• MiKaP® • Medienrecht im Kreise affirmativer Patent-, Marken- und Urheberrechte

MiKaP® 2015/01 Januar/Februar 2015 / 8. Jg.

ISSN 1866 - 1092 Seite 1 bis 17

Herausgeber: Rechtsanwalt Jochen Papenhausen,
Fachanwalt für IT-Recht und Urheber- & Medienrecht

Inhalt

Impressum:

MiKaP® ist eine Online-Veröffentlichung mit fortlaufenden Seiten für IT- und Medienrecht unter der Website http://www.mikap.de.

MiKaP® ist als Marke beim Deutschen Patent- und Markenamt, München (DPMA), eingetragen.

Deutsche Bibliothek, Frankfurt am Main: ISSN 1866-1092. Zitiervorschlag: MiKaP® [Jahr], [Seite].

Verantwortlicher Herausgeber:
Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Fachanwalt für Urheber- & Medienrecht
Jochen Papenhausen, Ritterstr. 2, D-49074 Osnabrück, Telefon: 0541 - 99 899 788, Telefax: 0541 - 99 899 789,
E-Mail: post@kanzlei-papenhausen.de, Internet: http://www.kanzlei-papenhausen.de.
Das ausführliche Impressum können Sie unter der folgenden URL einsehen: http://www.mikap.de.
Sämtliche Publikationen sind dauerhaft abrufbar unter http://www.mikap.de.
Bitte beachten Sie auch die wichtigen Hinweise am Ende dieser Ausgabe (insbesondere den Haftungsausschluss).

BGH: Schnäppchen bei eBay-Auktion (Kurzmitteilung)

Der BGH[1] hat wie die Vorinstanzen (LG Mühlhausen[2] und OLG Jena[3]) den Vertragsschluss eines im Wege einer Internetauktion abgeschlossenen Kaufvertrags – bei dem ein grobes Missverhältnis zwischen dem Kaufpreis und dem Wert der Kaufsache besteht – bejaht:

Im vorliegenden Fall bot der Verkäufer (hier der Beklagte) seinen Gebrauchtwagen bei eBay zum Kauf an und setzte ein Mindestgebot von Euro 1,00 fest. Der Käufer (Kläger) bot diesen Mindestbetrag.

Einige Stunden später brach der Beklagte die eBay-Auktion ab, da er den Pkw anderweitig verkauft hat.

Der Kläger begehrte hier Schadensersatz wegen Nichterfüllung, legte dar, dass der Pkw einen Wert von Euro 5.250,00 habe und klagte Euro 5.249,00 ein.

Die Instanzgerichte wie auch der BGH gaben dem Kläger Recht:

Der Kaufvertrag sei nicht etwa wegen Sittenwidrigkeit (§ 138 Abs. 1 BGB) nichtig: Es mache gerade den Reiz einer Internetauktion aus, den Auktionsgegenstand zu einem Schnäppchenpreis zu erwerben, während umgekehrt der Veräußerer die Chance wahrnehme, einen für ihn vorteilhaften Preis im Wege des Überbietens zu erzielen.

Auch könne dem Kläger nicht der Einwand des Rechtsmissbrauchs entgegengehalten werden: Dass das Fahrzeug letztlich zu einem Preis von Euro 1,00 verkauft wurde, beruhe auf den freien Entscheidungen des Beklagten, der das Risiko eines für ihn ungünstigen Auktionsverlaufs durch die Wahl eines niedrigen Startpreises ohne Festsetzung eines Mindestgebots eingegangen ist und durch den nicht gerechtfertigten Abbruch der Auktion die Ursache dafür gesetzt hat, dass das Risiko sich verwirklicht.

LG Heidelberg: Suchmaschinenhaftung /Persönlichkeitsrechtsverletzung (Kurzmitteilung)

Nach dem LG Heidelberg[4] haftet die Betreiberin einer Internet-Suchmaschine für die von ihr angezeigten Links zu Internetseiten mit persönlichkeitsrechtsverletzendem Inhalt:

Eine unionsrechtskonforme Auslegung der gesetzlichen Bestimmungen über die Störerhaftung gebiete es nach dem Landgericht Heidelberg, dass die Betreiberin einer Web-Suchmaschine grundsätzlich als verantwortliche Störerin für die von ihrer Suchmaschine angezeigten Suchergebnisse mit persönlichkeitsrechtsverletzenden Inhalten in Anspruch genommen werden kann.[5]

---

[1] BGH, Urteil vom 12.11.2014, Az. VIII ZR 42/14.
[2] LG Mühlhausen, Urteil vom 09.04.2013, Az. 3 O 527/12.
[3] OLG Jena, Urteil vom 15.01.2014, Az. 7 U 399/13.
[4] LG Heidelberg, Urteil vom 09.12.2014, Az. 2 O 162/13.
[5] Vgl. dazu die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Die von der Persönlichkeitsrechtsverletzung betroffenen Person kann grundsätzlich die Berichtigung, Löschung und/oder Sperrung von solchen Daten verlangen.[6]

AG Kassel, Verjährung beim Filesharing / Abweisung einer Zahlungsklage (Kurzmitteilung)

Das AG Kassel[7] hatte über eine Zahlungsklage wegen angeblichen Urheberrechtsverstößen im Rahmen von Filesharing / Tauschbörsenteilnahme zu urteilen.

Das AG Kassel stellte fest, dass die geltend gemachten Ansprüche aus §§ 97, 97a UrhG der Verjährung unterliegen und die regelmäßige Verjährungsfrist für diese Ansprüche gemäß § 195 BGB 3 Jahre beträgt.[8]

Auch die zwischenzeitlich abgegebene Unterlassungserklärung des Beklagten hatte keinen Einfluss auf die Verjährung des hier geltend gemachten Lizenzanalogieschadensersatzanspruches und Aufwendungsersatzanspruches.

Das AG Kassel stellt hierzu fest: „Insbesondere liegt kein einen Neubeginn der Verjährung hervorrufendes Anerkenntnis im Sinne des § 212 Abs. 1 Nr. 1 BGB vor. Denn mit der Abgabe einer strafbewehrten Unterlassungserklärung ist ein Anerkenntnis dieser Art nicht verbunden. Darin liegt nicht einmal ein Anerkenntnis des mit der Unterlassungserklärung erfüllten entsprechenden Unterlassungsanspruches. Denn mit der Abgabe einer solchen Erklärung will der Abgemahnte regelmäßig keinen konkreten Inhalt mit konkreten Rechtsfolgen fixieren. Es bleibt mithin mit der bloßen Abgabe der Erklärung offen, ob er lediglich Kostenrisiken und Aufwand des Prozesses über den Unterlassungsanspruch meiden will, an der zukünftigen Wiederholung der abgemahnten Handlung kein Interesse mehr hat oder ob er tatsächlich die Berechtigung der Abmahnung anerkennt (BGH, Urteil vom 24.09.2013 - I ZR 219/12 - medizinische Fußpflege, zit. n. Juris). Sofern mit der Unterlassungserklärung nicht ausdrücklich auch der Kostenerstattungsanspruch betreffend die Abmahnung anerkannt ist, lässt sich aus der Erklärung oder ihrer Abgabe auch nicht das Anerkenntnis des Kostenerstattungsanspruches ableiten. Eine solche ausdrückliche Erklärung weist die von der Klägerin vorgelegte schriftliche Erklärung des Beklagten nicht aus. Es sind auch keine sonstigen Anhaltspunkte erkennbar, die eine Auslegung mit dem Ergebnis eines Anerkenntnisses zuließen. Ist jedoch mit der Unterlassungserklärung bereits kein Anerkenntnis der damit vorrangig angesprochenen Ansprüche der Klägerin erklärt, so kann erst recht kein Anerkenntnis des Weiteren etwa bestehenden Anspruches auf Zahlung eines Lizenzanalogieschadens damit verbunden sein.“

Auch hat das AG Kassel entschieden, dass die Klägerin für sich auch nicht die zehnjährige Verjährungsfrist des § 852 S. 2 BGB reklamieren kann: „Nach dieser Vorschrift unterliegen diejenigen Ansprüche einer längeren Verjährung, die auf die Herausgabe des deliktisch Erlangten

[6] Vgl. hierzu auch: EuGH, Entscheidung vom 13.05.2014, Az. C-131/12.
[7] AG Kassel, Urteil vom 24.07.2014, Az. 410 C 625/14.
[8] Siehe zur Verjährung auch: AG Düsseldorf, Urteil vom 13.01.2015, 57 C 7592/14: Der bereicherungsrechtliche Anspruch nach §§ 852 S. 1, 812 ff. BGB verjähre nach 10 Jahren.

zielen. Es handelt sich somit um einen quasi deliktischen Bereicherungsanspruch. Diese Vorschrift findet wegen § 102 S. 2 UrhG entsprechende Anwendung. Voraussetzung ist aber, dass der Schädiger tatsächlich etwas erlangt hat. Dies kann die ersparte Lizenzgebühr sein, wenn die Wahrnehmung des Urheberrechts typischerweise nur gegen eine Lizenzgebühr eingeräumt wird (BGH, Urteil vom 27.10.2011 - I ZR 175/10 - Bochumer Weihnachtsmarkt, zit. n. Juris). Dies ist etwa dann der Fall, wenn die Rechtewahrnehmung bei einer Verwertungsgesellschaft lizenziert werden kann. Hier liegen jedoch die tatsächlichen Verhältnisse anders, so dass die Grundsätze der eben zitierten Rechtsprechung des Bundesgerichtshofs vorliegend keine Anwendung finden können. Denn dem erkennenden Gericht ist kein Anbieter bekannt, der Werke der Musik oder Filmwerke dergestalt lizenziert, dass sie im Wege des Filesharings angeboten werden können. Dies ergibt sich bereits aus dem Umstand, dass die Klägerin - wie alle dem erkennenden Gericht bekannten Gläubiger vergleichbarer Ansprüche - Schadensersatz im Wege der Lizenzanalogie begehren. Lizenzanalogie bedeutet aber, dass zumeist im Wege der Schätzung ein Schadensersatzanspruch danach ermittelt wird, was dem verletzten Urheber an Lizenzgebühren entgangen ist. Ein bereicherungsrechtlich abschöpfbarer Vorteil muss dabei dem Schädiger gar nicht entstanden seien. So ist es hier. Der Hauptzweck des typischen Nutzers einer Internet-Tauschbörse beim Filesharing liegt darin, beispielsweise das Musikstück zu erhalten. Der technisch damit zugleich verbundene Upload wird damit gleichsam nur als notwendiges Übel verbunden, ohne dass er zielgerichtet beabsichtigt ist. Es wird allenfalls billigend in Kauf genommen, dass ein weiterer Teilnehmer der Tauschbörse nunmehr in der Lage ist, dasselbe Musikstück seinerseits herunter zu laden. Er erspart sich mithin keine Lizenzgebühren, weil er diese auch bei einer legalen Vorgehensweise gerade nicht bezahlt hätte. Gezahlt worden wäre allenfalls der übliche Kaufpreis etwa einer CD. Denn dem Nutzer geht es beim Filesharing nur um den Gebrauch des konkreten Werkes für eigene Zwecke, nicht um die darüber hinausgehende Nutzung oder gar Verbreitung. Darin unterscheidet sich der typische Tauschbörsenteilnehmer von demjenigen, der etwa seine Verkaufsstätte mit Musikwerken beschallt, um damit das Kaufverhalten potentieller Kunden zu befördern. Ein solcher Urheberrechtsverletzer würde bei legalem Vorgehen nämlich entsprechende Lizenzgebühren bezahlen. Das erkennende Gericht folgt insoweit der Rechtsprechung des Amtsgerichts Bielefeld (Urteil vom 06.03.2014 - 42 C 368/13, zit. n. Juris Rdnr. 16). Dabei berücksichtigte das Gericht auch, dass typischerweise die verwendeten Programme den Upload nicht vollständig durchführen, sondern nur Bruchteile der Dateien wieder in die Tauschbörse einstellen, auch wenn diese Bruchteile notwendig sind, damit der nächste Tauschbörsenteilnehmer wieder die gesamte Datei auf seinen Computer herunter laden kann."

Siehe zu Abmahnungen wegen angeblicher Teilnahme an Tauschbörsen auch: *Papenhausen: Aktuelle Rechtsprechung zur urheberrechtlichen Störerhaftung / Filesharing*, MiKaP 2014/04.

AG Bielefeld: Tatsächliche Vermutung und sekundäre Darlegungslast in Filesharing-Fällen

Das AG Bielefeld[9] hat erhebliche Zweifel an Strömungen in der Rechtsprechung[10], nach der eine tatsächliche Vermutung dafür bestehen solle, dass dann, wenn ein geschütztes Werk der

[9] AG Bielefeld, Urteil vom 04.09.2014, Az. 42 C 45/14.

Öffentlichkeit von einer IP-Adresse aus zugänglich gemacht wird, die zum fraglichen Zeitpunkt einer bestimmten Person zugeteilt ist, diese Person für die Rechtsverletzung verantwortlich ist.

Das AG Bielefeld[11] führt dazu aus: „Die Annahme einer derartigen tatsächlichen Vermutung begegnet in Haushalten, in denen mehrere Personen selbständig und unabhängig Zugang zum Internet haben, bereits grundsätzlichen Bedenken.

Das Aufstellen einer tatsächlichen Vermutung setzt voraus, dass es einen empirisch gesicherten Erfahrungssatz aufgrund allgemeiner Lebensumstände dahingehend gibt, dass ein Anschlussinhaber seinen Internetzugang in erster Linie nutzt und über Art und Weise der Nutzung bestimmt und diese mit Tatherrschaft bewusst kontrolliert. Ein derartiger Erfahrungssatz existiert nicht. Die alltägliche Erfahrung in einer Gesellschaft, in der das Internet einen immer größeren Anteil einnimmt und nicht mehr wegzudenken ist, belegt vielmehr das Gegenteil. Wenn sich der Internetanschluss in einem Mehrpersonenhaushalt befindet, entspricht es vielmehr üblicher Lebenserfahrung, dass jeder Mitbewohner das Internet selbständig nutzen darf, ohne dass der Anschlussinhaber Art und Umfang der Nutzung bewusst kontrolliert (AG Düsseldorf, Urteil vom 19.11.2013 - 57 C 3144/13). Dies entspricht auch einer amtlichen Statistik zur Internetnutzung und Verteilung der Anschlüsse, wonach Gemeinschaftsanschlüsse den Regelfall darstellen und somit kein entsprechender Erfahrungssatz existiert, nach welchem ein Internetanschluss allein durch den Anschlussinhaber genutzt wird (Zimmermann, MMR 2014, 368). Dies hat auch der BGH erkannt und daher die tatsächliche Vermutung der Verantwortlichkeit des Anschlussinhabers zwar nicht abgeschafft, ihren Anwendungsbereich jedoch erheblich eingeschränkt. Nach den im BearShare-Urteil aufgestellten Grundsätzen (BGH, Urteil vom 08.01.2014 – I ZR 169/12) ist eine tatsächliche Vermutung für eine Täterschaft des Anschlussinhabers nicht begründet, wenn zum Zeitpunkt der Rechtsverletzung auch andere Personen diesen Anschluss benutzen konnten. Zur Widerlegung der tatsächlichen Vermutung reicht es aus, dass der Anschlussinhaber vorträgt, der Internetanschluss sei zum Zeitpunkt der Rechtsverletzung nicht hinreichend gesichert gewesen oder bewusst anderen Personen zur Nutzung überlassen worden. Insoweit trägt nach allgemeinen prozessualen Grundsätzen nicht der Anschlussinhaber, sondern vielmehr die klagende Partei die Beweislast dafür, dass der Internetanschluss hinreichend gesichert war und nicht anderen Personen zur Nutzung überlassen wurde.

Den Anschlussinhaber trifft jedoch eine sekundäre Darlegungslast, sofern über seinen Internetanschluss eine Rechtsverletzung begangen wird. Dieser Darlegungslast genügt der Anschlussinhaber, sofern er vorträgt, ob und gegebenenfalls welche anderen Personen selbständigen Zugang zu seinem Internetanschluss hatten und damit als mögliche Täter der Rechtsverletzung in Betracht kommen. Nach Ansicht des BGH ist der Anschlussinhaber insoweit im Rahmen des Zumutbaren auch zu Nachforschungen verpflichtet. Der BGH unterlässt es jedoch, nähere Ausführungen dazu zu machen, welche Ermittlungsmaßnahmen im Allgemeinen und welche im Besonderen unter Berücksichtigung verwandtschaftlicher oder enger persönlicher Beziehungen zwischen Anschlussinhaber und Nutzer möglich und zumutbar sind. Aus der

[10] Das AG Bielefeld verweist in diesem Rahmen auf den BGH, Urteil vom 12.05.2010, Az. I ZR 121/08, Sommer unseres Lebens.
[11] AG Bielefeld, Urteil vom 04.09.2014, Az. 42 C 45/14.

Wortwahl („insoweit" im Leitsatz und „in diesem Umfang" in den Entscheidungsgründen) ergibt sich zweifelsfrei, dass der Anschlussinhaber nur zu ermitteln hat, welchen anderen Personen bewusst die Möglichkeit zur Mitbenutzung des Internetanschlusses eingeräumt wurde. Hierbei handelt es sich um dem Anschlussinhaber ohne weiteres mögliche und zumutbare Angaben, wobei der Anschlussinhaber die weiteren Nutzer so genau zu bezeichnen hat, dass dem Anspruchssteller eigene Ermittlungen zur Identität des eigentlichen Täters, beispielsweise im Rahmen einer sog. Berechtigungsanfrage ermöglicht werden. Die Nachforschungspflicht geht nicht soweit, dass der Anschlussinhaber ermitteln muss, wer die Rechtsverletzung tatsächlich begangen hat. Eine derart weitgehende Nachforschungspflicht lässt sich auch nicht mit dem Hinweis des BGH auf die Recherchepflicht beim Verlust oder einer Beschädigung von Transportgut (BGH, TranspR 2013, 437) begründen, da dem Frachtführer weitreichende, nicht nur auf die eigene Entlastung beschränkte Auskünfte schon wegen der gegenseitigen vertraglichen Treuepflichten (§ 241 Abs. 2 BGB) zumutbar sind (Neurauter, GRUR 2014, 657, 662). Darüber hinaus fehlt es in diesen Fällen an dem erforderlichen qualifizierten Verschulden, da die Zurverfügungstellung eines privaten Internetanschlusses nicht mit der gewerblichen Tätigkeit eines Frachtführers zu vergleichen ist (Brüggemann, CR 2014, 476)." [12]

Siehe zu Abmahnungen wegen angeblicher Teilnahme an Tauschbörsen auch: *Papenhausen: Aktuelle Rechtsprechung zur urheberrechtlichen Störerhaftung / Filesharing*, MiKaP 2014/04.

AG Koblenz: Software Observer ungeeignet, Urheberrechtsverletzungen zu ermitteln

Nach einem Hinweisbeschluss des AG Koblenz[13] ist die Software „Observer" ungeeignet, Urheberrechtsverletzungen im Rahmen von Filesharing zu ermitteln[14]: „Unabhängig davon wäre die Klage auch unschlüssig hinsichtlich der klägerseits behaupteten, vom Beklagten bestrittenen Richtigkeit der Ermittlung der IP-Adresse des Beklagten zum Internetanschluss, von dem aus die behauptete Urheberrechtsverletzung vom 24.12.2009 begangen worden sein soll. Sowohl das OLG Köln im Beschluss vom 20.01.2012, AZ: 6 W 242/11, als auch das LG Berlin mit Urteil vom 03.05.2011, AZ: 16 O 55/11, haben festgestellt, dass die Ermittlungen der klägerseits eingesetzten Fa. Guardaley Ltd. und die von dieser benutzten Software „Observer" ungeeignet sind, Urheberrechtsverletzungen zutreffend zu ermitteln. Auch das AG Frankenthal hat in einem aktuellen Urteil vom 23.06.2014 (Az: 3b C 145/14) erhebliche Zweifel an der Zuverlässigkeit der auch im vorliegenden Fall eingesetzten Ermittlungssoftware Observer der Fa. Guardaley Ltd geäußert und die dortige Klage vollumfänglich abgewiesen." [15]

[12] Siehe zur sekundären Darlegungslast in Filesharing-Fällen auch: AG Landshut, Urteil vom 28.11.2014, Az. 10 C 1392/14.
[13] AG Koblenz, Hinweisbeschluss vom 02.01.2015, Az. 153 C 3184/14.
[14] Siehe zu Abmahnungen wegen angeblicher Teilnahme an Tauschbörsen auch: Papenhausen: Aktuelle Rechtsprechung zur urheberrechtlichen Störerhaftung / Filesharing, MiKaP 2014/04.
[15] AG Koblenz, Hinweisbeschluss vom 02.01.2015, Az. 153 C 3184/14.

BGH: Kein Entgelt für Papierrechnung, kein Pfand für SIM-Karte/AGB-Recht

Nach dem BGH[16] darf ein Mobilfunkanbieter in den Allgemeinen Geschäftsbedingungen (AGB) kein Entgelt für Papierrechnung verlangen.

Die vom BGH hierzu aufgestellten Leitsätze lauten wie folgt:

„Die Klausel in Allgemeinen Geschäftsbedingungen eines Mobilfunkanbieters, nach der für die Überlassung der SIM-Karte ein "Pfand" in Höhe von 29,65 € erhoben wird, das als "pauschalierter Schadensersatz" einbehalten wird, sofern der Kunde die Karte nicht innerhalb von drei Wochen nach Ablauf der Gültigkeitsdauer und Beendigung des Kundenverhältnisses in einwandfreiem Zustand zurücksendet, ist unwirksam.

Die Klausel in Allgemeinen Geschäftsbedingungen eines Mobilfunkanbieters, nach der für die Zusendung einer Rechnung in Papierform (zusätzlich zur Bereitstellung in einem Internetkundenportal) ein gesondertes Entgelt anfällt, ist jedenfalls dann unwirksam, wenn der Anbieter sein Produkt nicht allein über das Internet vertreibt."

LG Darmstadt: Bankkunde trägt Risiko beim Online-Banking (Volltext)

Das LG Darmstadt[17] hat entschieden, dass der Bankkunde das Risiko beim Online-Banking im Falle eines sog. Man-in-the-Middle-Angriffs trägt.

Das LG Darmstadt[18] führt hierzu u. a. aus:

„Tatbestand:

Die Klägerin begehrt von der Beklagten Ersatz für zwei Überweisungsvorgänge mittels Online-Banking. Die Klägerin war Bankkundin der Beklagten. Um ihre Bankgeschäfte per Internet (Online) zu tätigen, nutzte die Klägerin das ihr von der Beklagten zur Verfügung gestellte sog. Smart-TAN-plus Verfahren.

Zur Vornahme von Banküberweisungen mittels des Smart-TAN-plus-Verfahrens meldet sich der Kunde im Internet zunächst über die Homepage der Beklagten durch Eingabe eines sog. Privat-Keys (eine dem Kunden zugeordnete individuelle Nummer, die einer Kundennummer vergleichbar ist) sowie einer nur dem Bankkunden bekannten PIN-Nummer an. Sodann gibt er am Bildschirm die Überweisungsdaten (Empfänger, dessen Kontonummer und BLZ bzw. dessen IBAN und BIC sowie zu überweisender Betrag) in eine auf der Homepage der Beklagten bereitgestellte Maske ein. Zur Autorisierung der Überweisung verwendet der Bankkunde anschließend ein ihm von der Beklagten zur Verfügung gestelltes gesondertes Karten-Lesegerät mit Display (sog. TAN-Generator), in das er vor jeder Transaktion zunächst seine EC-Karte einführen muss. An den TAN-Generator werden die auf der Bildschirmmaske eingegebenen Überweisungsdaten

[16] BGH, Urteil vom 09.10.2014, Az. III ZR 32/14.
[17] LG Darmstadt, Urteil vom 28.08.2014, Az. 28 O 36/14.
[18] LG Darmstadt, Urteil vom 28.08.2014, Az. 28 O 36/14.

übermittelt, was sich durch eine optische Schnittstelle (Grafik) auf dem PC-Bildschirm des Bankkunden sowie durch Anhalten des TAN-Generators an den PC-Bildschirm und eine damit einhergehende Datenübertragung durch Lichtsignale über die optischen Sensoren des TAN-Generators vollzieht (sog. Flickering). Alternativ kann der Bankkunde die Überweisungsdaten, die er bereits auf der Bildschirmmaske eingetragen hat, nochmals manuell in den TAN-Generator eingeben. Nach optischer oder manueller Übermittlung der Überweisungsdaten an den TAN-Generator werden die Überweisungsdaten (Empfänger, dessen Kontonummer und BLZ sowie zu überweisender Betrag) auf dem Display des TAN-Generators angezeigt. Der Bankkunde muss die Überweisungsdaten durch Drücken der O.K.-Taste des TAN-Generators bestätigen. Im Anschluss daran errechnet der TAN-Generator auf Grundlage der an ihn zuvor übermittelten Daten sowie auf Basis der von der EC-Karte ausgelesenen Chipkartennummer und Kundenkontonummer eine auf die konkrete Überweisung bezogene sog. TAN. Diese wird von dem Bankkunden in die Überweisungsmaske auf dem PC-Bildschirm eingegeben. Das Online-Banking-System der Beklagten - konkret: deren Bankserver - nimmt dieselbe Berechnung zur Ermittlung der auftragsbezogenen TAN vor wie zuvor der TAN-Generator. Stimmen die vom Bankkunden eingegebene und die vom TAN-Generator errechnete (auftragsbezogene) TAN mit der vom Bankserver ermittelten - auftragsbezogenen - TAN überein, wird die Transaktion von dem Online-Banking-System der Beklagten angenommen und ausgeführt.

Die Manipulationsmöglichkeiten und die Systemsicherheit des Smart-TAN-plus-Verfahrens sind zwischen den Parteien streitig.

Die Klägerin nutzte das Smart-TAN-plus-Verfahren der Beklagten auf Grundlage der zwischen den Parteien vereinbarten Sonderbedingungen für das Online-Banking (Bl. 81 f. d. A.). Diese sehen unter Ziffer 7.4 vor, dass der Bankkunde verpflichtet ist, Daten aus seinem Online-Banking-Auftrag (z. B. der Betrag, Kontonummer des Zahlungsempfängers), die er über ein Chipkartenlesegerät mit Display zur Bestätigung angezeigt erhält, vor der Bestätigung auf Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Die Parteien vereinbarten zudem, dass Verfügungen über das Online-Banking auf 20.000,00 € täglich begrenzt werden.

Am 12.11. und am 27.11.2013 führte der Geschäftsführer der Klägerin mittels des Smart-TAN plus Verfahrens mehrere Überweisungen von dem Geschäftskonto bei der Beklagten aus (am 12.11.2013 vier Überweisungen in der Zeit von 16:42 bis 16:46 Uhr, am 27.11.2013 fünf Überweisungen in der Zeit vom 15:52 bis 16:02 Uhr). An beiden Tagen war allein der Geschäftsführer der Klägerin im Besitz der EC-Karte, die er zur Bedienung des TAN-Generators verwendete. Der Computer, von dem aus der Geschäftsführer der Klägerin die Überweisungen vornahm, war durch einen aktuellen Virenschutz (Avira Free Antivirus) und eine Firewall gesichert, Betriebssystem und Internetbrowser waren auf einem aktuellen Stand. Der Geschäftsführer der Klägerin stellte am 12.11. und am 27.11.2013 weder grobe grammatische oder orthografische Fehler auf der von ihm aufgerufenen Homepage der Beklagten noch sonstige Auffälligkeiten fest. Es kam am 12.11. und am 27.11.2013 noch zu weiteren Belastungen des Geschäftskontos der Klägerin. Diese sind streitgegenständlich. Konkret wurde am 12.11. um 16:37 Uhr das Konto der Klägerin mit 9.500,00 € zugunsten eines Zahlungsempfängers „(…)" mit

dem Verwendungszweck „(…)" und am 27.11.2013 um 15:44 Uhr mit 9.000,00 € zugunsten eines Zahlungsempfängers „(…) mit dem Verwendungszweck „(…) belastet.

Die beiden Zahlungsempfänger sind der Klägerin nicht bekannt. Die Klägerin wollte die beiden streitgegenständlichen Zahlungsvorgänge auch nicht veranlassen. Vielmehr gab ihr Geschäftsführer in die ihm auf dem PC-Bildschirm ersichtliche Überweisungsmaske am 12.11. und am 27.11.2013 Daten für eine Überweisung an eine Firma A GmbH & Co. KG ein. Diese beiden Zahlungsaufträge gingen der Beklagten jedoch nicht zu und wurden von ihr daher auch nicht ausgeführt.

In dem „Nachweisprotokoll der SEPA-Aufträge" der Beklagten wurden die beiden streitgegenständlichen Belastungen des Klägerkontos als Online-Überweisungen mittels TAN-Generator und dabei erzeugter übereinstimmender TAN des TAN-Generators und des Bankservers erfasst. Ausweislich des Protokolls sollen die Transaktionen unter Verwendung der Bankcard des Geschäftsführers der Klägerin, Herrn B, und unter Verwendung dessen „Private Key" und PIN-Nummer beim Einloggen erfolgt sein (Bl. 79 f. d. A.).

Am 29.11.2013 bemerkte die Klägerin die beiden streitgegenständlichen Zahlungsvorgänge erstmals und stellte Strafanzeige. Die staatsanwaltschaftlichen Ermittlungen ergaben, dass die Überweisung am 27.11.2013 von einer IP-Adresse mit 31.18.64.5 vorgenommen wurde, die zu einem bei C verwalteten Kontingent gehört. Weitere Erkenntnisse brachten die Ermittlungen nicht, da sämtliche Daten bereits gelöscht / nicht mehr gespeichert waren.

Ebenfalls am 29.11.2013 versuchte der Geschäftsführer der Klägerin vergeblich, die Beklagte über eine Notfallhotline zu erreichen und über die aus ihrer Sicht unberechtigten Kontenbelastungen zu informieren.

Mit Schreiben ihres Prozessbevollmächtigten vom 02.12.2013 forderte die Klägerin die Beklagte zur Rückzahlung der abgebuchten 18.500,00 € unter Fristsetzung bis zum 05.12.2013 auf (Bl. 39 d. A.). Am selben Tag unterrichtete die Klägerin die Beklagte von den aus ihrer Sicht nicht autorisierten streitgegenständlichen Kontenbelastungen (Bl. 8 d. A.).

Im Januar 2014 warnte die Beklagte ihre Kunden auf ihrer Homepage davor, dass gefälschte E-Mails in betrügerischer Absicht scheinbar in ihrem Namen versendet werden. In diesen E-Mails werde der Bankkunde aufgefordert, auf einen Link zu klicken. Dieser Link diene jedoch einzig dazu, den Computer des Bankkunden mit Schadcode („Trojaner") zu kompromittieren (Bl. 101 d. A.).

Die Klägerin hat das Vertragsverhältnis mit der Beklagten mittlerweile unter Auflösung des streitgegenständlichen Geschäftskontos gekündigt.

Die Klägerin behauptet, ihr Geschäftsführer habe bei jeder Überweisung mittels Online-Banking die Überweisungsdaten auf der Maske des Bildschirms mit den auf dem Display des TAN-Generators angezeigten Überweisungsdaten abgeglichen und dabei keine Auffälligkeiten

festgestellt. Wäre die Beklagte über ihre Notfallhotline am 29.11.2013 zu erreichen gewesen, so hätte die Rückbuchung der Kontobelastung vom 27.11.2013 noch erfolgen können. Die Klägerin ist der Ansicht, die Beklagte habe dadurch, dass sie erst im Januar 2014 vor den Gefahren betrügerischer E-Mails gewarnt habe, eine Vertragspflicht verletzt. Die Beklagte habe zudem dadurch eine weitere Pflichtverletzung begangen, dass sie die beiden streitgegenständlichen Überweisungen mit „derart hohen Beträgen" ausgeführt habe, ohne dass - unstreitig - ein unterschriebener Überweisungsträger vorgelegt wurde.

Die Klägerin beantragt,

1.) die Beklagte zu verurteilen, an sie 18.500,00 € nebst Zinsen in Höhe von 8 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 06.12.2013 zu zahlen;

2.) die Beklagte zu verurteilen, an sie 562,16 € außergerichtliche Rechtsverfolgungskosten nebst Zinsen in Höhe von Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, der Geschäftsführer der Klägerin, Herr B, habe die auf dem Display des TAN-Generators angezeigten Daten der beiden streitgegenständlichen Überweisungen durch Drücken der O.K.-Taste bestätigt und damit autorisiert. Das sei auch dann der Fall, wenn diese von dritter Seite manipuliert worden seien. In diesem Fall stünden der Beklagten Schadensersatzansprüche gegen die Klägerin zu, mit der sie - unstreitig - die Aufrechnung erklärt (Bl. 65 d. A.).

Das Gericht hat Beweis erhoben durch Einholung eines schriftlichen Gutachtens des Sachverständigen Dr.-Ing. D. Hinsichtlich des Ergebnisses der Beweisaufnahme wird auf das Gutachten vom 01.07.2014 verwiesen. Im Übrigen wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe:

Die zulässige Klage ist unbegründet. Die Klägerin kann von der Beklagten weder die Zahlung von 18.500,00 € noch die Erstattung vorgerichtlicher Rechtsanwaltskosten von 562,16 € verlangen.

Der zwischen den Parteien bestehende Girovertrag mitsamt den Sonderbedingungen für das Online-Banking ist ein Geschäftsbesorgungsvertrag, der die Erbringung von Zahlungsdiensten zum Gegenstand hat, § 675c Abs. 1 BGB. Der Klägerin steht aus diesem Vertrag gegen die Beklagte kein Anspruch aus § 675u S. 2 BGB auf Zahlung von 18.500,00 € zu.

Gem. § 675u S. 2 BGB ist der Zahlungsdienstleister verpflichtet, das Zahlungskonto des Zahlers im Falle eines nicht autorisierten Zahlungsvorganges wieder auf den Stand zu bringen, den es ohne die nicht autorisierte Belastung hätte. Dieser Anspruch ist zwar grundsätzlich nur auf Valutakorrektur mittels Stornobuchung gerichtet. Der Zahler hat jedoch dann einen Anspruch auf Auszahlung des zu Unrecht belasteten Betrages, wenn die Kontobeziehung inzwischen unter Ausgleich des Saldos aufgelöst ist (vgl. Nobbe, in: Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2. Aufl. 2013, § 675u BGB Rn. 44). Das ist hier der Fall, da die Vertragsbeziehung der Parteien mittlerweile beendet ist.

Die Voraussetzungen des § 675u S. 2 BGB liegen nicht vor. Zwar wurde das bei der Beklagten unterhaltene Geschäftskonto der Klägerin durch die beiden streitgegenständlichen Zahlungsvorgänge vom 12.11. und 27.11.2013 belastet. Diese Zahlungsvorgänge waren jedoch von der Klägerin autorisiert im Sinne des § 675j Abs. 1 BGB.

Im Einzelnen: Autorisierung im Sinne des § 675j Abs. 1 BGB meint die Erklärung des Einverständnisses mit dem Zahlungsvorgang als tatsächliches Ereignis (Palandt/Sprau, a. a. O., § 675j Rn. 3). Die Autorisierung ist eine Willenserklärung und kann gem. § 675j Abs. 1 S. 4 BGB auch mittels eines bestimmten Zahlungsauthentifizierungsinstruments - beim Online Banking mittels PIN und TAN (vgl. Palandt/Sprau, a. a. O., § 675j Rn. 6) - erteilt werden. Für die Autorisierung des Zahlungsvorganges ist die Beklagte als Zahlungsdienstleister darlegungs- und beweisbelastet, § 675w S. 1 BGB (vgl. Schmalenbach, in: Bamberger/Roth, Beck'scher Online-Kommentar BGB, Stand: 01.05.2014, § 675w Rn. 7). Dabei benennen § 675w S. 1 u. S. 2 BGB bestimmte Mindestanforderungen, die gegeben sein müssen, um eine Autorisierung anzunehmen (vgl. Nobbe, a. a. O., § 675 w BGB Rn. 16). Diese Mindestvoraussetzungen hat die Beklagte dargetan. Denn beim Online-Banking erbringt der Zahlungsdienstleister den Nachweis der Authentifizierung gem. § 675w S. 2 BGB, wenn er belegt, dass Kundenkennung, PIN und TAN überprüft wurden (vgl. Palandt/Sprau, BGB, 73. Aufl. 2014, § 675w Rn. 3). Diesen Anforderungen hat die Beklagte durch Vorlage des Nachweis-Protokolls der SEPA-Aufträge vom 12.11. und 27.11.2013 (Bl. 79 f. d. A.) sowie des Protokolls der „SB-Karte-PRK (…) (Bl. 78 d. A.) genügt, da aus den Protokollen ersichtlich ist, dass die vorgenannten Nachweise überprüft wurden und Grundlage der Transaktionen waren. Die Beklagte hat auch den nach § 675w S. 1 geforderten Nachweis, dass der Zahlungsvorgang ordnungsgemäß aufgezeichnet, verbucht sowie nicht durch eine Störung beeinträchtigt wurde, durch Vorlage des Protokolls der SEPA-Aufträge vom 12.11. und 27.11.2013 (Bl. 79 f. d. A.) geführt. Die ordnungsgemäße Aufzeichnung, Verbuchung und störungsfreie, keine Auffälligkeiten aufweisende technische Abwicklung kann nämlich durch aussagekräftige Transaktionsprotokolle belegt werden, wenn sich aus diesen ergibt, dass der Zahlungsvorgang nicht durch einen technischen Zusammenbruch oder eine andere Panne beeinträchtigt wurde (vgl. Caspar, in: MüKo-BGB, 6. Aufl. 2012, § 675w Rn. 6). Das von der Beklagten vorgelegte Protokoll beinhaltet SEPA-Überweisungen, die über das Zahlungsdienstesystem der Beklagten an den streitgegenständlichen Tagen erfolgten. Ausweislich der Protokolle sind unmittelbar nach den streitgegenständlichen Überweisungen am 12.11. und am 27.11.2013 auch andere Zahlungsvorgänge von anderen Kunden der Beklagten abgewickelt worden, sodass ein technischer Zusammenbruch o. ä. ausscheidet. Sind die Mindestvoraussetzungen des § 675w S. 1 u. S. 2 BGB gegeben, reicht dies nach § 675w S. 3

BGB nicht stets für den Nachweis, dass der Bankkunde die Zahlung autorisiert hat (vgl. Nobbe, a. a. O., § 675 w BGB Rn. 17). Vielmehr müssen die Umstände des Einzelfalles gem. § 286 Abs. 1 ZPO berücksichtigt werden (vgl. Caspar, a. a. O., § 675w Rn. 9; Palandt/Sprau, a. a. O., § 675w Rn. 4). Nach dem Ergebnis der Beweisaufnahme steht für das Gericht mit der von § 286 Abs. 1 ZPO geforderten Gewissheit fest, dass eine Autorisierung der beiden streitgegenständlichen Zahlungsvorgänge durch die Klägerin vorliegt. Die Klägerin hat ihr Einverständnis zu den beiden streitgegenständlichen Zahlungsvorgängen zwar nicht selbst erteilt, sondern wurde Opfer eines sog. „Man-in-the-Middle-Angriffs". Ihr ist die mittels des Zahlungsauthentifizierungsinstruments PIN und TAN erteilte Zustimmung des „Angreifers" zu den manipulierten Zahlungsvorgängen jedoch nach Rechtsscheinsgrundsätzen zuzurechnen.

Im Einzelnen: Die Klägerin kannte die beiden (vermeintlich) aus Lettland stammenden (ggf. fiktiven) Zahlungsempfänger nicht und stand mit ihnen insbesondere auch nicht in einer Geschäftsbeziehung. Die Klägerin besaß daher keine Veranlassung, derart hohe Auslandsüberweisungen an die beiden Zahlungsempfänger zu tätigen. Hinzu kommt, dass die Klägerin an den beiden streitgegenständlichen Tagen Überweisungen an eine A GmbH & Co KG ausführen wollte und deren Daten in die auf dem PC-Bildschirm ersichtliche Überweisungsmaske eingab. Diesem Umstand stellte die Beklagte mit Schriftsatz vom 21.07.2014, S. 3 (Bl. 135 d. A.), unstreitig. Nach den überzeugenden Feststellungen des Sachverständigen Dr. D ist es für einen betrügerischen sog. „Man-in-the-Middle-Angriff" geradezu typisch, dass eine beabsichtigte Überweisung, deren Daten in die (manipulierte) Überweisungsmaske auf dem PC-Bildschirm eingegeben werden, nicht an die Bank übermittelt und von dieser daher auch nicht ausgeführt wird. Denn der „Angreifer" kann keine eigenen, vom Benutzer losgelösten Transaktionen starten, sondern muss immer eine vom dem Zahler gewollte Aktion in seinem Sinne verändern (manipulieren). Der Klägerin ist das Einverständnis zu den beiden streitgegenständlichen Zahlungsvorgängen jedoch nach den Grundsätzen der Anscheinsvollmacht zuzurechnen, die auf die Autorisierung nach § 675j Abs. 1 BGB entsprechend anwendbar sind (vgl. Palandt/Sprau, a. a. O., § 675j Rn. 2; Omlor, in: Staudinger, BGB, Neub. 2012, § 675u Rn. 6). Dies ergibt sich zur Überzeugung des Gerichts aus den nachvollziehbaren Ausführungen des Sachverständigen, der Folgendes feststellte: Das Smart-Tan-plus-Verfahren weist eine hohe Systemsicherheit auf. Aus technischer Sicht ist es nach derzeitigem Stand so gut wie ausgeschlossen, dass bei Verwendung dieses Verfahrens tatsächlich erfolgte Online-Überweisungen nicht von dem Bankkunden selbst vorgenommen wurden. Auf Grundlage der überzeugenden Feststellungen des Sachverständigen bestehen bei dem Smart-TAN-plus-Verfahren im konkreten Fall lediglich zwei in Betracht zu ziehende Manipulationsmöglichkeiten, wobei es sich bei beiden um sog. „Man-in-the-Middle-Angriffe" handelt: Entweder wurde der Angriff durch eine sich auf dem Computer der Klägerin befindliche Schadsoftware (Trojaner) oder durch eine anderweitige Umleitung der Netzwerkpakete auf ein drittes System ermöglicht. Bei diesen beiden Szenarien gab der Geschäftsführer der Klägerin die Daten der von ihm jeweils beabsichtigten Überweisung an die A GmbH & Co. KG in die ihm auf dem PC-Bildschirm ersichtliche (manipulierte) Überweisungsmaske ein. Im Hintergrund - und damit für den Geschäftsführer nicht sichtbar - wurden die streitgegenständlichen Überweisung vorbereitet und deren Daten über die optische Schnittstelle des Bildschirms an den TAN-Generator übermittelt. Der TAN-Generator erzeugte jeweils eine TAN, die für die streitgegenständliche Überweisung bestimmt und auf diese bezogen

war. Auf dem Display des TAN-Generators wurden - für den Geschäftsführer der Klägerin sichtbar - die Daten (Empfänger, dessen Kontonummer und BLZ bzw. IBAN und BIC sowie zu überweisender Betrag) der streitgegenständlichen Überweisungen angezeigt. Sodann drückte der Geschäftsführer der Klägerin trotz dieser Anzeige die O.K.-Taste und erzeugte damit die TAN für die streitgegenständlichen Überweisungen. Anschließend gab der Geschäftsführer der Klägerin die erzeugte TAN in die Online-Überweisungsmaske ein. Auf dieser war wegen des betrügerischen Angriffs nach wie vor die von ihm gewollte Überweisung an die A GmbH & Co. KG angezeigt. Der „Angreifer" fing die derart am 12.11. und am 27.11 erzeugten TAN ab und nutzte sie sodann für die streitgegenständlichen Überweisungen. Bei dieser Sachlage ist der Klägerin die Zustimmung zu den beiden streitgegenständlichen Überweisungen nach den entsprechend anwendbaren Grundsätzen der Anscheinsvollmacht zuzurechnen. Eine Anscheinsvollmacht ist gegeben, wenn der Vertretene (hier: die Klägerin) das Handeln des Scheinvertreters (hier: des „Angreifers") nicht kennt, er es aber bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können, und wenn der Geschäftspartner (hier: die Beklagte) annehmen durfte, der Vertretene kenne und billige das Handeln des Vertreters. Bei dem hier vorliegenden, mit einer Identitätstäuschung verbundenen Handeln unter fremdem Namen ist bei Anwendung dieser Grundsätze auf das Verhalten des Namensträgers abzustellen (BGH, Urt. v. 11.05.2011 - VIII ZR 289/09, Rn. 16 - juris; Palandt/Ellenberger, a. a. O., § 172 Rn. 11). Diese Voraussetzungen der Rechtsscheinhaftung liegen vor. Aus den überzeugenden Ausführungen des Sachverständigen folgt, dass die Klägerin den „Man-in-the-Middle-Angriff" hätte erkennen und verhindern können. Denn die Klägerin hatte die Möglichkeit, durch Kontrolle der auf dem Display des TAN-Generators angezeigten Überweisungsdaten die Manipulation der Zahlungsvorgänge zu erkennen und hätte sodann den Zahlungsvorgang abbrechen können. In diesem Fall hätten die von ihr erzeugten Daten nicht missbraucht werden können. Die Klägerin hat eine Kontrolle der auf dem Display angezeigten Überweisungsdaten offenbar aus Unachtsamkeit nicht vorgenommen und damit auch gegen ihre Pflicht aus Ziff. 7.4 der Allgemeinen Sonderbedingung für das Online-Banking verstoßen.

Die Beklagte durfte auch von einer Kenntnis und Billigung der streitgegenständlichen Zahlungsvorgänge durch die Klägerin ausgehen. Denn die beiden streitgegenständlichen Überweisungen wurden unter Verwendung der EC-Karte der Klägerin, nach Einloggen mit PIN und Private-Key auf der Homepage der Beklagten und unter Verwendung der TAN ausgeführt, die der TAN-Generator der Klägerin erzeugte und anzeigte (vgl. insb. S. 18 des Sachverständigengutachtens). Da Zahlungsauthentifizierungsinstrumente (TAN, PIN) gerade dazu dienen, die Ausführung des Zahlungsvorganges eindeutig der Klägerin als Veranlasserin zuzuordnen (vgl. Palandt/Sprau, a. a. O., § 675j Rn. 6), durfte die Beklagte von Kenntnis und Billigung der Klägerin annehmen. Das Smart-TAN-plus-Verfahren bietet nach den Ausführungen des Sachverständigen auch eine ausreichende Systemsicherheit, um einen solchen Vertrauenstatbestand zu begründen (vgl. zur Bedeutung der Systemsicherheit für die Annahme des Vertrauenstatbestandes: BGH, Urt. v. 11.05.2011 - VIII ZR 289/09, Rn. 18 - juris): Soweit Manipulationsmöglichkeiten in Betracht kommen, kann die Ausführung des manipulierten Zahlungsvorganges durch Kontrolle der auf dem Display des TAN-Generators angezeigten Überweisungsdaten vermieden werden.

Die Annahme einer Anscheinsvollmacht setzt in der Regel weiter voraus, dass das Verhalten, das den Rechtsschein einer Bevollmächtigung erzeugt, von einer gewissen Dauer und Häufigkeit ist (Palandt/Ellenberger, a. a. O., § 172 Rn. 12 m w. N.). Ob dieses Erfordernis im vorliegenden Fall erfüllt sein muss, ist zweifelhaft, kann aber letztlich offen bleiben. Das ergibt sich aus Folgendem: In der Sache geht es vorliegend darum, ob die Beklagte aufgrund der ihr übermittelten personalisierten und transaktionsbezogenen Sicherheitsmerkmale (§ 675j Abs. 1 S. 4 BGB) davon ausgeht durfte, dass der Zahlungsvorgang mit Einverständnis der Klägerin erfolgte. Hierfür kann die wiederholte Manipulation der Zahlungsvorgänge durch einen „Angreifer" richtigerweise keinen Vertrauenstatbestand begründen, da eine (erfolgreiche) Manipulation als solche für den Rechtsverkehr gar nicht erkennbar ist (vgl. Faust, JuS 2011, 1027 (1028); Schinkels, LMK 2011, 320461). Denn ebenso wie bei einem nicht manipulierten Zahlungsvorgang wird dem Zahlungsdienstleister bei einem „Man-in-the-Middle-Angriff" die Zustimmung (unterschiedslos) einzig mittels des Zahlungsauthentifizierungsinstruments (PIN, TAN) erteilt. Das drängt dazu, die Grundsätze der Anscheinsvollmacht auf die vorliegende Frage lediglich entsprechend anzuwenden (vgl. Hauck, JuS 2011, 967 (969)) und auf das Kriterium einer gewissen Dauer und Häufigkeit für die Annahme des Vertrauenstatbestands zu verzichten (Härting, BB 2011, 2187 (2188)).

Der Bundesgerichtshof hat im Fall einer unberechtigten Nutzung eines eBay-Kontos für das Vorliegen einer Anscheinsvollmacht jedoch eine gewisse Häufigkeit oder Dauer der unbefugten Verwendung gefordert (BGH, Urt. v. 11.05.2011 - VIII ZR 289/09, Rn. 18 - juris).[19] Fehle es hieran, läge kein Vertrauenstatbestand vor, auf den sich der Rechtsverkehr stützen könne. Zur Begründung führt der Bundesgerichtshof an, dass angesichts des derzeit vorhandenen Sicherheitsstandards im Internet auch bei einem eBay-Account nicht zuverlässig geschlossen werden könne, dass unter einem registrierten Mitgliedsnamen ausschließlich dessen tatsächlicher Inhaber auftritt (BGH, a. a. O.). Für die Annahme des Vertrauenstatbestandes soll damit das Erfordernis einer gewissen Dauer und Häufigkeit die geringe Systemsicherheit und Missbrauchsanfälligkeit kompensieren. Damit liegt nahe, nach Maßgabe der Rechtsprechung des Bundesgerichtshofs vorliegend auf das Kriterium einer gewissen Dauer oder Häufigkeit für eine Zurechnung nach Rechtsscheinsgrundsätzen zu verzichten. Denn nach den bereits dargestellten überzeugenden Ausführungen des Sachverständigen weist das Smart-TAN-plus-Verfahren eine hohe Systemsicherheit mit lediglich wenigen Manipulationsmöglichkeiten auf. Der Bankkunde kann die Manipulation zudem dadurch verhindern, dass er die auf dem Display des TAN-Generators angegeben Überweisungsdaten vor dem Drücken der O. K. Taste kontrolliert. Abs. 51
Letztlich kann die Frage, ob es vorliegend einer gewissen Dauer oder Häufigkeit mittels „Man-in-the-Middle-Angriffen" manipulierter Zahlungsvorgänge bedarf, offen bleiben. Denn die Klägerin wurde Opfer zweier „Man-in-the-Middle-Angriffe". Eine gewisse Häufigkeit und Dauer der Missbrauchsfälle ist damit gegeben.

Es liegen auch die weiteren Voraussetzungen einer Rechtsscheinshaftung der Klägerin vor. So bestand der Rechtsschein, die Klägerin habe die beiden streitgegenständlichen Zahlungsvorgänge veranlasst, auch und gerade im Zeitpunkt der beiden streitgegenständlichen

[19] Anmerkung Red.: Siehe zu BGH: Haftung des Kontoinhabers bei unbefugter Nutzung seines eBay-Mitgliedskontos (Urteil vom 11.05.2011, Az. VIII ZR 289/09) auch MiKaP 2011/05, S. 62.

Überweisungen und war für die beiden Zahlungsvorgänge ursächlich. Schließlich war die Beklagte auch gutgläubig. Sie hatte keinen Grund, von nicht durch die Klägerin veranlassten Zahlungsvorgängen auszugehen. Daran ändert - entgegen der Ansicht der Klägerin - auch die Tatsache nicht, dass es sich um aus Sicht der Klägerin betragsmäßig hohe und für sie seltene Auslandsüberweisungen handelte. Denn eine Bank muss weder generell prüfen, ob die Abwicklung eines Zahlungsverkehrsvorganges Risiken für einen Beteiligten begründet, noch Kontobewegungen allgemein und ohne nähere Anhaltspunkte überwachen. Ohne besondere weitere Anhaltspunkte geben auch Überweisungen mit Auslandsberührung, der Einsatz glatter Beträge und dadurch ggf. eintretende Kontoüberziehungen einer Bank keinen hinreichenden Anlass, von diesem Grundsatz eine Ausnahme zu machen. Kreditinstitute werden im bargeldlosen Zahlungsverkehr nämlich nur zum Zweck der technisch einwandfreien, einfachen und schnellen Abwicklung tätig und haben sich schon wegen dieses begrenzten Geschäftszwecks und der Massenhaftigkeit der Geschäftsvorgänge grundsätzlich nicht um die beteiligten Interessen ihrer Kunden zu kümmern (vgl. BGH, Urt. v. 24. 04.2012 - XI ZR 96/11 Rn. 32, 34 -, juris). Eine Autorisierung der beiden streitgegenständlichen Zahlungsvorgänge nach den entsprechend anwendbaren Grundsätzen der Anscheinsvollmacht liegt nach alldem vor. Die Klägerin konnte diese ihr nach Rechtsscheinsgrundsätzen zugerechneten Autorisierungen auch nicht mittels Anfechtung beseitigen, in dem sie Beklagte am 02.12.2013 über die beiden von ihr nicht selbst vorgenommenen Zahlungsvorgänge informierte und Rückzahlung verlangte. Denn das bloß tatsächliche Setzen eines rechtsscheinsbegründenden Vertrauenstatbestandes, dessen rechtsgeschäftliche Folgen auf schuldhafter Veranlassung beruhen, kann keinem Willensmangel unterliegen. Es handelt sich auch nicht um einen vergleichbaren Vorgang und berechtigt aus diesem Grund nicht zur Anfechtung (vgl. Schilken, in: Staudinger, BGB, Neub. 2009, § 167 Rn. 45 m. w. N.).

Ein Anspruch der Klägerin aus § 676u S. 2 BGB besteht nach dem Vorstehenden nicht. Weitere Anspruchsgrundlagen für das Begehren der Klägerin kommen aufgrund der abschließenden Regelung des § 675u BGB nicht in Betracht, § 675z S. 1 BGB. Selbst wenn man die Sperrwirkung des § 675z S. 1 BGB nicht auch auf Ansprüche aus § 280 I BGB erstrecken wollte, könnte die Klägerin kein Schadensersatz von der Beklagten unter dem Gesichtspunkt verlangen, dass sie an der Notfallhotline der Beklagte am 29.11.2013 niemanden erreichen konnte. Zwar folgt aus § 675m Abs. 1 Nr. 3 BGB die Verpflichtung des Zahlungsdienstleisters, sicherzustellen, dass der Zahlungsdienstleistungsnutzer durch geeignete Mittel jederzeit die Möglichkeit hat, eine Anzeige nach § 675l S. 2 BGB vorzunehmen. Es fehlte jedoch jedenfalls an der Kausalität einer etwaigen Pflichtverletzung für den streitgegenständlichen Schaden der Klägerin. Denn ausweislich der Mitteilung von C von 11.12.2013 an die Polizei Hamburg kann C den Kunden, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, nur dann ermitteln, wenn die fragliche Internetaktivität nicht länger als 48 Stunden zurückliegt (Bl. 32 d. A.). Bereits im Zeitpunkt des Bemerkens der betrügerischen Abbuchungen vom 27.11.2013 durch die Klägerin gegen 18:25 Uhr am 29.11.2013 konnten die mutmaßlichen Manipulierer der ermittelten IP-Adresse nicht mehr zugeordnet werden. Selbst wenn die Klägerin die Beklagte über die Notfallhotline erreicht hätte, wäre des demnach nicht zu einer Namhaftmachung der Manipulierer gekommen. Es fehlt an alldem an der erforderlichen Kausalität zwischen Pflichtverletzung und Schaden.

Der Klägerin steht auch kein Ersatz für die mit dem Klageantrag Ziff. 2 geltend gemachten vorgerichtlichen Kosten der Rechtsverfolgung gem. § 280 Abs. 2, 286 Abs. 1 BGB zu, der durch § 675z BGB nicht ausgeschlossen wäre (Palandt/Sprau, a. a. O., § 675z Rn. 2). Da kein Rückzahlungsanspruch der Klägerin bestand, befand sich die Beklagte trotz der Zahlungsaufforderung vom 02.12.2013 nicht im Verzug.

Die Entscheidung zu den Kosten findet ihre Grundlage in § 91 Abs. 1 S. 1 ZPO, die zur vorläufigen Vollstreckbarkeit in § 709 S. 1 u. 2. ZPO."

Anmerkung RA Papenhausen:

Das LG Darmstadt[20] vertritt im vorliegenden Fall[21] die Ansicht, dass der Bankkunde das Risiko bei einem sog. Man-in-the-Middle-Angriff beim Online-Banking trage, er demnach nicht das an einen betrügerischen Dritten angewiesene Geld von der Bank zurückerhalte, obwohl der Bankkunde im vorliegenden Fall sein Einverständnis zu den beiden streitgegenständlichen Zahlungsvorgängen unstreitig nicht selbst erteilt hatte, sondern Opfer des oben genannten Man-in-the-Middle-Angriffs wurde.

Das LG Darmstadt[22] ist der Meinung, der Bankkunde habe den Man-in-the-Middle-Angriff erkennen und verhindern können, da der Bankkunde die Möglichkeit gehabt habe, durch Kontrolle der auf dem Display des TAN-Generators angezeigten Überweisungsdaten die Manipulation der Zahlungsvorgänge zu erkennen und sodann den Zahlungsvorgang abbrechen zu können.

Letztlich stellt das Landgericht gemäß den Ausführungen des Sachverständigen fest, dass das Smart-Tan-plus-Verfahren eine hohe Systemsicherheit aufweise. Aus technischer Sicht sei es nach derzeitigem Stand so gut wie ausgeschlossen, dass bei Verwendung dieses Verfahrens tatsächlich erfolgte Online-Überweisungen nicht von dem Bankkunden selbst vorgenommen wurden.

Wichtige Hinweise:

[20] LG Darmstadt, Urteil vom 28.08.2014, Az. 28 O 36/14.
[21] Siehe in dieser Ausgabe im Volltext: LG Darmstadt, Urteil vom 28.08.2014, Az. 28 O 36/14.
[22] LG Darmstadt, Urteil vom 28.08.2014, Az. 28 O 36/14.