institut für finanzdienstleistungen e.V.

infobrief 12/2018

Montag, 31. Juli 2018 **Niklas Korff**

- Seit 1995 - **Ein Service des *iff* für die Verbraucherzentralen** - Seit 1995 -
Infobriefe im Internet: http://www.iff-hamburg.de/index.php?id=3030

Stichwörter

Haftung des Kontoinhabers für nicht autorisierte Überweisungen per Online-Banking, Urteil des LG Kiel vom 20.04.2018, Az.:12 O 562/17

1 Einführung

Online-Banking, also die Abwicklung von Bankgeschäften im Internet, erfreut sich großer Beliebtheit, da es den Bankkunden ermöglicht, unabhängig von Öffnungszeiten immer und überall ihre Bankgeschäfte mittels Computer oder Mobiltelefon vorzunehmen. Nach einer Hochrechnung von Bitkom Research lag die Zahl der Online-Banking-Nutzer in Deutschland im Jahr 2017 bei rund 42 Millionen.[1] Allerdings ist das Online-Banking keineswegs risikolos. Auf vielfältige Art und Weise versuchen Betrüger, an Kontodaten zu gelangen, um sodann von den betroffenen Konten Überweisungen vorzunehmen und diese leer zu räumen.

Mit einer solchen Konstellation des Online-Banking hatte sich nun auch das Landgericht Kiel auseinanderzusetzen. Diese Entscheidung vom 20.04.2018, Aktenzeichen: 12 O 562/17, verdient Beachtung, weil hier Rechtsfragen zum Online-Banking unter Einsatz der sogenannten SMS-Tan aufgearbeitet werden, die für Verbraucher von Bedeutung sind.

2 Sachverhalt

Der Kläger, ein Kunde der beklagten Förde-Sparkasse, unterhält bei dieser ein Konto.

Der Kläger begehrt die Erstattung zweier von ihm nicht autorisierter Überweisungen von seinem Konto bei der Beklagten. Im Jahr 2007 wurde zwischen den Parteien vereinbart, dass der Kläger per Online-Banking unter Verwendung eines Anmeldenamens, einer persönlichen Geheimzahl (PIN) und einer Transaktionsnummer (TAN) Anweisungen an die Beklagte erteilen kann. Im Jahr 2011 vereinbarten die Parteien die Verwendung des sms-TAN-Verfahrens. Die dazu online einzugebende Transaktionsnummer sendet die Beklagte dem Kläger auf dessen Mobiltelefon per SMS zu.

[1] Siehe https://de.statista.com/statistik/daten/studie/29516/umfrage/anzahl-der-nutzer-von-online-banking-in-deutschland/ , zuletzt aufgerufen am 29.07.2018.

Am Morgen des 30.08.2017 stellte der Kläger fest, dass sein Mobiltelefon nicht mehr funktionierte, was er seinem Mobilfunkanbieter umgehend meldete. Am 31.08.2017 um 11:36 und um 11:40 Uhr wurden unter Verwendung des sms-TAN-Verfahrens per Online-Banking zwei unautorisierte Überweisungen vom Konto des Klägers in Höhe von zusammen 28.170 € an unbekannte Empfänger vorgenommen. Der Kläger bemerkte dies noch am Vormittag desselben Tages und meldete die unautorisierten Überweisungen der Beklagten sogleich. Das Geld war jedoch nicht wieder zurückzuerlangen, weil sofort nach Eingang des Geldes bei den Empfängern darüber verfügt worden war. Der Kläger verlangte nun von der Beklagten die Rückbuchung der Kontobelastungen, was von dieser jedoch verweigert wurde.

Aus diesem Grunde erhob der Kläger entsprechende Klage vor dem Landgericht Kiel und beantragte, die Beklagte zu verurteilen, das bei der Beklagten geführte Zahlungskonto wieder auf den Stand zu bringen, auf dem sich das Zahlungskonto des Klägers ohne die Belastung der nicht autorisierten Zahlungsvorgänge in Höhe von 28.170 € befunden hätte.

3 Entscheidung des Landgerichtes Kiel

Das Landgericht hat der Klage (bis auf den ebenfalls geltend gemachten Zinsanspruch) stattgegeben. Es ist der Meinung, dass der Kläger von der Fördersparkasse gemäß § 675 u BGB a.F. (es sind die §§ 675c ff. BGB in ihrer bis zum 13.01.2018 geltenden Fassung anzuwenden, vgl. Art. 229 § 45 Abs. 2 EGBGB) verlangen kann, dass sein Zahlungskonto wieder auf den Stand vor den beiden nicht autorisierten Zahlungsvorgängen vom 31.07.2018 gebracht wird.

Diesem Anspruch kann die Förde-Sparkasse auch keinen Schadensersatzanspruch gemäß § 675v BGB a.F. entgegenhalten, da die nicht autorisierten Zahlungsvorgänge nicht auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Zahlungsauthentifizierungsinstruments beruhen (§ 675v Abs. 1 S. 1 BGB a.F.), weil der hinsichtlich des Mobiltelefons und der SIM-Karte nicht den Besitz verloren hat.

Es liegt nach Ansicht des Landgerichts auch kein Fall vor, in dem der Schaden infolge einer sonstigen missbräuchlichen Verwendung eines Zahlungsauthentifizierungsinstruments entstanden ist und der Zahler die personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat (§ 675v Abs. 1 S. 2 BGB a.F.). Personalisierte Sicherheitsmerkmale sind solche, die eine Authentifizierung erlauben, wie TAN und PIN im Online-Banking.[2] Sicher aufbewahrt sind die Merkmale, wenn der Zahler alle zumutbaren Vorkehrungen trifft, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen (vgl. § 675l S. 1 BGB a.F.).

Alleine der Umstand, dass die korrekte PIN zur Durchführung der Überweisung zum Einsatz gekommen sei, lässt nach Meinung des Landgerichts Kiel nicht darauf schließen, dass der Kläger die PIN nicht sicher aufbewahrt habe. Ein entsprechender Erfahrungssatz im Sinne eines typischen, regelhaften Geschehensablaufs ist nicht ersichtlich. Auch bei Anwendung der zumutbaren Sorgfalt ist ein unbefugter Zugriff auf personalisierte Sicherheitsmerkmale erfahrungsgemäß nicht auszuschließen. Es kommt immer wieder vor, dass Nutzereingaben wie die Eingabe eines

[2] Jungmann, in: Münchener Kommentar zum BGB, § 675j BGB, Rn. 40 f.

PIN-Codes mithilfe von Schadsoftware abgefangen werden. Dabei ist allgemein bekannt, dass die Infektion eines informationstechnischen Systems mit Schadsoftware häufig auch vom Anwender unbemerkt beim Besuch von Webseiten (sogenannte Drive-by-Downloads) erfolgt,[3] woraus dem Anwender kein Vorwurf zu machen ist. Auch durch Öffnen von E-Mails aus (scheinbar) vertrauenswürdiger Quelle kann eine unbemerkte Infektion mit Schadsoftware erfolgen, ohne dass dem Anwender daraus ein Vorwurf zu machen ist. Selbst aktuelle Virenschutzprogramme bieten stets nur gegen einen Teil der vorhandenen Schadprogramme Schutz.

Eine Umkehr der Beweislast, die hinsichtlich der Voraussetzungen des Schadensersatzanspruches bei der beklagten Förder-Sparkasse liegt, ergibt sich nicht daraus, dass die Aufbewahrung der Sicherheitsmerkmale ausschließlich in der Sphäre des Zahlers erfolgt und die Beklagte darauf keinen Einfluss hat. Aus dem Wortlaut des § 675v Abs. 1 S. 2 BGB ergibt sich eindeutig, dass die unsichere Aufbewahrung Voraussetzung eines Anspruchs des Zahlungsdienstleisters ist, wobei die Anspruchsvoraussetzungen nach allgemeinen Grundsätzen von demjenigen nachzuweisen sind, der den Anspruch geltend macht.

Der Beklagten kommen die Grundsätze der sekundären Darlegungslast zugute. Danach muss der Zahler dem Vorwurf der unsicheren Aufbewahrung substantiiert entgegentreten und zu den Sicherheitsvorkehrungen vortragen. Dies hat der Kläger hier in der mündlichen Verhandlung ausreichend getan. Dem Zahlungsdienstleister, hier der Förder-Sparkasse, ist es zumutbar, das verbleibende Restrisiko der Unaufklärbarkeit der Schadensursache zu tragen. Denn sein gewerbliches Geschäftsmodell des Angebots von Zahlungsdiensten über das Internet ist untrennbar mit einem gewissen Verlustrisiko verbunden, welches einzukalkulieren ist.

Der Kläger hat die nicht autorisierten Zahlungsvorgänge vorliegend zudem nicht durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Pflichten gemäß § 675l BGB herbeigeführt (§ 675v Abs. 2 Nr. 1 BGB a.F.) Dass der Kläger zumutbare Vorkehrungen zum Schutz von PIN und TAN unterlassen habe, hat die Beklagte nicht nachgewiesen. Hierfür ist sie jedoch beweispflichtig. Es kann im vorliegenden Fall offenbleiben, ob der Kläger auf seinem zum Online-Banking genutzten PC zum Schutz vor Schadsoftware ein Virenschutzprogramm installieren, verwenden und auf dem aktuellen Stand halten musste, weil der Kläger unwiderlegt vorträgt, dies getan zu haben. Soweit die Beklagte die Richtigkeit dieses Vortrags bestreitet, verkennt sie, dass ihr der Nachweis einer Pflichtverletzung obliegt und den Kläger insoweit lediglich eine sekundäre Darlegungslast trifft.

Es gibt auch keinen Erfahrungssatz, wonach bei einem Missbrauch des Online-Bankings bereits eine korrekte Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die beanstandungsfreie Prüfung der Authentifizierung für eine grob fahrlässige Pflichtverletzung des Zahlungsdienstnutzers sprechen, sodass sich der Zahlungsdienstleister für den ihm im Rahmen von § 675v Abs. 2 BGB a.F. obliegenden Nachweis auch nicht auf den Beweis des ersten Anscheins stützen kann.[4] Es ist nicht ungewöhnlich, dass es ohne Verschulden des Zahlenden zu unautorisierten Transaktionen kommt.

---

[3] vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2017; BKA, Bundeslagebild Cybercrime 2016.

[4] BGH, Urteil vom 26. Januar 2016, XI ZR 91/14, BGHZ 208, 331- 357, Rn. 68.

4 Kontext der Entscheidung

Das überzeugende Urteil des Landgerichts Kiels ist durchweg zu begrüßen. Die Besonderheiten des hier vorliegend zu beurteilten Online-Banking im Wege des sms-TAN Verfahrens und die damit einhergehenden Konsequenzen für die Beweisgrundsätze werden überzeugend vom Gericht herausgearbeitet. Hier zeigt sich, dass jede einzelne Konstellation des unbefugten Abhebens oder Überweisens vom Konto einer separaten Betrachtung unter Beachtung der jeweiligen Besonderheiten bedarf.

Während es beispielsweise in anderen Sachverhalten wie demjenigen, dass an Geldausgabeautomaten mit der zutreffenden Geheimzahl Geld abgehoben wird, nach der (durchaus kritikwürdigen) Rechtsprechung des BGH einen Beweis des ersten Anscheins dafür gibt, dass entweder der Karteninhaber die Abhebungen selbst vorgenommen hat oder ein Dritter nach der Entwendung der Karte von der Geheimnummer nur wegen ihrer gemeinsamen Verwahrung Kenntnis erlangen konnte, lassen die technischen Besonderheiten des vorliegenden Falles eine analoge Anwendung dieser Grundsätze nicht zu. Dies ist aber auch gerechtfertigt. Eine andere Entscheidung hätte dazu geführt, dass es für betroffene Verbraucher in entsprechenden Fällen nahezu unmöglich sein würde, den Schadensersatzanspruch der Kreditinstitute erfolgreich entgegenzutreten. Damit würde eine Umkehr der gesetzlichen Wertungen erreicht werden.

Eine Besonderheit in diesem Fall war, dass der mit der Angelegenheit befasste Richter besondere Sachkunde in Dingen des Internets und Datenschutzes besaß, war er doch bis 2017 Fraktionsvorsitzender der Piraten-Partei im Schleswig-Holsteiner Landtag.

5 Fazit

- Das Urteil des Landgerichts Kiel vom 20.04.2018, Az.:12 O 562/17 vermag zu überzeugen. Es zeigt deutlich auf, wie die Verteilung der Beweislast im Online-Banking im Wege des sms-TAN Verfahrens ist.
- Für Verbraucher, die in Bezug auf dieses Verfahren Opfer eines Betrugs geworden sind, bestehen gute Chancen, sich gegen Schadensersatzansprüche des Kreditinstitutes zu wehren, sofern sie die erwartbaren Sicherheitsvorkehrungen getroffen haben.
- Es sollte generell von Verwendern des Online-Bankings darauf geachtet werden, potentiellen Betrugsversuchen soweit wie möglich vorzubeugen. Es empfiehlt sich, auf seinem zum Online-Banking genutzten PC zum Schutz vor Schadsoftware ein Virenschutzprogramm zu installieren, zu verwenden und auf dem aktuellen Stand zu halten. Gerade auch beim Einsatz von Mobiltelefonen ist entsprechendes zu beachten.
- Es bleibt zu hoffen, dass das OLG Schleswig in der Berufungsinstanz (und ggf. auch der BGH in der Revisionsinstanz) zu keiner anderen rechtlichen Einschätzung kommt, sondern dass das überzeugende Urteil des Landgerichts Kiel bestehen bleibt und Rechtskraft erlangt.

institut für finanzdienstleistungen e.V. (*iff*) | Vorstand: Udo Philipp, Prof. Dr. Ingrid Größl | Direktor: Dr. Dirk Ulbricht

Grindelallee 100
20146 Hamburg
Fon +49(0)40 30 96 91 - 0
Fax +49(0)40 30 96 91 - 22

www.iff-hamburg.de
institut@iff-hamburg.de
USt-IdNr. DE 118713543
AG Hamburg VR 13836

Hamburger Sparkasse
IBAN DE62 2005 0550 1238 1229 21
BIC HASPDEHHXXX
Gläubiger ID: DE39ZZZ00000988279

Postbank Hamburg
IBAN DE23 2001 0020 0584 9552 00
BIC PBNKDEFF