AG München, Endurteil v. 21.01.2025 – 222 C 15098/24

Titel:

Grob fahrlässige Sorgfaltspflichtverletzung bei Eingabe von Kreditkartendetails auf Phishing-Seite

Normenkette:

BGB § 675u S. 2, § 675j Abs. 1 S. 1, § 675l Abs. 1

Leitsätze:

1. Die sogenannte Autorisierung als zustimmende Willenserklärung gem. § 675j BGB muss tatsächlich vom Kunden stammen oder diesem über die Regeln der Stellvertretung zuzurechnen sein. (Rn. 25) (redaktioneller Leitsatz)

2. Jeder auch nur durchschnittlich aufmerksame Marktteilnehmer weiß, dass Kreditkartendaten und persönliche Sicherheitsmerkmale wie SMS-TANs keinen Dritten, insbesondere keinen Kaufinteressenten auf Kleinanzeigen, mitgeteilt werden dürfen. Gibt ein Kunde auf einer Phishing-Seite "sicher bezahlen" seine Kreditkartendetails an, handelt er daher grob fahrlässig. (Rn. 27 – 33) (redaktioneller Leitsatz)

Schlagworte:

Phishing, sms-Tan

Fundstellen:

BeckRS 2025, 5067

MMR 2025, 661

LSK 2025, 5067

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

Beschluss

Der Streitwert wird auf 2.407,25 € festgesetzt.

Tatbestand

1
Mit vorliegender Klage begehrt der Kläger die Rücküberweisung zweier Transaktionen auf sein Konto bei der Beklagten.

2
Der Kläger hatte mit der Beklagten unter dem 06.11.2018 einen Allgemein-Verbraucherdarlehens- vertrag abgeschlossen, der von der Fa. … vermittelt wurde. Dieser sah neben der Erstverfügung in Höhe von EUR 1.333,96 die Einräumung eines flexibel vom Kläger in Anspruch zu nehmenden Kreditrahmens in Höhe von EUR 2.500 sowie die Überlassung einer Kreditkarte vor. Hinsichtlich der Einzelheiten wird verwiesen auf die Anlage B1.

3
Hinsichtlich des Online Banking kommt ein sogenanntes 3D-Secure Verfahren zum Einsatz.

4
Das 3D-Secure Verfahren ist ein Sicherheitsverfahren, das bei Online-Zahlungen zum Einsatz kommt, um die Authentifizierung von Kredit- oder Debitkarteninhabern zu verbessern. Der Begriff „3D“ steht dabei für

„Three Domain Secure“ und bezieht sich auf die drei beteiligten Parteien: den Karteninhaber, die ausstellende Bank und den Händler.

5
Beim 3D-Secure-Verfahren handelt sich um ein Freigabeverfahren mit 2-Faktor-Authentifizie- rung, bei dem der Kunde für die Freigabe von Kontoverfügungen eine mobileTAN per SMS oder eine Push-Benachrichtigung über die Banking-App auf sein mobiles Endgerät erhält.

6
Streitgegenständlich sind folgende zwei Transaktionen, von denen der Kläger behauptet, sie nicht autorisiert zu haben:

- Buchungsdatum 03.08.2023: 2.200,00 Euro an „… EUR 2200,00

- Buchungsdatum 07.08.2023: 207,25 Euro an „Ozon 2 USD 226,24 Kurs 1,0916284“ am 02.08.2023 um 21:16 Uhr

7
Der Kläger erhielt am 02.08.2023 um 15:08 Uhr eine SMS-TAN an die Mobilfunknummer des Klägers für die erste Aktivierung eines neuen Geräts und es wurde ein neues Gerät für das MasterCard 3D-Secure-Verfahren per Banking-App registriert.

8
Nach den Aufzeichnungen der Beklagten haben der Kläger und der Betrüger am 02.08.2023 sodann abwechselnd ihr jeweiliges Gerät als maßgebliches Freigabegerät in der Banking-App hinterlegt, wobei das klägerische Gerät ein Apple-Gerät ist und das des Betrügers ein Android Gerät. Hierzu war aufgrund der Erstregistrierung des Geräts des Betrügers keine SMS-TAN mehr erforderlich: Hinsichtlich der Einzelheiten wird verwiesen auf die Tabelle auf Seite 6 der Klageerwiderung.

9
Am Tag der streitgegenständlichen Verfügungen hatte der Kläger einen Gegenstand auf dem Portal Kleinanzeigen.de angeboten und wurde von einem vermeintlichen Kaufinteressenten kontaktiert. Unter Vortäuschung des Zahlungsmittels „Sicher bezahlen“ wurde der Kläger via Phishing zur Eingabe seiner Kreditkartendetails aufgefordert.

10
Der Kläger veranlasste telefonisch eine Kartensperrung und durch Schreiben vom 03.08.2023 ein Chargeback-Verfahren. Mit Schreiben vom 25.08.2023 lehnte die Beklagte eine Erstattung ab.

11
Am 02.08.2023 erstattete der Kläger außerdem Strafanzeige bei der Polizei.

12
Für den Fall, dass das Gericht von einer nicht ordnungsgemäß autorisierten Überweisung ausgeht, erklärt die Beklagte die (Hilfs-)Aufrechnung mit einem daraus resultierenden Schadensersatzanspruch in Höhe des von dem Kläger hinsichtlich der streitgegenständlichen Verfügung geltend gemachten Betrags.

13
Der Kläger behauptet, die streitgegenständlichen Transaktionen nicht autorisiert zu haben.

14
Dem Täter sei offensichtlich der Inhalt der SMS vom 02.08. 15:08 Uhr auf einen für den Kläger technisch nicht erklärenden Weg zugänglich gemacht worden. Der Kläger habe die mit der SMS übermittelten TAN weder in einer Banking-App noch sonstwo eingegeben. Vorliegend sei der Sicherheitsmechanismus der Banking-App durch den Täter umgangen worden bzw der Täter habe sich Zugang in das Online-Banking des Klägers verschaffen können aufgrund einer vorliegenden Sicherheitslücke bei der Bank.

15
Der Kläger beantragt:

1. Die Beklagte wird verurteilt, auf das Konto des Klägers mit der IBAN: … BIC: …, den Betrag in Höhe von EUR 2.407,25 nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz ab dem 13.11.2023 zu überweisen.

2. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von € 367,23 nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen.

16
Die Beklagte beantragt:

Die Klage wird abgewiesen.

17
Die Beklagte behauptet, dass der Kläger die von ihm erhaltene SMS-TAN auf der Phishing-Seite eingegeben habe, dies lasse sich widerspruchslos mit der Betrugsmasche in Einklang bringen. Das Verhalten des Klägers sei nicht nachvollziehbar, da zum Empfang einer Zahlung regelmäßig nicht erforderlich sei, die Kreditkartendaten anzugeben, sondern lediglich die Kontoverbindung.

18
Die Beklagte ist der Rechtsansicht, dass den streitgegenständlichen Überweisungen gemäß § 675j Abs. 1 Satz 1 BGB zugestimmt worden sei, sodass hier ein autorisierter Zahlungsvorgang vorliege. Selbst wenn man davon ausgehe, dass keine wirksame Autorisierung vorliege, so läge jedenfalls eine grob fahrlässige Sorgfaltspflichtverletzung vor, denn der Kläger habe einem Dritten zur Freischaltung der Banking App eine an seine Mobilfunknummer versandte SMS-TAN mitgeteilt, sodass dieser die SMS-TAN auf seinem Gerät zur Aktivierung eingeben konnte. Daraus resultiere ein Schadensersatzanspruch, mit dem gegen die Klageforderung aufgerechnet werden könne.

19
Eine Beweisaufnahme fand nicht statt. Mit Zustimmung der Parteien entscheidet das Gericht im schriftlichen Verfahren gemäß § 128 Abs. 2 ZPO.

20
Im Übrigen wird verwiesen auf die Schriftsätze der Parteien nebst Anlagen sowie das Protokoll der mündlichen Verhandlung vom 19.11.2024.

Entscheidungsgründe

21
Die zulässige Klage ist unbegründet.

I.

22
Der Kläger hat keinen Anspruch gegen die Beklagte auf Überweisung von 2.407,25 Euro auf sein Konto gem. § 675u Satz 2 BGB.

23
1. Der klägerische Anspruch ist nicht schon deshalb nicht gegeben, da die streitgegenständllichen Verfügungen durch den Kläger autorisiert wurden gern. § 675j Abs. 1 S. 1 BGB.

24
Aus der Übersicht in der Klageerwiderung ergibt sich, dass nicht durch das klägerische iOS-End- gerät, sondern durch ein Android Endgerät die Transaktionen freigegeben wurden.

25
Zwar lag bei einer technischen Betrachtung und aus der ex-ante Sicht der Beklagten eine solche Autorisierung vor. Diese war aber nicht wirksam, da sie dem Kläger nicht zugerechnet werden kann. Die sogenannte Autorisierung als zustimmende Willenserklärung gemäß § 675j BGB muss tatsächlich vom Kunden stammen oder diesem über die Regeln der Stellvertretung zuzurechnen sein. Eine Vollmacht des Klägers zugunsten der unbekannt gebliebenen Täter kann ausgeschlossen werden. Danach lag zwar eine technisch nicht zu beanstandende Autorisierung vor, die aber indessen nicht von dem Kläger stammte.

26
2. Der Anspruch des Klägers ist jedoch erloschen gern. § 389 BGB durch die Aufrechnung mit dem Anspruch auf Schadensersatz gem. § 675v Abs. 3 Nr. 2 BGB. Denn der Kläger hat in grob fahrlässiger Weise gegen die gesetzliche Vorgabe in § 675v Abs.3 Nr.2 a) BGB in Verbindung mit § 675l Abs. 1 BGB verstoßen

27
Es liegt zur Überzeugung des Gerichts eine grob fahrlässige Sorgfaltspflichtverletzung vor.

28
Der Kläger hat in grober Weise die im (Zahlungs-)Verkehr zu fordernde Sorgfalt nicht an den Tag gelegt, indem er seine Kreditkartendaten sowie seine persönlichen Sicherheitsmerkmale an Dritte herausgegeben hat. Jeder auch nur durchschnittlich aufmerksame Marktteilnehmer weiß, dass Kreditkartendaten und persönliche Sicherheitsmerkmale wie SMS-TANs keinen Dritten, insbesondere keinen Kaufinteressenten auf Kleinanzeigen, mitgeteilt werden dürfen. Die Geheimhaltungspflicht dieser Daten ergab sich auch aus den Vertragsbedingungen.

29
Das Gericht geht davon aus, das der Kläger auf der Phishing-Seite „sicher bezahlen“ die erhaltene SMS-TAN zur Freigabe eines neuen Endgeräts eingegeben hat. Mit Hilfe dieser TAN konnte der Täter dann ein neues Endgerät registrieren und die streitgegenständlichen Verfügungen ausführen.

30
Der Kläger war unstreitig auf der Phishing-Seite „sicher bezahlen“ und wurde dort aufgefordert zur Eingabe seiner Kreditkartendetails. Der Kläger hat auch unstreitig am 02.08.2023 um 15:08 Uhr per SMS eine TAN erhalten zur Registrierung eines neuen Endgeräts. Daher sieht das Gericht in dieser Konstellation eine sekundäre Darlegungslast auf der Klägerseite dazu, wie die TAN zeitnah an den Täter gelangt ist wenn nicht dadurch, dass der Kläger sie auf der Phishing-Seite angegeben hat. Dieser sekundären Darlegungslast ist der Kläger nicht nachgekommen. Es wurde lediglich vorgetragen, dass der Täter auf irgendeinem, für den Kläger technisch nicht zu erklärenden Weg an die TAN gelangt ist. Dies ist nicht ausreichend, um im Wege der sekundären Darlegungslast darzulegen, wie der Täter an die TAN gelangt sein kann.

31
Die Weitergabe der TAN durch den Kläger stellt eine grobe Sorgfaltspflichtverletzung dar.

32
Der Kläger ist als Verkäufer auf der Plattform aufgetreten. Warum man als Verkäufer und damit als Person, die Geld erhalten soll, eine (vorgetäuschte) Zwei-Faktor-Freigabe erteilt, erschließt sich dem Gericht nicht. Der Kläger mag ggfs nicht bewusst die per SMS erhaltene TAN auf der Phishing-Seite eingegeben haben und es mag ihm auch nicht erinnerlich sein. Indessen lässt sich der Vorgang plausibel nicht anders erklären. Die Weitergabe eines Verifizierungscodes an eine andere Person oder die Eingabe eines solches Codes auf einer Internetpräsenz, die nicht der Bank des Nutzers zugeordnet werden kann, verbietet sich von selbst.

33
Es darf von jedem verständigen Nutzer der Bezahlstruktur im Internet erwartet werden, dass er die grundlegende Bedeutung derartiger Freigabecodes versteht. Mit einem solchen Freigabecode kann, insbesondere nachdem man die Basisdaten seiner Kreditkarte bereits offenbart hatte, eine dritte Person jegliche Transaktion autorisieren, mithin auch ein neues Endgerät installieren. Damit wird die Sicherheitsarchitektur ausgehebelt. Das Gericht ist davon überzeugt, dass das konkrete Verhalten des Klägers als grob fahrlässig einzustufen ist. In diesem Zusammenhang sei auf die folgende Entscheidung verwiesen: OLG Frankfurt – Az.: 3 U 3/23 – Urteil vom 06.12.2023.

II.

34
Da die Klage in der Hauptsache abzuweisen war, besteht auch kein Anspruch hinsichtlich der geltend gemachten Nebenforderungen.

III.

35
Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO.

36
Die Entscheidung hinsichtlich der vorläufigen Vollstreckbarkeit ergibt sich aus §§ 708 Nr. 11, 711 ZPO.