Landgericht Köln, 21 O 116/19

Datum:	10.09.2019
Gericht:	Landgericht Köln
Spruchkörper:	21. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	21 O 116/19
ECLI:	ECLI:DE:LGK:2019:0910.21O116.19.00

Tenor:

Die Klage wird abgewiesen.

Der Kläger trägt die Kosten des Rechtsstreits.

Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 120 % des jeweils zu vollstreckenden Betrages.

Tatbestand: 1

Der Kläger führt bei der Beklagten unter der Kontonummer #####/#### ein Girokonto, von dem am 07.01.2019 ohne Berechtigung 9.850,00 €, am 08.01.2019 9.350,00 € und am 09.01.2019 2.600,00 € auf ein Konto einer türkischen Bank überwiesen wurden. Seit 2002 nutzt der Kläger das Online-Banking der Beklagten, zuletzt im sogenannten SMS-TAN-Verfahren. Bei diesem Verfahren eröffnet der Nutzer zunächst durch Eingabe eines nur ihm bekannten Benutzernamens und eines Kennwortes eine Online-Banking-Sitzung. Dort hinterlegt er eine Mobilfunknummer, auf welches die SMS mit den TANs für seine Zahlungs- uns sonstigen Aufträge gesendet wird. Ein Überweisungsauftrag wird von der Beklagten nur ausgeführt, wenn der Nutzer die korrekte TAN für diesen Auftrag in der Online-Banking-Maske ausgibt. 2

Den vorgenannten Überweisungen war Folgendes vorausgegangen: 3

Mitte 2018 meldete sich bei dem Kläger der vermeintliche Mitarbeiter der Beklagten L2 und gab vor, in der Abteilung Kundenbetreuung tätig zu sein. Herr L2, vermutlich ein Alias-Name, kannte die Kontonummer, die Adresse und das Geburtsdatum des Klägers. Er teilte mit, dass eine ihm bekannte ausländische Firma versucht habe, vom Konto des Klägers Geld abzubuchen, und er wolle entsprechende unberechtigte Abbuchungen in der Zukunft verhindern. In der Folge erhielt der Kläger – entsprechend den Angaben des Herrn L2 – ein 4

Schreiben einer ihm unbekannten Firma, mit welcher diese eine Zahlung forderte. Er vernichtete das Schreiben.

Am 27.11.2018 meldete sich der vermeintliche Mitarbeiter der Beklagten abermals beim Kläger und gab an, dass erneut eine Auslandsabbuchung versucht worden sei, das Konto allerdings gegen solche Auslandsabbuchungen gesichert werden könne. Mit Datum vom 20.11.2018 erhielt der Kläger ein Forderungsschreiben einer N AG. 5

Am 07.12. und 10.12.2018 rief Herr L2 abermals beim Kläger an, wobei er – wie auch zuvor – eine vermeintliche Telefonnummer der Beklagten nutzte. Er erklärte in den Telefonaten, dass er nun die angebliche Kontoabsicherung durchführen werde. Wie der Kläger in seiner persönlichen Anhörung vom 13.08.2019 erklärte, teilte ihm Herrn L2 in einem dieser Gespräche eine neue Kennnummer und eine neue PIN für die Eröffnung von Online-Banking-Sitzungen mit. Kurz darauf erhielt der Kläger – wie zuvor von Herrn L2 angekündigt – eine TAN, die er telefonisch an diesen durchgab. Nachfolgend betrieb der Kläger mit seinen neuen Kenndaten Online-Banking-Sitzungen. 6

In einem Telefonat vom 24.12.2018 gab Herr L2 an, dass er nun auch die EC-Karten des Klägers und seiner Ehefrau gegen Auslandsangriffe sichern wolle. In diesem Zusammenhang versendete er an den Kläger eine weitere TAN. In der SMS, mit welcher die Beklagte diese TAN an den Kläger sandte, hieß es: 7

„*ACHTUNG: Ihr Institut verlangt niemals eine neue Mobilfunknr. zu registrieren. Mobilfunknr. +49/176/91005239 LS-Rückgabe hat dann Zugriff auf Ihre Konten. Die TAN für die Registrierung vom 24.12.2018 10:49:25 ist 253038. Bei Zweifeln brechen Sie den Vorgang ab und wenden sich an ihren Berater.*“ 8

Wenige Minuten später wurde eine inhaltlich gleichlautende SMS mit einer weiteren TAN an den Kläger versandt, wobei der Kläger hierzu in seiner persönlichen Anhörung angab, dass er diese zweite TAN an den vermeintlichen Mitarbeiter der Beklagten weitergegeben habe. 9

In der Folge nutzte der Kläger noch mehrmals das Online-Banking zu Überweisungen, wobei er jeweils zwischen zwei Mobilfunknummern, seiner eigenen und einer von Herrn L2 hinterlegten, auswählen musste. Im Zeitraum vom 07. bis 09.01.2019 kam es dann zu den streitgegenständlichen Überweisungen. 10

Mit Schreiben vom 20.02.2019 forderten die Prozessbevollmächtigten des Klägers die Beklagte auf, die Abbuchungen vom 07. bis 09.01.2019 zu erstatten, was diese aber ablehnte. 11

Der Kläger ist der Auffassung, dass die Beklagte die Verantwortung für die unberechtigten Abbuchungen trage. Insbesondere stelle sich die Frage, warum sie keine Sicherheitssysteme habe, die typische Phishing-Situationen bei ihren Kunden verhindere. Die Beklagte fördere durch das Nichtvorhandensein von Sicherheitsmaßnahmen Online-Banking-Betrüge. Ferner sei nicht nachvollziehbar, warum die Beklagte nicht standardmäßig ihr Konto so eingestellt habe, dass beispielsweise eine Limitierung von Einzelüberweisungen erfolge. Der Kläger bestreitet, dass bei einer 2-Faktor-Authorisierung ein Missbrauch nur möglich sei, wenn der Täter die Zugangsdaten zum Onlinebanking kenne und Zugriff auf ein Mobiltelefon habe. Der Kläger ist der Auffassung, er habe jedenfalls nicht grob fahrlässig gehandelt. Er habe insbesondere keinen Anlass gehabt, an den glaubhaften Ausführungen des vermeintlichen Mitarbeiters der Beklagten zu zweifeln, zumal dieser einen persönlich glaubwürdigen Eindruck vermittelt. 12

Der Kläger beantragt, 13

1. 14

die Beklagte zu verurteilen, an ihn 21.800,00 € nebst Zinsen in Höhe von 9 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 10.01.2019 zu zahlen; 15

2. 16

hilfsweise die Beklagte zu verurteilen, dass bei ihr geführte Zahlungskonto mit der Kontonummer ######### wieder auf den Stand zu bringen, auf dem sich sein Zahlungskonto ohne die Belastung durch die nicht autorisierten Zahlungsvorgänge in Höhe von insgesamt 21.800,00 € nebst Zinsen in Höhe von 9 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 10.01.2019 befunden hätte. 17

Die Beklagte beantragt, 18

die Klage abzuweisen. 19

Sie ist der Auffassung, dass der Kläger grob fahrlässig gehandelt habe, indem er dem Herrn L2 den Zugriff auf das in Streit stehende Zahlungskonto eröffnet habe. Insoweit gehe es auch nicht um die Frage, ob die Beklagte Sicherheitsmaßnahmen gegen Phishing-Angriffe hätte treffen müssen, denn es handele sich schlichtweg um einen Online-Betrug, dem der Kläger zum Opfer gefallen sei. Sie erklärt die Aufrechnung gegen die klägerischen Ansprüche mit einem Schadenersatzanspruch nach § 674 v Abs. 3 Nr. 2 BGB. 20

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze sowie auf die zu den Akten gereichten Unterlagen Bezug genommen. 21

Entscheidungsgründe: 22

Die zulässige Klage ist unbegründet. 23

I. 24

Ein Zahlungsanspruch – wie mit dem Klageantrag zu 1. geltend gemacht – steht dem Kläger von vornherein nicht zu. Denn im Falle der unberechtigten Überweisung von einem Zahlungskonto ist der Anspruch des Zahlers auf Gutschrift des schon belasteten Betrages gerichtet, nicht aber auf Zahlung, § 675 u Satz 2 BGB (MüKoBGB/*Zetsche*, 7. Auflage 2017, § 675 u Rn 20 ff.). 25

II. 26

Aber auch ein Anspruch des Klägers aus § 675 u Satz 2 BGB besteht nicht, weil die Beklagte diesem Anspruch – der grundsätzlich aufgrund der nicht autorisierten Überweisungen vom 07. bis 09.01.2019 besteht – einen Schadenersatzanspruch nach § 675 v Abs. 3 Nr. 2 BGB entgegenhalten kann. Mit diesem hat sie die Aufrechnung gegen die Klageforderung erklärt. 27

Der Kläger hat gegen die vertraglichen Sorgfalts- und Mitwirkungspflichten des Nutzers bei der Verwendung des PIN-TAN-Verfahrens, die – unwidersprochen – bereits bei Vertragsschluss zwischen ihm und der Rechtsvorgängerin der Beklagten Vertragsbestandteil waren (Anlage B 4), grob fahrlässig verstoßen (§ 675 v Abs. § Nr. 2 lit. b). Ziffer 9 lit. a) der 28

AGB in der bei Vertragsschluss geltenden Bedingungen für die Nutzung des OnlineBanking-Angebotes der Stadtsparkasse mit PIN und TAN (bzw. Ziffer 7 der Bedingungen für das Online-Banking in der Fassung vom 13.01.2018) auferlegte dem Kläger die Pflicht, dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TANs erlangt.

Gegen diese Verpflichtung hat der Kläger verstoßen, indem er – was zumindest nach seinen Angaben im Rahmen seiner persönlichen Anhörung unstreitig ist – dem angeblichen Mitarbeiter der Beklagten L2 diejenige TAN weitergab, die es diesem ermöglichte, seine eigene Mobiltelefonnummer für die spätere Abfrage von computergenerierten TANs zu hinterlegen. 29

Diese vertragliche Sorgfaltspflicht verletzte der Kläger grob fahrlässig. Grob fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt in besonders schwerem Maße verletzt, einfachste und naheliegende Überlegungen nicht anstellt und in der konkreten Situation das nicht beachtet, was sich jedem aufdrängt (MüKoBGB/*Zetsche*, 7. Auflage 2017, § 675 v Rn 33), wobei sich aus Erwägungsgrund 33 der ZDRL ergibt, dass die Ausgestaltung des Begriffs nationalem Recht überlassen ist (MüKoBGB/*Zetsche*, a.a.O.). Nach diesen Grundsätzen stellt sich das Verhalten des Klägers in der Gesamtschau als grob fahrlässig dar, wobei – wie nachfolgend aufgezeigt wird – dahin stehen kann, ob bereits der Umstand, dass der Täter die Zugangsdaten zum Online-Banking (Kennwort und PIN) erlangt hat, auf grober Fahrlässigkeit beruhte. 30

Dem Kläger hätte bereits auffallen müssen, dass es für ein Kreditinstitut absolut außergewöhnlich ist, dass ein angeblicher Mitarbeiter telefonisch ankündigt, ihm eine TAN zu schicken, um das bisherige Kennwort und die bisherige PIN zu ändern. Bereits dies hätte einem durchschnittlich sorgfältigen Online-Banking-Kunden Anlass zu Misstrauen und ggf. einer Vorsprache bei der Bank gegeben. Noch auffälliger und mit den Usancen im Bankverkehr unvereinbar war es, dass der Mitarbeiter sodann die telefonische Durchgabe der TAN verlangte. Bereits dieser – erste – Verstoß gegen die vertraglich vereinbarte Pflicht, die TAN an Dritte weiterzugeben, erfolgte grob fahrlässig. Jedenfalls aber verstieß der Kläger in nicht nachzuvollziehender Weise gegen die ihm obliegenden Sorgfaltspflichten, indem er Herrn L2 am 24.12.2018 eine weitere TAN durchgab, nachdem dieser angegeben hatte, er wolle nunmehr die EC-Karten des Klägers und seiner Ehefrau gegen Angriffe aus dem Ausland sichern (wobei es schon keinen Sinn ergibt, warum hierfür Einstellungen im Online-Banking-Konto vorgenommen werden mussten). Mit dieser TAN war es dem Täter möglich, eine zweite Telefonnummer für die Übermittlung von TANs zu hinterlegen. Insoweit war es aber zum einen wiederum absolut ungewöhnlich, dass ein angeblicher Mitarbeiter des Kreditinstitutes die telefonische Durchgabe einer TAN verlangte, und zum anderen hat der Kläger selbst eingeräumt, die mit der Hinterlegung der Telefonnummer verbundene, unmissverständliche Warnnachricht der Beklagten schlichtweg nicht gelesen zu haben. Darüber hinaus hat er selbst angegeben, dass er in der Folge weitere Online-Banking-Überweisungen getätigt habe, bei denen er zwischen seiner und der neu hinterlegten Telefonnummer auswählen musste. Spätestens zu diesem Zeitpunkt war ihm sogar bekannt, dass ein weiterer, ihm unbekannter Nutzer von seinem Konto Überweisungen tätigen konnte, zumindest musste sich ihm diese Erkenntnis aufdrängen. Sämtliche, vorstehend aufgeführten und jeder für sich die grobe Fahrlässigkeit begründenden Umstände werden zudem davon umklammert, dass jeglicher (!) Kontakt telefonisch stattfand und es kein einziges Schriftstück der Beklagten betreffend den angeblichen Angriff auf das klägerische Konto gab. Dass es sich bei Herrn L2 um einen psychologisch gut geschulten Täter handelte und der Betrug zulasten des Klägers perfide ausgestaltet war, entlastet ihn angesichts der Vielzahl der vorstehend aufgezählten Umstände, aufgrund deren sich ein Betrugsverdacht aufdrängen 31

musste, und aufgrund der dazwischen liegenden Zeiträume, in denen der Kläger die jeweiligen Vorgänge hätte reflektieren können, nicht. Die Kammer ist nach der durchgeführten Anhörung auch davon überzeugt, dass der Kläger – der bis zum Renteneintritt als Kernphysiker tätig war – von zumindest überdurchschnittlicher Intelligenz ist und daher die Möglichkeit hatte, den Betrug zu seinen Lasten zu erkennen und zu verhindern.

Soweit der Kläger den Vorwurf erhebt, die Beklagte habe keine Sicherheitssysteme gegen „*solche Phishing-Angriffe*“, erhebt er nach dem Verständnis der Kammer den Einwand des Mitverschuldens betreffend den zur Aufrechnung gestellten Schadenersatzanspruch. Dieser Einwand geht allerdings schon deshalb ins Leere, weil der Kläger nicht Opfer eines Phishing-Angriffs wurde, sondern die schadenauslösende Handlung selbst vorgenommen hat, indem er dem Täter den Zugriff auf die Mobil-TANs ermöglichte (s.o.). Der weitere Vorwurf, die Beklagte habe das Online-Banking-Konto nicht standardmäßig so eingestellt, dass Einzelüberweisungen limitiert seien, geht bereits deshalb ins Leere, weil einerseits eine entsprechende Schadensminderungspflicht nicht erkennbar ist und andererseits der Kläger seit 2002 das Online-Banking nutzt, ohne auch nur die Einrichtung eines Limits angefragt zu haben; dass er nicht gewusst hat, dass ein solches Limit möglich ist, trägt er bereits nicht vor. Ebenso wenig bestand eine Verpflichtung der Beklagten, vor Einzelüberweisungen ins Ausland eine gesonderte Sicherheitsabfrage durchzuführen. 32

III. 33

Die prozessualen Nebenentscheidungen folgen den §§ 91, 709 Satz 1 und 2 ZPO. 34

IV. 35

Der Streitwert beträgt 21.800,00 €. Da Haupt- und Hilfsantrag des Klägers auf dasselbe wirtschaftliche Ziel gerichtet sind, findet eine Streitwertaddition nicht statt (§ 45 Abs. 1 Satz 3 GKG). 36
