Landgericht Landshut

Urteil vom 14.07.2011

Az.: 24 O 1129/11

1. Die Beklagte wird verurteilt, an den Kläger 6.000,- Euro zuzüglich Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.04.2011 sowie vorgerichtliche Anwaltskosten in Höhe von 546,69 Euro zu zahlen.

2. Die Beklagte trägt die Kosten des Rechtsstreits.

3. Das Urteil ist für die Klagepartei gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

4. Der Streitwert des Verfahrens wird auf 6.000,- Euro festgesetzt.

Tatbestand

Der Kläger begehrt von der Beklagten Erstattung aus einem zugrundeliegenden Kontokorrentvertrag als Geschädigter eines Phishing-Angriffs zulasten seines Girokontos.

Der Kläger unterhält bei der Filiale der Beklagten in P. ein privates Girokonto mit der Konto-Nr. ... Der Kläger nutzt das von der Beklagten angebotene Online-Banking, wobei er als Authentifizierungsinstrument das von der Beklagten bereitgestellte „iTAN-Verfahren“ verwendet. Hierzu hatte der Kläger unter dem 18.01.2008 einen Rahmenvertrag zur Nutzung des ... Direct-B@nking abgeschlossen, in den auch die Sonderbedingungen für das ...-Direct-B@nking eingeschlossen wurden. Bei dem von der Beklagten angebotenen Direct-B@nking können Transaktionen grundsätzlich nur unter Verwendung der allein dem autorisierten Nutzer bekanntgegebenen Legitimationsdaten vorgenommen werden. Im Rahmen des iTAN-Verfahrens wird zudem jeder TAN eine Index-Nummer zugeordnet und beklagtenseits bei jeder Transaktion eine konkrete TAN aus der nur dem Kunden vorliegenden TAN-Liste durch Nennung der zugehörigen Index-Nummer abgefragt. Die TAN-Nummern werden dem Kunden vorab auf einer sogenannten TAN-Liste von der Bank per Post zugesandt.

Am 20.02.2011 wurde der Kläger Opfer eines sogenannten Phishing-Angriffs. Bei Aufruf der Internetseite der Beklagten für Zwecke des Online-Bankings öffnete sich während des Authentifizierungsvorgangs eine gefälschte

Internetseite, die der Internetseite der Beklagten in Text, Funktion und Aussehen äußerlich ähnlich sah. Auf dieser Seite wurde dem Kläger mitgeteilt, dass im Zusammenhang mit der Einführung neuer Sicherheitsmaßnahmen aus Sicherheitsgründen alle laufenden TAN-Listen aus dem Verkehr gezogen werden müssten. Der Kläger sollte daher die ihm vorliegenden insgesamt 100 TAN-Nummern in dafür vorgesehene Eingabefelder eingeben.

Der Kläger ist osteuropäischer Herkunft und spricht deutsch nicht als Muttersprache. Er ist von Beruf angestellter Schlosser und besitzt in Sachen Internet nur geringe Kenntnisse. Der Kläger kam der Aufforderung in der Abfrage nach, da er der Meinung war, dass diese Aufforderung tatsächlich von der Beklagten stammte und eine Eingabe der TAN-Nummern aufgrund der Ausführungen auf der Internetseite für plausibel hielt.

Die gefälschte Internetseite wurde jedoch durch Schadsoftware (Trojaner) mit der Bezeichnung SpyEye erzeugt. Diese erzeugte, nachdem sie auf den Rechner des Klägers gelangt war, beim Einloggen in die Online-Banking-Sitzung die TAN-Abfrage, wobei keine Möglichkeit besteht, diese Abfrage zu überspringen oder zu umgehen. Daraufhin wird unbemerkt eine Verbindung zum Server des Täters aufgebaut und dorthin werden dann die eingetragenen TANs übertragen.

Nachdem der Kläger entsprechend der Abfrage sämtliche 100 TAN-Nummern in die entsprechenden Felder eingetragen hatte, wurden am 23.02.2011 von unbekannten Tätern insgesamt 6.000,- Euro in sechs Einzelabbuchungen zu je 1.000,- Euro zugunsten eines dem Kläger unbekannten Herrn K. aus W. vorgenommen, ohne dass der Kläger dies veranlasst hatte oder Kenntnis hiervon hatte. Der Kläger bemerkte diese Abbuchungen am 27.02.2011 und erstattete umgehend noch am gleichen Tag Anzeige gegen Unbekannt. Am 28.02.2011 informierte der Kläger die Beklagte über die Vorfälle und ersuchte um umgehende Rückbuchung des Fehlbetrags, da eine dementsprechende Überweisung von ihm nicht veranlasst oder gewollt gewesen sei.

Der Kläger ist der Ansicht, dass ihm Ersatzansprüche gegenüber der Beklagten zustünden, weil er selbst keinen wirksamen Überweisungsauftrag erteilt habe und weil ihm auch keine schuldhafte Sorgfaltspflichtverletzung zur Last gelegt werden könne, auf die die Beklagte ihrerseits einen Schadensersatzanspruch ihm gegenüber stützen könnte. Er habe keinen Anlass gehabt, die täuschend echt nachgeahmte Aufforderung zur Eingabe der TANs in Zweifel zu ziehen, weil dafür ein plausibler Grund genannt worden sei. Der Kläger habe seinen Computer durch ein aktuelles Antivirenprogramm und eine Firewall abgesichert. Die Aufmachung der Seite habe das Vertrauen des Klägers in die Echtheit des Hinweises erweckt. Es habe kein Grund bestanden, an der Echtheit der Aufforderung zu zweifeln, da sowohl das Erscheinungsbild als auch die Begründung in sich schlüssig waren. Auch der Zeitpunkt des Auftretens des Popups habe genau in den Geschehensablauf gepasst, weil

dieses nämlich erst bei Betätigung der Schaltfläche für den Log-In aufgetreten sei. Die Beklagte sei umgekehrt vielmehr verpflichtet, dafür zu sorgen, dass Dritte ihre Kunden nicht mit derartigen Seiten täuschen könnten. Die Warnhinweise auf der Hompage der Beklagten seien insoweit viel zu ungenau formuliert.

Der Kläger beantragt:

Die Beklagte wird verurteilt, an den Kläger 6.000,- Euro zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.04.2011 sowie vorgerichtliche Anwaltskosten in Höhe von 546,69 Euro zu zahlen.

Die Beklagte beantragt:

Klageabweisung.

Die Beklagte ist der Auffassung, dass der Kläger dem unbefugten Dritten den Zugriff auf sein Konto unter Verletzung der ihm obliegenden Sorgfalt grob fahrlässig durch Preisgabe seiner Legitimationsdaten ermöglicht habe, so dass der Beklagten ein aufrechenbarer Schadensersatzanspruch zustehe. Dem Kläger sei bekannt gewesen, dass für den Log-In lediglich die Direct-B@nking-Nummer und die PIN, nicht aber TAN-Nummern einzugeben sind. Auf der Log-in-Seite der Beklagten befinde sich in der rechten Rubrik auch folgender Hinweis: „Geben Sie nur dann eine TAN ein, wenn Sie selbst zuvor z. B. eine Überweisung erfasst haben!“ Die Abfrage der TAN-Nummern auf der Internetseite habe dem Kläger daher keinesfalls plausibel erscheinen können und widersprach gerade den Warnhinweisen der Beklagten. Auch das Erfordernis einer Eingabe von 100 TAN-Nummern hätte den Kläger stutzig machen müssen. Weiter sei dem Kläger zum Vorwurf zu machen, dass die Beklagte zur Durchführung des Online-Bankings bereits seit Mai 2009 auch ein sogenanntes „mobiles TAN-Verfahren“ zur Verfügung stellt, welches sicherer sei, als das iTAN-Verfahren.

Zur Ergänzung des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Eine Beweisaufnahme fand nicht statt.

Entscheidungsgründe

Die zulässige Klage ist begründet.

I.

Der Kläger hat gegen die Beklagte einen Rückzahlungsanspruch aus § 675 u Satz 2 BGB in Höhe von 6.000,-Euro.

1. Es liegt ein nicht autorisierter Zahlungsvorgang im Sinne des § 675 u Satz 1 BGB vor.

Es steht außer Streit, dass der Kläger die streitgegenständlichen Überweisungen nicht selbst veranlasst hat. Dem Kläger sind die Überweisungsaufträge auch nicht unter dem Gesichtspunkt einer Anscheinsvollmacht deshalb zurechenbar, weil er durch Eingabe von PIN und TAN das berechtigte Vertrauen der Beklagten darauf geweckt hätte, dass die Überweisungen von ihm legitimiert seien. Nach den von der Rechtsprechung entwickelten Grundsätzen der Anscheinsvollmacht ist ein Verhalten dann wegen eines schuldhaft verursachten Rechtsscheins zuzurechnen, wenn der Vertretene das Handeln des Scheinvertreters nicht kennt, es aber bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können und der andere Teil annehmen durfte, der Vertretene dulde und billige das Handeln des Vertreters (vgl. Palandt, 70. Aufl., § 172 BGB Rdnr. 11, BGH NJW 1981, 1728). Daran fehlt es jedoch vorliegend, weil der Kläger durch die Eingabe der TAN-Nummern den missbräuchlichen Zugriff auf sein Konto zwar ermöglicht hat, er die dann von dritter Seite veranlassten Überweisungen aber nicht etwa am Computerbildschirm verfolgen konnte. Er konnte das Handeln seines „Scheinvertreters“ daher nicht erkennen.

2. Der Beklagten steht auch kein gemäß § 389 BGB aufrechenbarer Schadensersatzanspruch gegen den Kläger nach § 675 v Abs. 2 BGB zu.

Der Kläger ist der Beklagten nicht zum Schadensersatz verpflichtet, weil der Kläger die nicht autorisierten Zahlungsvorgänge nicht durch vorsätzliche oder grob fahrlässige Verletzung seiner Pflichten herbeigeführt hat.

Der Kläger hat die TAN-Nummern nicht willentlich Dritten offenbart. Ihm kann auch nicht zur Last gelegt werden, die unbefugte Verwendung seiner Geheimdaten durch Dritte dadurch ermöglicht zu haben, dass er seinen Computer nicht durch ein entsprechendes Programm hinreichend vor Phishing-Angriffen geschützt habe. Die Beklagte, der die Darlegungs- und Beweislast für die ihren Schadensersatzanspruch begründenden Umstände obliegt, hat keine konkreten Anhaltspunktspunkte dafür genannt oder gar unter Beweis gestellt, dass der Computer des Klägers nicht durch ein aktuelles handelsübliches Virenschutzprogramm und eine Firewall ausreichend gesichert gewesen sei. Dafür bietet der bloße Umstand, dass der Computer des Klägers offenbar dem Angriff eines Trojaners unterlag, kein stichhaltiges Indiz. Es liegt in der Natur der Sache, dass ein Schutz vor Computerviren regelmäßig nur in Reaktion auf bekannte Viren entwickelt werden kann. Deshalb kann auch ein regelmäßig aktualisiertes Schutzprogramm keine vollständige Gewähr dafür bieten, dass der Computer nicht von einem neu entwickelten Trojaner infiziert wird.

Das Verhalten des Klägers ist auch nicht deshalb als grob fahrlässig zu werten, weil die Aufforderung, alle 100 TAN-Nummern einzugeben, im Online-Banking unüblich ist und dem Kläger Anlass hätte geben müssen, Verdacht zu schöpfen.

Eine nach § 675 v Abs. 2 erforderliche grobe Fahrlässigkeit erfordert eine Außerachtlassung der verkehrserforderlichen Sorgfalt im besonders schwerem, ungewöhnlich hohem Maße. Das ist der Fall, wenn schon einfachste, ganz naheliegende Überlegungen nicht angestellt werden und dasjenige unbeachtet blieb, was unter den gegebenen Umständen jedem einleuchten musste (Palandt, 70 Aufl., § 277 BGB Rdnr. 5, Jauernig, 13. Aufl., § 276 BGB Rdnr. 33, BGHZ 10, 16, BGHZ 77, 276). Grobe Fahrlässigkeit setzt zunächst in objektiver Hinsicht eine das gewöhnliche Maß der Fahrlässigkeit erheblich übersteigende Schwere eines Sorgfaltsverstoßes voraus. Den Handelnden muss aber auch in subjektiver Hinsicht ein schweres Verschulden treffen (Palandt, 70. Aufl. § 277 BGB Rdnr. 5, Jauernig, 13. Aufl., § 276 BGB Rdnr. 33, BGH NJW 1988, 1265, BGHZ 119, 149), es sind daher auch in der Person des Handelnden liegende subjektive Umstände mit zu berücksichtigen. So ist etwa zu berücksichtigen, ob der Handelnde insoweit ungeübt und Nichtfachmann ist, zudem ist auch das Bewusstsein der Gefährlichkeit erforderlich (Palandt, 70. Aufl., § 277 BGB Rdnr. 5, BGH NJW-RR 1989, 991).

Diesen - auch subjektiven - Maßstab zugrunde gelegt, ist das Verhalten des Klägers zwar durchaus als fahrlässig, nicht jedoch als grob fahrlässig im Sinne des § 675 v Abs. 2 BGB zu qualifizieren.

In diesem Zusammenhang ist zunächst zu berücksichtigen, dass es sich bei dem Kläger um einen gebürtigen Osteuropäer handelt, der deutsch nicht als Muttersprache spricht. Der Kläger ist als angestellter Schlosser tätig und besitzt nur äußerst rudimentäre Computerkenntnisse. An diesen in der Person des Klägers liegenden Umständen gemessen, ist der Vortrag des Klägers daher durchaus plausibel, dass er die Nachahmung der Internetseite, die nach ihrer optischen Gestaltung dem Internetauftritt der Beklagten sehr ähnlich sieht, für echt gehalten hat. Neben dem Erscheinungsbild passte auch der Zeitpunkt des Auftretens der gefälschten Seite genau in den Geschehensablauf. Diese trat nämlich erst unmittelbar nach dem Log-In auf und nicht zu einem beliebigen Zeitpunkt. Zudem wurde in der gefälschten Seite auch durchaus schlüssig begründet, warum ausnahmsweise eine Eingabe von TANs notwendig sei, nämlich weil im Zusammenhang mit der Einführung neuer Sicherheitsmaßnahmen aus Sicherheitsgründen alle laufenden TAN-Listen aus dem Verkehr gezogen werden müssten. Diese Begründung durfte dem Kläger durchaus als plausibel erscheinen. Die Beklagte gibt zwar insoweit zu bedenken, dass sich auf ihrer Internetseite ausdrücklich folgender Hinweis befindet: „Geben Sie nur dann eine TAN ein, wenn Sie selbst zuvor z. B. eine Überweisung erfasst haben!“ Hierzu ist jedoch zunächst festzuhalten, dass dieser Hinweis äußerst unpräzise formuliert ist, da sich dem Online-

Bankkunden nicht erschließt, welche Fälle außer der Tätigung einer Überweisung mit der Formulierung „z. B.“ noch erfasst sein sollen, in denen man ebenfalls eine TAN eingeben darf. Darüber hinaus ist auf der gefälschten Seite ausdrücklich ausgeführt, dass aufgrund der Ausnahmesituation, die durch die aufgetretenen Sicherheitsprobleme entstanden ist, eine Ausnahmemaßnahme durchgeführt werde, um alle laufenden TAN-Listen aus dem Verkehr zu ziehen. Hierdurch konnte beim Kunden also durchaus der Eindruck entstehen, dass die grundsätzlichen Hinweise der Beklagten aufgrund der Ausnahmekonstellation in diesem Fall gerade nicht gelten würden. Es kann daher bei dieser Konstellation nicht von grober Fahrlässigkeit ausgegangen werden, wenn der Kläger trotz des auf der Homepage der Beklagten befindlichen Hinweises aufgrund der Ausführungen in der gefälschten Seite TAN-Nummern eingab.

Eine grobe Fahrlässigkeit des Klägers ergibt sich auch nicht aus dem Umstand, dass der Kläger sämtliche 100 TAN-Nummern eingegeben hat. Hierzu ist er durch die gefälschte Seite ja gerade aufgefordert worden. Es ist also nur als konsequent zu bewerten, wenn der Kläger, der auf die Richtigkeit und Ordnungsgemäßheit der Aufforderung zur Eingabe sämtlicher TAN-Nummern ausging, hierauf auch sämtliche TAN-Nummern eingibt. Umgekehrt wäre es vielmehr als grob fahrlässig zu bewerten, wenn der Kläger beispielsweise 50 oder 60 TAN-Nummern eingegeben und dann mit der Eingabe weiterer Nummern aufgehört hätte, weil ihm die Sache verdächtig erschienen wäre. Wenn der Kläger aber, der Aufforderung in der gefälschten Seite konsequent folgend, sämtliche 100 TAN-Nummern eingibt, so lässt dies lediglich den einen Schluss zu, dass er auf die Ordnungsgemäßheit der Anforderung vertraut und gerade keinen Verdacht geschöpft hat. Aufgrund des Umstandes, dass der Kläger, nachdem er sämtliche Felder ausgefüllt hatte, wieder auf sein Konto zugreifen konnte, durfte der Kläger durchaus annehmen, dass dies alles so seine Richtigkeit habe.

Auch der Umstand, dass der Kläger zunächst noch mehrfache Versuche unternommen hat, ohne Eingabe der TAN-Nummern auf sein Konto zuzugreifen und die Internetseite mehrfach aufgerufen und wieder geschlossen hat, gab keine ausreichende Veranlassung für ein Misstrauen des Klägers. Vielmehr hat der Kläger offensichtlich gerade aufgrund des Umstandes, dass die fragliche TAN-Abfrage bei jedem Aufruf der Internetseite erneut in gleicher Weise aufgetreten ist, letztlich darauf vertraut, dass es insoweit seine Richtigkeit habe. Dies ist auch durchaus nachvollziehbar. Anders wäre es beispielsweise dann gewesen, wenn sich dem Kläger bei jedem Aufruf der Seite ein anderes Erscheinungsbild geboten hätte. Dies hätte dann eher Veranlassung für ein Misstrauen begründen müssen als wenn die Seite jedes Mal in genau gleicher Weise erscheint.

Dem Kläger kann auch nicht zum Vorwurf gemacht werden, dass er weiterhin das iTAN-Verfahren benutzt hat, obwohl die Beklagte bereits seit Mai 2009

auch das mobile TAN-Verfahren zur Verfügung stellt. Solange die Beklagte ihren Kunden auch das iTAN-Verfahren zur Verfügung stellt, kann sie das Verhalten ihrer Kunden nicht als grob fahrlässig qualifizieren, wenn diese von diesem Verfahren Gebrauch machen. Es obliegt vielmehr der Beklagten, hineichend dafür zu sorgen, dass ihre Kunden vor entsprechenden Manipulationsversuchen Dritter umfassend gewarnt werden.

Nach alledem ist das Verhalten des Klägers als nicht grob fahrlässig im Sinne des § 675 v Abs. 2 zu qualifizieren.

3. Der Zinsanspruch des Klägers ergibt sich aus §§ 286 Abs. 1, 288 Abs. 1 BGB. Die Beklagte wurde mit Fristsetzung zum 20.04.2011 zur Zahlung aufgefordert. Damit war sie gemäß § 286 Abs. 2 Nr. 1 BGB ab dem 21.04.2011 in Verzug.

Die Zinshöhe ergibt sich aus § 288 Abs. 1 Satz 2 BGB.

Die vorgerichtlichen Anwaltskosten des Klägers waren ebenfalls nach Verzugsgrundsätzen gemäß §§ 280, 286, 249 BGB zu erstatten.

II.

1. Die Kostenentscheidung beruht auf § 91 ZPO.

2. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 Satz 1, Satz 2 ZPO.

3. Der Streitwert des Verfahrens wurde gemäß § 3 ZPO festgesetzt.