Dass gültige TAN und PIN beim Online-Banking eingesetzt wurden, lässt nicht den sicheren Schluss zu, dass es sich um die Autorisierung durch berechtigte Personen handelt

Gericht

BGH

Datum

26.01.2016

Aktenzeichen

XI ZR 91/14

Branche/ Lebenslage

Nachweis der Autorisierung eines Zahlungsauftrags beim Online-Banking, sekundäre Darlegungslast des Nutzers, Online-Banking, Autorisierung

Akteure

Online-Bankkonto-Nutzer, Bank

Wer haftet?

Bank, bzw. kein Haftungsanspruch gegen den Nutzer des Online-Bankkontos

Haftungsart

–

Haftungsumfang

Ausgleich des negativen Schlusssaldos

Haftungsbegründendes Verhalten

Unbefugte Zahlungsanweisungen im Online-Banking durch unbefugte Dritte

Technische Umstände

Online-Zahlungsverfahren sind oft von Anfang an manipulationsanfällig, sodass ein Authentisierungsvorgang nicht immer zu zweifelsfreien Ergebnissen führen kann

Persönliche Umstände

Die Verwendung korrekter Authentisierungsdaten lässt keine automatische Haftung des Online-Bankkonten-Nutzers zu

Möglichkeiten der Haftungsvermeidung

Nichtherausgabe der Online-Banking-Zugangsdaten; Bei Kenntnis unbefugter Nutzung sollte das unverzüglich der Bank mitgeteilt werden, da sonst eine Haftung nach Rechtsscheinsgrundsätzen zumindest nicht ausgeschlossen ist

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Die klagende Bank begehrte von der beklagten Bankkundin Ausgleich ihres Schlusssaldos. Die Beklagte hielt dem entgegen, der Fehlbetrag sei auf eine Überweisung im Online-Banking zurückzuführen, die diese nicht autorisiert hatte.

Das Gericht entschied, nicht allein, dass eine gültige TAN und PIN im Online-Banking-Verfahren verwendet wurde, lasse den Schluss zu, dass ein befugter Überweisungsauftrag vorliegt. Für einen Aufwendungsersatzanspruch (§ 675c Abs. 1, § 675 i.V.m. § 670 BGB) der Bank gegen die Bankkundin ist aber nachzuweisen, dass diese den Zahlungsauftrag tatsächlich autorisiert hat (Zustimmung des Zahlers).

> *Ist – wie hier – die Autorisierung eines Zahlungsvorgangs streitig, hat der Zahlungsdienstleister nach § 675w Satz 1 BGB zunächst die Authentifizierung sowie die ordnungsgemäße Aufzeichnung, Verbuchung und störungsfreie, keine Auffälligkeiten aufweisende technische Abwicklung des Zahlungsvorgangs nachzuweisen.*

Den Nachweis der störungsfreien Authentifizierung konnte die Bank noch erbringen. Allerdings entschied das Gericht auch, dass

> *die Authentifizierung und die Aufzeichnung der Nutzung des Zahlungsauthentifizierungsinstruments einschließlich der personalisierten Sicherheitsmerkmale aber nicht notwendigerweise ausreichen, den dem Zahlungsdienstleister – hier der Klägerin – obliegenden Nachweis einer Autorisierung des Zahlungsvorgangs zu führen.*

Grundsätzlich ist zwar auch eine Berufung auf den Beweis des ersten Anscheins denkbar. Dieser muss jedoch den besonderen Voraussetzungen des § 675w S. 3 BGB genügen. Daes setzt voraus, dass

> *ein Sicherheitssystem, das allgemein praktisch nicht zu überwinden war, im konkreten Einzelfall ordnungsgemäß angewendet worden ist und fehlerfrei funktioniert hat.*

Somit ist ein allgemein praktisch nicht zu überwindendes und im konkreten Einzelfall ordnungsgemäß angewendetes und fehlerfrei funktionierendes Sicherheitssystem Voraussetzung für die Anwendung der Grundsätze des Anscheinsbeweises.

> *Gegenwärtig werden […] Authentifizierungsverfahren im Online-Banking dann noch allgemein als praktisch unüberwindbar angesehen, wenn diese von einer Kompromittierung der eingesetzten Geräte nicht berührt werden, ein Zugriff Unberechtigter auf den konkreten Zahlungsvorgang ausgeschlossen ist, die TAN an den konkreten Zahlungsvorgang gebunden ist und das Verfahren dem Zahlungsdienstnutzer vor einer Freigabe die Überprüfung des vollständigen, unverfälschten Zahlungsauftrags ermöglicht.*

Es gibt jedoch keinen Erfahrungssatz, wonach bei einem Missbrauch des Online-Bankings bereits die korrekte Aufzeichnung der Nutzung eines Zahlungsauthentifizierungsinstruments und die beanstandungsfreie Prüfung der Authentifizierung für eine grob fahrlässige Pflichtverletzung des Zahlungsdienstnutzers sprechen.

Dann kann sich der Zahlungsdienstleister für den ihm im Rahmen von § 675v Abs. 2 BGB (heute § 675v Abs. 3 BGB) obliegenden Nachweis auch nicht auf den Beweis des ersten Anscheins stützen.

ANMERKUNGEN

Der BGH hat hier ausführlich zu Grundsatzfragen des Anscheinsbeweises im Online-Zahlungsverkehr Stellung genommen.

Kann eine Bank nachweisen, dass das von ihr verwendete Zahlungssystem gegen jede Form der Manipulation gesichert ist, trifft den Nutzer eine sekundäre Darlegungslast bezüglich eigener Sicherheitsvorkehrungen auf dem genutzten Rechner und Mobiltelefon, sowie bezüglich der Notierung, Speicherung und Weitergabe der PIN. Nicht geklärt wurde allerdings, in welchem Umfang eigene Sicherungspflichten des Nutzers zu erfolgen haben (siehe auch Metz, VuR 2016, 264).

Welches konkrete Zahlungsverfahren einen ausreichenden Sicherheitsstandard bietet, beurteilt der BGH nach aktuellem technischen Kenntnisstand.

Der BGH bezweifelt in der vorliegenden Entscheidung generell, ob eine Anscheinshaftung neben den speziellen Regelungen der § 675j Abs. 1 S. 4, §§ 675u, 675v BGB bestehen kann, legt sich hierzu jedoch nicht ausdrücklich fest. Somit verbleibt ein Stück Rechtsunsicherheit.

Praxishinweis: Grundsätzlich wurde mit dieser Entscheidung die Möglichkeit der Bank nachzuweisen, dass eine Zustimmung des Zahlenden, also des Konto-Inhabers vorliegt, deutlich reduziert. Das schafft für Bankkunden ein hohes Schutzniveau bei Angriffen Dritter auf die Online-Zahlsysteme der Bank. Wenn die Bank aber tatsächlich das hohe Schutzniveau ihres Zahlungssystems nachweisen kann, hat der Bankkunde nachzuweisen, die Überweisung nicht autorisiert zu haben.