

Hengeler Müller & Kollegen

Rechtsanwälte · Fachanwälte für Bank- und Kapitalmarktrecht

Behrenstraße 42, 10117 Berlin · Tel.: +49 30 20 96 17 0 · Fax: +49 30 20 96 17 99 · berlin@hengeler-mueller.de

Hengeler Müller & Kollegen · Behrenstraße 42, 10117 Berlin

Landgericht Berlin

4. Zivilkammer

Tegeler Weg 17–21, 10589 Berlin

Ihr Zeichen: 4 O 218/25

Unser Zeichen: HMC-2025/BK-1147

Datum: 10. November 2025

KLAGEERWIDERUNG

In der Sache

Peter Mayer, Lietzenburger Straße 74, 10719 Berlin

— Kläger —

Prozessbevollmächtigter: RA Dr. Marcus Brezelmann, Kanzlei Brezelmann & Partner, Kurfürstendamm 195, 10707 Berlin

gegen

Sparkasse Berlin, Alexanderplatz 2, 10178 Berlin

— Beklagte —

Prozessbevollmächtigte: RA Prof. Dr. Katharina von Westhoff und RA Dr. Jan-Henrik Böttcher, Hengeler Müller & Kollegen, Behrenstraße 42, 10117 Berlin

Az.: 4 O 218/25

zeigen wir an, dass uns die Beklagte, Sparkasse Berlin, mit der Wahrnehmung ihrer rechtlichen Interessen in vorbezeichneter Sache beauftragt hat. Ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Namens und in Vollmacht der Beklagten beantragen wir:

1. Die Klage wird abgewiesen.
2. Der Kläger trägt die Kosten des Rechtsstreits.
3. Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages.

Begründung:

Die Klage ist unbegründet. Dem Kläger steht ein Erstattungsanspruch aus § 675u Abs. 2 BGB nicht zu, da er den Schaden durch grob fahrlässige Verletzung seiner Sorgfaltspflichten gemäß § 675v Abs. 3 Nr. 2 BGB selbst herbeigeführt hat. Die Beklagte hat ihre vertraglichen und gesetzlichen Pflichten vollumfänglich erfüllt.

I. Zum Sachverhalt

Die Darstellung des Sachverhalts durch den Kläger ist in wesentlichen Punkten unvollständig und bedürftig der Ergänzung und Richtigstellung.

1. Zum Vertragsverhältnis

Zutreffend ist, dass der Kläger seit dem 12. September 2003 ein Girokonto bei der Beklagten unterhielt. Der Kläger hat am 5. März 2024 bei der Neuregistrierung seines Endgeräts die **Sonderbedingungen für das pushTAN-Verfahren** akzeptiert. In Ziffer 3.2 dieser Sonderbedingungen heißt es unmissverständlich:

„Der Kunde darf die TAN keinem Dritten mitteilen oder sonst zugänglich machen. Die TAN darf nur in der Sparkassen-App oder im Online-Banking direkt eingegeben werden. Eine Weitergabe per Telefon, E-Mail, SMS oder auf sonstigem Wege ist unzulässig.“

Ferner regelt Ziffer 11.2 der Allgemeinen Geschäftsbedingungen:

„Die Sparkasse wird den Kunden niemals telefonisch, per E-Mail oder per SMS auffordern, TAN, PIN oder Passwörter mitzuteilen.“

Beweis: Sonderbedingungen pushTAN-Verfahren (Anlage B2), Allgemeine Geschäftsbedingungen der Beklagten

2. Zu den Sicherheitshinweisen

Der Kläger wurde im Zeitraum von April 2024 bis Januar 2025 **viermal** schriftlich über aktuelle Betrugsmaschen informiert – und zwar am 15. Januar 2025, am 15. Oktober 2024, am 15. Juli 2024, am 15. April 2024. Jedes dieser Schreiben enthielt den fettgedruckten Hinweis:

„Die Sparkasse wird Sie niemals telefonisch, per E-Mail oder SMS zur Eingabe von TANs, PINs oder Passwörtern auffordern.“

Darüber hinaus wurden die Sicherheitshinweise im Online-Banking-Portal der Beklagten dauerhaft angezeigt und sind beim Login des Klägers am 26. Mai 2025 – zwei Tage vor dem Vorfall – als Pop-up-Fenster eingeblendet worden.

Beweis: Sicherheitshinweise Q1-Q4 (Anlage B3), Systemprotokoll Login-Banner

3. Zum Vorfall am 28. Mai 2025

Der Kläger verschweigt in seiner Darstellung, dass der **vollständige** Anzeigetext in der pushTAN-App lautete:

*„Freigabe für Sicherheitssperre **und Transaktionsfreigabe – Mehrere Vorgänge**“*

Der Zusatz „und Transaktionsfreigabe – Mehrere Vorgänge“ war auf dem Bildschirm des iPhone 13 des Klägers vollständig sichtbar und hätte bei pflichtgemäßer Sorgfalt Anlass zu erhöhter Vorsicht geben müssen. Der Kläger hat diesen Text entweder nicht gelesen oder bewusst ignoriert – beides begründet grobe Fahrlässigkeit.

Entscheidend ist ferner: Der Kläger hat die TAN **telefonisch** an einen Dritten weitergegeben. Die TAN wurde auf seinem registrierten Endgerät generiert und dann **freiwillig** – wenngleich infolge einer Täuschung – einem Unbekannten mitgeteilt. Die technische Autorisierung der Zahlungsvorgänge erfolgte ordnungsgemäß unter Verwendung einer gültigen TAN.

4. Zur verzögerten Sperrung

Der Kläger kontaktierte den Sperr-Notruf erst um 11:45 Uhr – mithin **28 Minuten** nach der TAN-Eingabe um 11:17 Uhr. In diesem Zeitfenster waren sämtliche betrügerische Transaktionen längst abgeschlossen (letzte Transaktion: 11:18:28 Uhr). Zwar begründet diese Verzögerung für sich genommen keine grobe Fahrlässigkeit, sie zeigt jedoch, dass der Kläger trotz der sofortigen Push-Benachrichtigungen nicht mit der gebotenen Dringlichkeit reagierte.

II. Rechtliche Würdigung

1. Zur Autorisierung (§ 675j BGB)

Der Kläger behauptet, die Zahlungsvorgänge seien nicht autorisiert gewesen. Dies bedarf der Differenzierung.

Die Zahlungsvorgänge wurden unter Verwendung einer gültigen, auf dem registrierten Endgerät des Klägers generierten pushTAN autorisiert. Die starke Kundenauthentifizierung gemäß Art. 97 der Richtlinie (EU) 2015/2366 (PSD2) i.V.m. § 55 ZAG wurde ordnungsgemäß durchgeführt: Besitzelement (registriertes iPhone 13), Wissenselement (PIN/Biometrie zur App-Freigabe) und dynamische Verknüpfung (TAN mit Transaktionsdaten) waren gegeben.

Soweit der Kläger vorträgt, sein Wille sei auf eine „Sicherheitssperre“ gerichtet gewesen, begründet dieser subjektive Irrtum keinen Mangel der Autorisierung. Der BGH hat in ständiger Rechtsprechung klargestellt, dass für die Autorisierung allein die äußere Zustimmungshandlung – hier: die Generierung und Weitergabe der TAN – maßgeblich ist, nicht das innere Motiv des Zahlers (BGH, Urt. v. 26.01.2016 – XI ZR 91/14, Rn. 54 f.).

Selbst wenn man – wie die Klägerseite – von nicht autorisierten Zahlungsvorgängen ausgehen wollte, scheitert der Erstattungsanspruch jedenfalls an § 675v Abs. 3 Nr. 2 BGB.

2. Grobe Fahrlässigkeit des Klägers (§ 675v Abs. 3 Nr. 2 BGB)

Der Kläger hat den Schaden durch grob fahrlässige Verletzung seiner Pflichten aus § 675i Abs. 1 BGB i.V.m. den Sonderbedingungen für das pushTAN-Verfahren herbeigeführt. Er haftet daher gemäß § 675v Abs. 3 Nr. 2 BGB für den entstandenen Schaden in voller Höhe.

a) TAN-Weitergabe als Kardinalpflichtverletzung

Die telefonische Weitergabe einer TAN an einen Dritten stellt die denkbar schwerste Verletzung der dem Zahlungsdienstnutzer obliegenden Sorgfaltspflichten dar. Die TAN ist – bildlich gesprochen – der „Schlüssel zum Konto“. Ihre Preisgabe ist vergleichbar mit der Übergabe des EC-Karten-PIN an einen Unbekannten auf der Straße.

Der **Bundesgerichtshof** hat in zwei grundlegenden Entscheidungen judiziert, dass die Preisgabe von Authentifizierungselementen **regelmäßig** als grob fahrlässig zu qualifizieren ist:

- **BGH, Urt. v. 26.01.2016 – XI ZR 91/14**, Rn. 72 ff.: „Die Weitergabe von Authentifizierungselementen an Dritte – gleich aus welchem Anlass – stellt eine schwerwiegende Verletzung der dem Zahlungsdienstnutzer obliegenden Sorgfaltspflichten dar, die auch unter Berücksichtigung der konkreten Umstände des Einzelfalls regelmäßig den Vorwurf grober Fahrlässigkeit begründet.“
- **BGH, Urt. v. 29.11.2016 – XI ZR 429/15**: Bestätigung und Fortführung der Rechtsprechung; auch bei elaborierter Täuschung bleibt die grobe Fahrlässigkeit bestehen, wenn gegen eindeutige vertragliche Pflichten verstoßen wird.

Diese höchstrichterliche Rechtsprechung ist bindend. Die vom Kläger angeführten Entscheidungen untergeordneter Instanzgerichte (LG Köln, AG München) vermögen hieran nichts zu ändern und sind zudem auf den vorliegenden Fall nicht übertragbar (dazu unten lit. e).

b) Vertragliche Pflichten klar und unmissverständlich kommuniziert

Die vertraglichen Sorgfaltspflichten des Klägers waren ihm aus drei Quellen bekannt:

Erstens: Ziffer 3.2 der Sonderbedingungen pushTAN, die der Kläger am 5. März 2024 akzeptiert hat, verbietet die Weitergabe der TAN an Dritte ausdrücklich und ausnahmslos.

Zweitens: Ziffer 11.2 der Allgemeinen Geschäftsbedingungen stellt klar, dass die Beklagte niemals telefonisch nach TANs fragt.

Drittens: Der Kläger erhielt in den zwölf Monaten vor dem Vorfall **vier quartalsweise Sicherheitshinweise** (zuletzt am 15. Januar 2025), die jeweils den prägnanten Warnhinweis enthielten, dass die Sparkasse niemals telefonisch TANs anfordert. Der letzte Hinweis lag gerade einmal vier Monate und 13 Tage vor dem Vorfall.

Beweis: Sonderbedingungen (Anlage B2), Sicherheitshinweise Q1–Q4 mit Zustellnachweisen (Anlage B3)

c) Berufliche Stellung begründet erhöhte Sorgfaltspflicht

Der Kläger ist von Beruf Rechtsanwaltsfachangestellter und seit 25 Jahren in einer Anwaltskanzlei tätig. Er ist beruflich mit der Bearbeitung rechtlicher Vorgänge befasst und verfügt über ein überdurchschnittliches Verständnis für vertragliche Pflichten und rechtliche Zusammenhänge.

Das **OLG Frankfurt** (Urt. v. 27.02.2020 – 17 U 42/19) hat ausgeführt, dass bei der Beurteilung der groben Fahrlässigkeit auch die persönlichen Verhältnisse des Geschädigten zu berücksichtigen sind. Ein im Rechtsbereich Tätiger muss die Bedeutung vertraglicher Geheimhaltungspflichten in besonderem Maße kennen. Der Kläger kann sich nicht auf die Unkenntnis eines „durchschnittlichen Verbrauchers“ berufen, da er aufgrund seiner beruflichen Tätigkeit gerade kein „durchschnittlicher“ Verbraucher ist.

d) App-Anzeige war eindeutig

Der Kläger behauptet, die App-Anzeige sei irreführend gewesen. Dies trifft nicht zu. Der vollständige Anzeigetext lautete „Freigabe für Sicherheitssperre **und Transaktionsfreigabe – Mehrere Vorgänge**“. Dieser Text war auf dem 6,1-Zoll-Display des iPhone 13 des Klägers vollständig und ohne Scrollen sichtbar.

Der Zusatz „Transaktionsfreigabe“ ist eindeutig. Er signalisiert, dass eine **Zahlungsfreigabe** erteilt wird – nicht lediglich eine Kontosperrung. Der Zusatz „Mehrere Vorgänge“ macht zudem deutlich, dass nicht ein einzelner Verwaltungsakt, sondern mehrere finanzielle Transaktionen freigegeben werden.

Gemäß § 675I Abs. 1 S. 1 BGB ist der Zahlungsdienstnutzer verpflichtet, unmittelbar nach Erhalt eines Zahlungsauthentifizierungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Hierzu gehört die **sorgfältige Lektüre des Anzeigetextes** vor Bestätigung. Wer eine TAN generiert und weitergibt, ohne den vollständigen Anzeigetext zu lesen, handelt grob fahrlässig.

Beweis: Technisches Protokoll mit Screenshot-Rekonstruktion der App-Anzeige (Anlage B1), Sachverständigengutachten zur Darstellung auf iPhone 13

e) Call-ID-Spoofing ändert an der Bewertung nichts

Der Kläger stützt sich maßgeblich auf das Argument, die Anzeige der Sparkassen-Rufnummer habe ein berechtigtes Vertrauen begründet. Dem ist zu widersprechen:

- Das **OLG Frankfurt** (Urt. v. 27.02.2020 – **17 U 42/19**) hat klargestellt, dass die Anzeige einer bekannten Rufnummer **keinen schützenswerten Vertrauenstatbestand** begründet, wenn elementare Sicherheitsregeln missachtet werden. Die telefonische TAN-Weitergabe stellt eine solche elementare Regelverletzung dar.
- Das **OLG München** (Urt. v. 14.01.2021 – **17 U 3651/20**) hat judiziert, dass selbst bei sophisticated Social-Engineering-Attacken die grobe Fahrlässigkeit nicht entfällt, wenn – wie hier – gegen eindeutige, mehrfach kommunizierte Sicherheitsanweisungen verstoßen wird.
- Die Möglichkeit der Rufnummernmanipulation ist spätestens seit dem Inkrafttreten des **§ 66k TKG** (Gesetz gegen unerlaubte Telefonwerbung und zur Verbesserung des Verbraucherschutzes) allgemein bekannt. Über Call-ID-Spoofing wurde zudem in zahlreichen Medien berichtet (u.a. Tagesschau, Verbraucherzentrale, Polizeiliche Kriminalprävention).

Die vom Kläger angeführte Entscheidung des **LG Köln** (15 O 267/23) betrifft einen anders gelagerten Fall, in dem der Kunde die TAN nicht telefonisch weitergab, sondern auf einer gefälschten Webseite eingab. Zudem handelt es sich um eine erstinstanzliche, nicht rechtskräftige Entscheidung, die in der Literatur kritisiert wurde (vgl. Werner, WM 2024, 521 ff.). Sie vermag die gefestigte BGH-Rechtsprechung nicht in Frage zu stellen.

Gleiches gilt für die Entscheidung des AG München (132 C 49/23), die mangels Veröffentlichung in einer Fachzeitschrift nicht verallgemeinerungsfähig ist.

3. Keine Pflichtverletzung der Beklagten

a) Transaktionsüberwachung ordnungsgemäß

Das Transaktions-Monitoring-System (TMS) der Beklagten entspricht den aufsichtsrechtlichen Anforderungen gemäß § 55 Abs. 1 ZAG i.V.m. Art. 2 Nr. 1 der Delegierten Verordnung (EU) 2018/389. Die Beklagte verfügt über ein risikobasiertes Echtzeit-Monitoring, das von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Rahmen der letzten IT-Prüfung im Oktober 2024 als „ordnungsgemäß und den Anforderungen entsprechend“ bewertet wurde.

Das TMS hat die streitgegenständlichen Transaktionen tatsächlich als auffällig eingestuft (Score: 72 von 100). Gemäß der internen Risikomatrix löst ein Score ab 75 eine automatische Transaktionssperre aus, ein Score zwischen 65 und 74 generiert eine manuelle Überprüfungsanforderung. Diese wurde um 11:19 Uhr – weniger als zwei Minuten nach den Transaktionen – generiert. Zu diesem Zeitpunkt waren die Transaktionen jedoch bereits abgeschlossen.

Entscheidend ist: Die Transaktionen wurden technisch korrekt mit einer gültigen TAN autorisiert. Eine ordnungsgemäß autorisierte Transaktion löst systembedingt niedrigere Risikoscores aus als eine nicht autorisierte, da die starke Kundenauthentifizierung gerade dem Zweck dient, die Berechtigung des Auftraggebers sicherzustellen.

Beweis: Systemprotokoll Transaktionsüberwachung (Anlage B4), BaFin-Prüfbericht IT-Sicherheit Oktober 2024, Auszug (Anlage B5), Sachverständigengutachten zum TMS der Beklagten

b) App-Gestaltung entspricht den gesetzlichen Vorgaben

Die pushTAN-App der Beklagten erfüllt die Anforderungen des Art. 97 Abs. 2 PSD2 i.V.m. Art. 5 der Delegierten Verordnung (EU) 2018/389. Der Anzeigetext enthielt alle gesetzlich vorgeschriebenen Informationen: den Empfänger (in aggregierter Form bei Sammelaufträgen), den Betrag (als Sammelposition) und die Art des Vorgangs („Transaktionsfreigabe“).

Art. 5 Abs. 2 der Delegierten Verordnung (EU) 2018/389 gestattet bei Sammelaufträgen ausdrücklich eine aggregierte Darstellung. Die Formulierung „Mehrere Vorgänge“ ist daher rechtlich nicht zu beanstanden. Die von der Klägerseite geforderte Einzelanzeige jeder Transaktion ist bei

Batch-Autorisierungen technisch nicht vorgesehen und gesetzlich nicht gefordert.

c) Keine Kausalität zwischen angeblicher Pflichtverletzung und Schaden

Selbst wenn man – hypothetisch – eine Pflichtverletzung der Beklagten bei der App-Gestaltung unterstellen wollte, fehlte es an der erforderlichen Kausalität. Der Kläger hat die TAN nicht deshalb weitergegeben, weil die App-Anzeige irreführend war, sondern weil er dem Anrufer vertraute. Er hat nach eigener Darstellung die TAN generiert, weil der Anrufer ihn dazu aufforderte – **bevor** er überhaupt den Anzeigetext las. Die App-Gestaltung war daher für die Schadensentstehung nicht kausal.

4. Kein Mitverschulden der Beklagten (§ 254 BGB)

Der Kläger beantragt hilfsweise die Anwendung des § 254 BGB und beruft sich auf den Schlichtungsvorschlag des Ombudsmanns, der eine Quotelung von 70/30 zugunsten des Klägers empfahl. Hierzu ist festzustellen:

Erstens: Der Schlichtungsvorschlag ist gemäß § 11 der Verfahrensordnung der Kundenbeschwerdestelle beim DSGVO für keine der Parteien bindend. Er stellt keine rechtliche Beurteilung dar und hat keinen präjudiziellen Charakter für das gerichtliche Verfahren.

Zweitens: Die im Schlichtungsvorschlag vorgenommene Quotelung entbehrt einer tragfähigen rechtlichen Begründung. Der Schlichter hat die höchstrichterliche Rechtsprechung zur groben Fahrlässigkeit bei TAN-Weitergabe nicht hinreichend berücksichtigt.

Drittens: § 254 BGB setzt ein Verschulden **beider** Seiten voraus. Da die Beklagte – wie dargelegt – ihre Pflichten ordnungsgemäß erfüllt hat, scheidet ein Mitverschulden aus. Der Verursachungsbeitrag liegt allein beim Kläger und den Tätern.

III. Zu den vorgerichtlichen Rechtsanwaltskosten

Der Kläger beantragt die Freistellung von vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.054,10 €. Dieser Anspruch ist als Nebenforderung zur Hauptforderung unbegründet, da der Hauptanspruch – wie dargelegt – nicht besteht. Die Beklagte befand sich zu keinem Zeitpunkt in Verzug mit einer berechtigten Forderung.

IV. Beweisangebote

Die Beklagte bietet für ihr tatsächliches Vorbringen folgenden Beweis an:

- Technisches Protokoll der TAN-Verwendung vom 28. Mai 2025 (Anlage B1)
- Sonderbedingungen für das pushTAN-Verfahren, akzeptiert am 05.03.2024 (Anlage B2)
- Quartalsweise Sicherheitshinweise vom 15. Januar 2025, 15. Oktober 2024, 15. Juli 2024, 15. April 2024 mit Zustellnachweisen (Anlage B3)
- Systemprotokoll Transaktionsüberwachung mit TMS-Score-Dokumentation (Anlage B4)
- BaFin-Prüfbericht IT-Sicherheit Oktober 2024, Auszug (Anlage B5)
- Sachverständigengutachten zur Funktionsweise des pushTAN-Verfahrens und zur Sichtbarkeit des vollständigen Anzeigetextes auf dem iPhone 13 (Einholung wird angeregt)
- Zeugnis des Leiters IT-Sicherheit der Beklagten, Dipl.-Inf. Marcus Weber, zur Funktionsweise des TMS

V. Anlagenverzeichnis

Anlage	Bezeichnung
B1	Technisches Protokoll TAN-Verwendung vom 28. Mai 2025
B2	Sonderbedingungen für das pushTAN-Verfahren
B3	Sicherheitshinweise Q1–Q4 (4 Quartalsbriefe mit Zustellnachweisen)
B4	Systemprotokoll Transaktionsüberwachung (TMS-Score-Dokumentation)
B5	BaFin-Prüfbericht IT-Sicherheit Oktober 2024 (Auszug)

RA Prof. Dr. Katharina von Westhoff
 Fachanwältin für Bank- und Kapitalmarktrecht

RA Dr. Jan-Henrik Böttcher
 Fachanwalt für Bank- und Kapitalmarktrecht

Anlage B1

Technisches Protokoll TAN-Verwendung vom 28. Mai 2025

zur Klageerwiderung vom 10. November 2025
in der Sache Peter Mayer ./ Sparkasse Berlin, Az.: 4 O 218/25
Unser Zeichen: HMC-2025/BK-1147

(Dokument als separate Anlage beigelegt)

Anlage B2

Sonderbedingungen für das pushTAN-Verfahren

zur Klageerwiderung vom 10. November 2025
in der Sache Peter Mayer ./ Sparkasse Berlin, Az.: 4 O 218/25
Unser Zeichen: HMC-2025/BK-1147

(Dokument als separate Anlage beigelegt)

Anlage B3

Sicherheitshinweise Q1–Q4 (4 Quartalsbriefe mit Zustellnachweisen)

zur Klageerwiderung vom 10. November 2025
in der Sache Peter Mayer ./ Sparkasse Berlin, Az.: 4 O 218/25
Unser Zeichen: HMC-2025/BK-1147

(Dokument als separate Anlage beigelegt)

Anlage B4

Systemprotokoll Transaktionsüberwachung (TMS-Score-Dokumentation)

zur Klageerwiderung vom 10. November 2025
in der Sache Peter Mayer ./ Sparkasse Berlin, Az.: 4 O 218/25
Unser Zeichen: HMC-2025/BK-1147

(Dokument als separate Anlage beigelegt)

Anlage B5

BaFin-Prüfbericht IT-Sicherheit Oktober 2024 (Auszug)

zur Klageerwiderung vom 10. November 2025
in der Sache Peter Mayer ./ Sparkasse Berlin, Az.: 4 O 218/25
Unser Zeichen: HMC-2025/BK-1147

(Dokument als separate Anlage beigelegt)