Richtlinie knüpft damit an den von den EZB-Empfehlungen in Nr. 7.1 KC vorgegebenen Anwendungsbereich an.[37]

Für diese elektronischen Zahlungen wollen die Empfehlungen das Schutzniveau weiter verbessern.[38] Da insofern den Authentifikationsinstrumenten des Zahlers entscheidende Bedeutung zukommt, ist es nachvollziehbar, dass die Empfehlungen an diesen anknüpfen und der „verstärkten Kundenauthentifizierung" besondere bankenaufsichtsrechtliche Bedeutung zumessen.

Neue Anforderungen an die Authentifizierungsinstrumente sind aber nicht gleichbedeutend mit neuen Beweisanforderungen. So finden sich in den Empfehlungen für den Fall einer verstärkten Kundenauthentifizierung keine abweichenden Beweisanforderungen. Die Empfehlungen verlangen lediglich, dass die zu erlassenen Zahlungsdiensterichtlinien die verstärkte Kundenauthentifizierung aufnehmen und technisch gewährleisten.[39]

Davon scheint auch der europäische Richtliniengeber auszugehen, wenn er zwar die verstärkte Kundenauthentifizierung in Art. 87 Abs. 1 für das Online-Banking fordert, im Abschnitt über den „Nachweis der Authentifizierung" (Art. 64) aber keine anders lautenden Beweisanforderungen trifft. Im Gegenteil, der Richtlinientext führt den in der 1. Zahlungsdiensterichtlinie begründeten und durch § 675w BGB umgesetzten Weg weiter fort. Danach reicht „. . . die vom Zahlungsdienstleister und gegebenenfalls dem dritten Zahlungsdienstleister aufgezeichnete Nutzung eines Zahlungsinstruments [als Nachweis] für sich gesehen *nicht notwendigerweise* aus . . . ".

Vielmehr soll das bestehende Schutzniveau dadurch erweitert werden, dass Innovationsmöglichkeiten für eine Weiterentwicklung der bestehenden Zahlverfahren genutzt werden.[40]

Innovationsanreize wollen die Empfehlungen aber nicht durch eine Verschiebung der Beweisanforderungen bewirken, sondern durch eine verschärfte Haftung der Zahlungsdienstleister.[41]

Die Europäische Kommission hat diese Vorgaben in Art. 66 ZDRL II-E umgesetzt. So soll nach Art. 66 Abs. 1 Unterabs. 2 Satz 3 ZDRL II eine Kundenhaftung ausgeschlossen sein, wenn bei *„Zahlungen mittels eines Fernkommunikationsmittels . . . der Zahlungsdienstleister keine verstärkte Kundenauthentifizierung verlangt hat"*.

Damit bleibt festzustellen, dass die Empfehlungen die Sicherheit von Internetzahlungen durch eine verstärkte Kundenauthentifizierung weiter verbessern wollen, ohne dabei aber die geltenden Beweisanforderungen zu ändern. Vor dem Hintergrund der verschärften Haftung würde eine solche Kumulation auch eine unbillige Härte für den Zahlungsdienstleister bedeuten.

Soweit also die derzeit verwendeten Authentifizierungsinstrumente den Anforderungen an eine starke Authentisierung genügen,[42] kann für den Anscheinsbeweis nicht anderes gelten als bisher von der Rechtsprechung festgestellt wurde.

Auf den dem Anscheinsbeweis zugrunde liegenden Geschehensablauf hat die verstärkte Kundenauthentifizierung keine Auswirkung. Vielmehr wird die Grundlage des Anscheinsbeweises, nämlich ein ausreichend hohes Schutzniveau beim Zahlungsvorgang zu gewährleisten, durch die strengen Anforderungen an die Authentifizierungsinstrumente weiter konsolidiert.

---

[36] So auch die Deutsche Kreditwirtschaft in ihrer Stellungnahme zum Vorschlag der 2. Zahlungsdiensterichtlinie, S. 10, (zuletzt abgerufen am 2.3.2015) http://www.die-deutsche-kreditwirtschaft.de/uploads/media/131202_DK-Position-PSD_II.pdf.

[37] EZB, a.a.O. (Fn. 28), S. 9 Nr. 7.1 KC.

[38] EZB, a.a.O. (Fn. 28), S. 1.

[39] EZB, a.a.O. (Fn. 28), S. 9 Nr. 7.3 KC.

[40] Vgl. *Linardatos*, WM 2014, 300, 304.

[41] EZB, a.a.O. (Fn. 28), S. 10 Nr. 7.6 KC.

[42] Vertiefend *Hoeren/Kairies*, ZBB 2015, 35, 36.