Landgericht Köln
Pressestelle

Pressemitteilung

Aktenzeichen: EdM 01/2024

Datum 31.01.2024

Diana Renk
Pressesprecherin
Telefon (0221) 477-2749
Fax (0221) 477-1100
pressestelle@lg-koeln.nrw.de

Entscheidung des Monats

Betrug beim Online-Banking kommt leider häufiger vor. Bleibt der Kunde auf seinem Schaden sitzen, wenn Kriminelle sich unter Anzeige der Rufnummer der Bank telefonisch als Bankmitarbeiter ausgeben, sich so eine digitale Version der Debitkarte des Kunden erschleichen und anschließend mehr als 14.000 € mittels ApplePay abbuchen? Das Landgericht Köln entschied nun, dass das Bankinstitut dem Kunden in diesem Fall die betrügerischen Abbuchungen erstatten muss.

Der Kläger nimmt die beklagte Sparkasse auf Wiedergutschrift nicht autorisierter Zahlungsvorgänge in Anspruch. Er unterhält bei der Beklagten ein Privatgirokonto und nutzt hierfür seit mehreren Jahren auch das Online-Banking unter Verwendung des sog. pushTAN-Verfahrens als Authentifizierungsinstrument. Damit ermöglicht es die Beklagte ihren Kunden eine Überweisung oder eine sonstige Handlung − darunter beispielsweise auch die Freischaltung von ApplePay − webbasiert in der Banking App einzugeben. Veranlasst der Kunde einen Auftrag, benötigt er für dessen Freigabe zusätzlich eine TAN als elektronische Unterschrift. Hierzu bediente der Kläger sich des pushTAN-Verfahrens. Durch dieses Verfahren kann der Kläger von einem einzigen Gerät aus sowohl auf sein Online-Banking zugreifen als auch eine TAN anfordern. Wenn er einen Auftrag (z.B. Überweisung, PIN Änderung, Kartenfreischaltung pp.) initialisiert, erhält er für die elektronische Unterschrift eine TAN unter Angabe der konkreten Verwendung übersandt. Hierzu hat der Kläger auf seinem Mobiltelefon die pushTAN App installiert. Im September 2022 kontaktierte ein Unbekannter den Kläger telefonisch unter Anzeige der Rufnummer der Beklagten. Der Anrufer gab vor, ein Mitarbeiter der Beklagten zu sein, war dies jedoch tatsächlich nicht. Für den Anruf unter Anzeige der Nummer der Beklagten bediente er sich des sog. Call-ID Spoofings. Der Anrufer erfragte beim Kläger, ob dieser in der vergangenen Woche von betrügerischen Anrufen oder verdächtigen Kontobewegungen betroffen gewesen sei. Der Kläger verneinte dies. Der Anrufer teilte ihm daraufhin mit, dass er aufgrund aktueller Betrugsvorfälle vorsorglich das Konto und die Karte des Klägers gesperrt habe, dieses aber nun nach dessen Auskunft wieder entsperren könne. Er bat den Kläger sodann um entsprechende Freigabe über die pushTAN App der

Landgericht Köln
Luxemburger Str. 101
50939 Köln
Telefon (0221) 477-0
www.lg-koeln.nrw.de

Beklagten auf dem Mobiltelefon des Klägers. In der pushTAN App erschien daraufhin, ein Auftrag mit dem Text „*Registrierung Karte*“. Der Kläger gab den Auftrag frei. Mit dieser Freigabe bestätigte er tatsächlich aber einen durch die Täter initiierte Registrierung einer digitalen Version seiner Debitkarte zur Speicherung auf einem mobilen Endgerät. Diese installierten die Täter auf deren mobilen Endgerät und konnten infolgedessen in nur wenigen Tagen Zahlungen von über 14.000 € mit der digitalen Debitkarte unter Nutzung von ApplePay vornehmen. Nachdem die Beklagte vorgerichtlich zunächst einen Betrag von über 4.000 € erstattet hatte, lehnte sie trotz anwaltlicher Zahlungsaufforderung eine weitere Erstattung ab.

Der daraufhin beim Landgericht Köln erhobenen Klage, gab das Gericht vollumfänglich statt. Das Gericht führt aus, dass der Kläger gegen die Beklagte einen Anspruch habe, sein Konto auf den Stand zu bringen, auf dem es sich ohne die Belastungen durch die nicht autorisierten Zahlungsvorgänge befunden hätte (§ 675u S. 2 BGB). Die streitgegenständlichen Zahlungsvorgänge seien nicht durch den Kläger autorisiert gewesen. Dies sei bereits deshalb der Fall, weil sie nicht durch den Berechtigten, nämlich den Kläger, ausgeführt worden seien; eine Stellvertretung für den Kläger sei zudem ausgeschlossen. Dass der Kläger die Zahlungsvorgänge mittels ApplePay nicht selbst autorisiert habe, stehe nach dem Vortrag der Parteien fest.

Die Beklagte könne dem klägerischen Anspruch auch keinen Schadensersatzanspruch entgegenhalten. Zwar sei nach den gesetzlichen Regelungen ein Zahler seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Zahler entweder in betrügerischer Absicht gehandelt habe oder er den Schaden durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Pflichten nach Gesetz oder den vereinbarten Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments herbeigeführt habe. Entsprechendes habe die Beklagte dagegen nicht ausreichend dargelegt. Grobe Fahrlässigkeit erfordere einen in objektiver Hinsicht schweren und in subjektiver Hinsicht schlechthin unentschuldbaren Verstoß gegen die Anforderungen der konkret erforderlichen Sorgfalt. Daran fehle es hier. Das Verhalten des Klägers sei jedenfalls nicht als subjektiv schlechthin unentschuldbar zu werten. Dies stützt das Gericht dabei darauf, dass sich

die Täter des sog. Call-ID Spoofings bedient hätten. Dem Kläger sei infolgedessen die Nummer der Beklagten angezeigt worden, als die Täter ihn anriefen. Für einen verständigen, langjährigen Bankkunden sei die Nutzung einer ihm bekannten Nummer mit besonderem Vertrauen verbunden. Davon, dass die Möglichkeit bestehe, eine fremde Nummer zu nutzen, dürfte der Durchschnittsbürger keine Kenntnis haben. Auch, dass dem Kläger der angebliche Mitarbeiter der Beklagten nicht bekannt gewesen sei, sei für sich genommen noch kein besonders verdächtiger Umstand. In einer großen Organisation wie der der Beklagten herrsche regelmäßig eine gewisse Fluktuation bzw. es finde eine Arbeitsteilung statt. Etwas anderes gelte auch nicht aufgrund der Bezeichnung des Auftrags in der pushTAN App als „*Registrierung Karte*“. Zwar habe der Anrufer vorgegeben, er wolle die Karte des Klägers *entsperren*, nicht *registrieren*. Allerdings sei die Bezeichnung „*Registrierung*“ derart weit, dass für den Kläger – vor allem in der konkreten Überrumpelungssituation - überhaupt nicht erkennbar gewesen sei, dass es um die Einrichtung eines Zahlungssystems auf einem mobilen Endgerät und damit die Freigabe einer Möglichkeit zu Kontoverfügungen gehe. Dabei wäre es der Beklagten ohne weiteres möglich gewesen, durch einen eindeutigen Text, insbesondere durch Verwendung eines Hinweises gerade auf ApplePay dem Kunden deutlich vor Augen zu führen, welcher Zahlungsdienst hier freigegeben werden soll. Auch aus der Formulierung des Warntextes in der App, es sei „*kein Auftrag*“ freizugeben, der nicht „*explizit beauftragt*“ wurde, folge nach seinem natürlichen Wortsinn nicht, dass der Auftrag zwingend über die Online-Banking App erfolgt sein müsse. Der Kläger habe daher davon ausgehen dürfen, dass sein – vermeintlich − telefonisch erteilter „*Auftrag*“ diese Voraussetzungen ebenso erfülle.

Die am 08.01.2024 verkündete Entscheidung zum Az. 22 O 43/23 ist nicht rechtskräftig und in Kürze unter *www.nrwe.de* im Volltext abrufbar.

Renk

Diana Renk
Pressesprecherin