

Kanzlei Brezelmann & Partner

Rechtsanwälte und Fachanwälte für Bank- und Kapitalmarktrecht

Kurfürstendamm 195, 10707 Berlin · Tel.: +49 30 889 23 400 · Fax: +49 30 889 23 401 · kanzlei@brezelmann-partner.de

Kanzlei Brezelmann & Partner · Kurfürstendamm 195, 10707 Berlin

Landgericht Berlin

Tegeler Weg 17–21, 10589 Berlin

Unser Zeichen: 2025-B-0478

Datum: 15. September 2025

KLAGESCHRIFT

In der Sache

Peter Mayer, geb. am 14. März 1971,

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 —

wegen: Erstattung nicht autorisierter Zahlungsvorgänge gemäß § 675u BGB

Wert des Streitgegenstandes: 12.295,00 €

Namens und in Vollmacht des Klägers wird beantragt:

1. Die Beklagte wird verurteilt, an den Kläger **12.295,00 €** (in Worten: zwölftausendzweihundertfünfundneunzig Euro) nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 28. Mai 2025 zu zahlen.
 2. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von **1.054,10 €** (1,3-Geschäftsgebühr gemäß Nr. 2300 VV RVG aus einem Gegenstandswert von 12.295,00 € zzgl. Auslagenpauschale Nr. 7002 VV RVG und 19 % USt) freizustellen.
 3. Die Beklagte trägt die Kosten des Rechtsstreits.
 4. Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages.
-

Begründung:

I. Sachverhalt

1. Vertragsverhältnis

Der Kläger unterhielt bei der Beklagten seit dem 12. September 2003 ein Girokonto (IBAN DE89 1005 0000 0478 2395 42, Kundennummer: 478-239-561). Grundlage des Vertragsverhältnisses waren der Girokontovertrag sowie die Allgemeinen Geschäftsbedingungen der Beklagten. Der Kläger nahm ferner am pushTAN-Verfahren teil; die Sonderbedingungen hierfür wurden am 5. März 2024 bei der Neuregistrierung seines Endgeräts (Apple iPhone 13) akzeptiert.

Beweis: Girokontovertrag (Anlage K1), Sonderbedingungen pushTAN (Anlage K2)

2. Der Phishing-Angriff vom 28. Mai 2025

Am 28. Mai 2025 gegen 11:15 Uhr erhielt der Kläger an seinem Arbeitsplatz bei der Kanzlei Dr. Schneider & Partner, Berlin einen Anruf auf seinem Mobiltelefon. Auf dem Display wurde die Rufnummer 030-869869869 angezeigt – die offizielle Servicenummer der Beklagten. Der Kläger kannte diese Nummer, da er sie in der Vergangenheit selbst genutzt hatte, um die Beklagte zu kontaktieren.

Beweis: Eidesstattliche Versicherung des Klägers (Anlage K14), Zeugenaussage Marina Vogt (Anlage K15)

Der Anrufer stellte sich als „Thomas Bergmann vom Sicherheitsteam der Sparkasse Berlin“ vor. Er sprach professionell und akzentfrei. Er nannte den vollständigen Namen des Klägers sowie die letzten Ziffern seiner Kontonummer. Er teilte dem Kläger mit, es seien verdächtige Abbuchungsversuche aus Rumänien festgestellt worden. Das Konto müsse dringend gesperrt werden, um weiteren Schaden abzuwenden.

Der Anrufer erzeugte bewusst eine akute Drucksituation, indem er behauptete, bei verzögerter Reaktion drohe der Verlust sämtlicher Ersparnisse. Er forderte den Kläger auf, zur „Verifizierung“ und „Kontosperre“ eine pushTAN zu generieren.

Der Kläger öffnete die pushTAN-App auf seinem registrierten iPhone 13. Die App zeigte als Beschreibung des Vorgangs an: „Freigabe für Sicherheitssperre“. Diese Formulierung korrespondierte exakt mit der Behauptung des Anrufers. Der Kläger generierte daraufhin die TAN (Wert: 487923) und teilte sie dem Anrufer telefonisch mit. Die TAN-Generierung erfolgte um 11:16:42 Uhr, die TAN-Eingabe durch den Täter um 11:17:14 Uhr.

Beweis: Technisches Protokoll TAN-Verwendung der Beklagten (Anlage K24 – liegt der Beklagten vor), Screenshots pushTAN-App (Anlage K11), Eidesstattliche Versicherung (Anlage K14)

3. Die betrügerischen Transaktionen

Innerhalb von weniger als 70 Sekunden nach der TAN-Eingabe wurden folgende Transaktionen über das Konto des Klägers durchgeführt:

Nr.	Transaktion	Betrag
1.	Überweisung an Digital Services GmbH	4,500.00 €
2.	Überweisung an TechPay Solutions	3,200.00 €
3.	Lastschriftrückgabe Miete	1,850.00 €
4.	Lastschriftrückgabe Versicherungen (gesamt)	645.00 €
5.	Apple Pay Transaktionen (Elektronikfachgeschäfte München/Stuttgart)	2,100.00 €

Gesamt

12,295.00 €

Beweis: Kontoauszüge Nr. 10/2025 und 11/2025 (Anlage K12), Screenshots Push-Benachrichtigungen (Anlage K11)

Bemerkenswert ist, dass die TAN-Eingabe von einer IP-Adresse 185.220.XXX.XXX erfolgte, die als Tor-Exit-Node in den Niederlanden identifiziert wurde. Die Einkäufe mittels Apple Pay erfolgten zeitgleich in München und Stuttgart – der Kläger befand sich nachweislich an seinem Arbeitsplatz in Berlin. Es handelt sich offenkundig um ein automatisiertes Angriffsskript, das die TAN sofort für mehrere vorbereitete Transaktionen verwendete.

4. Unverzügliche Reaktion des Klägers

Der Kläger erkannte anhand der Push-Benachrichtigungen sofort, dass er Opfer eines Betrugs geworden war. Er rief um 11:45 Uhr den Sperr-Notruf 116 116 an und veranlasste die Sperrung seiner Karte und des Online-Bankings. Anschließend kontaktierte er die Hotline der Beklagten. Am 29. Mai 2025 erstattete er Strafanzeige beim Landeskriminalamt Berlin, Dezernat 24 – Cybercrime (Az.: LKA 24/250529/0847).

Beweis: Bestätigung Strafanzeige LKA Berlin (Anlage K13), Eidesstattliche Versicherung (Anlage K14), Zeugenaussage Vogt (Anlage K15)

II. Rechtliche Würdigung

1. Anspruch aus § 675u Abs. 2 BGB

a) Zahlungsdiensterahmenvertrag

Zwischen dem Kläger und der Beklagten besteht ein Zahlungsdiensterahmenvertrag i.S.d. § 675f BGB in Form des Girovertrags. Der Kläger ist Zahler i.S.d. § 675e Abs. 1 BGB, die Beklagte ist Zahlungsdienstleisterin. Die Beklagte unterliegt damit den Pflichten der §§ 675c ff. BGB.

b) Nicht autorisierte Zahlungsvorgänge (§ 675j BGB)

Gemäß § 675j Abs. 1 S. 1 BGB ist ein Zahlungsvorgang gegenüber dem Zahler nur wirksam, wenn dieser dem Zahlungsvorgang zugestimmt hat (Autorisierung). Die Zustimmung muss sich auf den konkreten Zahlungsvorgang beziehen – also auf den Empfänger, den Betrag und den Verwendungszweck (BGH, Ur. v. 26.01.2016 – XI ZR 91/14, Rn. 53).

Der Kläger hat zu keinem Zeitpunkt die Zustimmung zur Ausführung von Überweisungen an die „Digital Services GmbH“ oder „TechPay Solutions“ erteilt. Er hat ebenso wenig der Aktivierung von Apple Pay oder kontaktlosen Zahlungen in München und Stuttgart zugestimmt. Sein Wille war einzig und allein darauf gerichtet, eine „Sicherheitssperre“ seines Kontos zu veranlassen. Ein Autorisierungswille in Bezug auf die tatsächlich ausgeführten Zahlungsvorgänge lag nicht vor.

Die TAN wurde nicht freiwillig im Bewusstsein einer Zahlungsfreigabe erteilt, sondern durch arglistige Täuschung erschlichen. Der BGH hat in seinem Urteil vom 26.01.2016 (XI ZR 91/14, Rn. 58) klargestellt, dass eine durch Täuschung erschlichene Autorisierung keine wirksame Autorisierung im Sinne des § 675j BGB darstellt, wenn der Täuschende selbst nicht Zahlungsdienstleister ist.

c) Erstattungsanspruch dem Grunde nach

Da die streitgegenständlichen Zahlungsvorgänge nicht autorisiert sind, ist die Beklagte gemäß § 675u Abs. 2 BGB verpflichtet, dem Kläger den Zahlungsbetrag unverzüglich zu erstatten und das belastete Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. Der Erstattungsanspruch ist dem Grunde nach gegeben.

2. Kein Ausschluss durch § 675v Abs. 3 Nr. 2 BGB (grobe Fahrlässigkeit)

Die Beklagte wird sich voraussichtlich auf § 675v Abs. 3 Nr. 2 BGB berufen und dem Kläger grobe Fahrlässigkeit bei der telefonischen Weitergabe der TAN vorwerfen. Dieser Einwand greift aus folgenden Gründen nicht durch:

a) Maßstäbe der Rechtsprechung

Grobe Fahrlässigkeit liegt vor, wenn die im Verkehr erforderliche Sorgfalt in besonders schwerem Maße verletzt wird, also wenn schon einfachste, ganz naheliegende Überlegungen nicht angestellt werden und das nicht beachtet wird, was im gegebenen Fall jedem einleuchten musste (BGH, Urt. v. 26.01.2016 – XI ZR 91/14, Rn. 72). Entscheidend ist eine Gesamtwürdigung aller Umstände des Einzelfalls. Die Beweislast für das Vorliegen grober Fahrlässigkeit trägt gemäß § 675v Abs. 4 S. 1 BGB die Beklagte als Zahlungsdienstleisterin.

b) Call-ID-Spoofing als hochprofessionelle Täuschung

Die Täter verwendeten eine technisch anspruchsvolle Methode der Rufnummernmanipulation (sog. Call-ID-Spoofing). Auf dem Mobiltelefon des Klägers wurde die offizielle Servicenummer der Beklagten (030-869869869) angezeigt. Für den Kläger war es objektiv unmöglich, die Fälschung zu erkennen.

Die Anzeige der authentischen Sparkassen-Nummer begründete ein berechtigtes Vertrauen in die Identität des Anrufers. Dieses Vertrauen wurde zusätzlich dadurch verstärkt, dass der Anrufer über persönliche Daten des Klägers (Name, Kontodaten) verfügte. Ein durchschnittlicher Verbraucher durfte bei dieser Sachlage davon ausgehen, tatsächlich mit seiner Bank zu telefonieren.

Das **Landgericht Köln** hat in seinem Urteil vom 08.01.2024 (Az. **15 O 267/23**) in einem vergleichbaren Fall die grobe Fahrlässigkeit verneint. Das Gericht führte aus, dass Call-ID-Spoofing für den durchschnittlichen Verbraucher nicht erkennbar sei und die Anzeige der Bankrufnummer ein erhebliches Vertrauenselement darstelle.

c) Irreführende Anzeige in der pushTAN-App

Der in der pushTAN-App angezeigte Text lautete: „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“. Die **primäre** und optisch hervorgehobene Anzeige „Freigabe für Sicherheitssperre“ korrespondierte **exakt** mit der vom Täter geschilderten Maßnahme.

Diese Formulierung ist objektiv geeignet, den Nutzer in die Irre zu führen. Der Zusatz „und Transaktionsfreigabe – Mehrere Vorgänge“ war auf dem Mobilgerät leicht zu übersehen, insbesondere unter dem psychologischen Druck der Situation. Eine eindeutige Bezeichnung wie „Überweisung an Digital Services GmbH: 4.500,00 €“ wäre technisch möglich und nach Art. 97 Abs. 2 PSD2 geschuldet gewesen.

Es kann dem Kläger nicht als grobe Fahrlässigkeit vorgeworfen werden, einer Anzeige vertraut zu haben, die von der Beklagten selbst so gestaltet wurde, dass sie den wahren Charakter der Transaktion verschleierte.

d) Psychologische Drucksituation

Der Täter erzeugte bewusst eine akute Stresssituation durch die Behauptung, es drohten unmittelbar weitere Schäden durch angebliche Abbuchungsversuche aus Rumänien. Der Kläger handelte unter erheblichem Zeitdruck. Das **Amtsgericht München** (Urt. v. 05.12.2023 – **132 C 49/23**) hat judiziert, dass in einer solchen psychologischen Drucksituation die Schwelle zur groben Fahrlässigkeit erhöht ist. Ein unter Stress und Zeitdruck handelnder Verbraucher erfüllt nicht notwendig den Vorwurf grober Fahrlässigkeit, selbst wenn er objektiv gegen Sorgfaltspflichten verstößt.

e) Berufliche Stellung des Klägers unerheblich

Der Kläger ist von Beruf Rechtsanwaltsfachangestellter. Die Beklagte wird voraussichtlich argumentieren, dass seine berufliche Nähe zum Rechtsbereich ein überdurchschnittliches

Problembewusstsein begründe. Dies ist zurückzuweisen. Die Tätigkeit als Rechtsanwaltsfachangestellter vermittelt keine besonderen Kenntnisse im Bereich der IT-Sicherheit oder Telekommunikationstechnik. Der Maßstab des § 675v Abs. 3 Nr. 2 BGB stellt auf den „durchschnittlichen Zahlungsdienstnutzer“ ab (vgl. ErwGr. 72 PSD2), nicht auf einen IT-Fachmann.

f) Neuere Rechtsprechungsentwicklung

Die von der Beklagten voraussichtlich herangezogene BGH-Rechtsprechung (Urt. v. 26.01.2016 – XI ZR 91/14; Urt. v. 29.11.2016 – XI ZR 429/15) betrifft Fälle, in denen der Geschädigte auf Phishing-E-Mails reagierte – eine deutlich weniger sophistische Täuschungsmethode. Die neuere Instanzrechtsprechung differenziert zunehmend:

- **LG Köln** (Urt. v. 08.01.2024 – 15 O 267/23): Keine grobe Fahrlässigkeit bei Call-ID-Spoofing, wenn die Bankrufnummer angezeigt wird.
- **AG München** (Urt. v. 05.12.2023 – 132 C 49/23): Erhöhte Schwelle zur groben Fahrlässigkeit bei psychologischer Drucksituation.
- **LG Kiel** (Urt. v. 22.03.2024 – 12 O 85/23): Mitverschulden der Bank bei unzureichender Transaktionsüberwachung trotz atypischer Transaktionsmuster.

Diese Entwicklung trägt der Erkenntnis Rechnung, dass die Qualität moderner Phishing-Angriffe die früheren Fälle bei weitem übersteigt und die pauschale Zurechnung grober Fahrlässigkeit den Realitäten des digitalen Zahlungsverkehrs nicht mehr gerecht wird.

3. Eigene Pflichtverletzung der Beklagten

a) Mangelnde Transaktionsüberwachung

Gemäß Art. 97 Abs. 1 lit. b) der Richtlinie (EU) 2015/2366 (PSD2) i.V.m. § 55 Abs. 1 ZAG sind Zahlungsdienstleister verpflichtet, über Sicherheitsvorkehrungen zu verfügen, die die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer schützen. Hierzu gehört ein wirksames Transaktions-Monitoring-System (TMS).

Im vorliegenden Fall hätten folgende Anomalien eine Echtzeit-Intervention auslösen müssen:

- Zwei Überweisungen in Höhe von insgesamt 7.700,00 € an bisher nicht bekannte Empfänger mit ausländischen IBANs (Litauen, Estland) – beides Hochrisikoländer für Geldwäsche
- TAN-Eingabe von einer IP-Adresse, die als Tor-Exit-Node klassifiziert ist – ein klassischer Indikator für betrügerische Aktivitäten
- Apple-Pay-Aktivierung für ein nicht registriertes Gerät unmittelbar nach den Überweisungen
- Drei kontaktlose Zahlungen in München und Stuttgart innerhalb von 30 Sekunden – während der Kontoinhaber seinen Wohnsitz in Berlin hat

Dass das Transaktions-Monitoring-System der Beklagten diese offensichtlichen Anomalien nicht erkannte, stellt eine Verletzung ihrer Pflichten aus § 675f Abs. 2 BGB i.V.m. Art. 97 PSD2 dar.

b) Irreführende App-Gestaltung

Die Beklagte ist gemäß Art. 97 Abs. 2 PSD2 i.V.m. § 55 Abs. 2 ZAG verpflichtet, bei der starken Kundenauthentifizierung sicherzustellen, dass dem Nutzer eindeutige Informationen über den zu autorisierenden Vorgang angezeigt werden („dynamic linking“). Die Formulierung „Freigabe für Sicherheitssperre“ erfüllt diese Anforderung evident nicht. Sie verschleiert den wahren Charakter der Transaktion und erleichtert dadurch betrügerische Angriffe.

c) Unzureichende Betrugserkennungssysteme

Gemäß Art. 2 Nr. 1 der Delegierten Verordnung (EU) 2018/389 sind Zahlungsdienstleister verpflichtet, über Transaktionsüberwachungsmechanismen zu verfügen, die mindestens folgende risikobasierte Faktoren berücksichtigen: den Betrag des Zahlungsvorgangs, bekannte Betrugsszenarien, Anzeichen für Malware-Infektionen in der Sitzung des Zahlungsdienstnutzers und – sofern das Gerät bereitgestellt wird – die Angemessenheit des Standorts des Geräts. Die Beklagte hat gegen sämtliche diese Pflichten verstoßen.

4. Hilfsweise: Mitverschulden (§ 254 BGB)

Selbst wenn das Gericht – entgegen der hier vertretenen Auffassung – eine Mitverantwortung des Klägers annehmen sollte, wäre diese auf maximal 30 % des Gesamtschadens zu beschränken. Der ganz überwiegende Verursachungsbeitrag liegt bei den Tätern und der Beklagten:

- Die Täter haben eine hochprofessionelle Täuschung unter Nutzung technischer Mittel durchgeführt (Hauptverursacher).
- Die Beklagte hat durch die irreführende App-Gestaltung und unzureichende Transaktionsüberwachung die Täuschung ermöglicht bzw. nicht verhindert.
- Der Kläger hat lediglich – durch die Täuschung veranlasst – eine TAN weitergegeben.

Der Ombudsmann der Sparkassen hat in seinem Schlichtungsvorschlag vom 15. August 2025 (Az.: S-2025/07-0891) eine Quotelung von 70/30 zugunsten des Klägers vorgeschlagen. Wir halten eine vollständige Erstattung für gerechtfertigt, akzeptieren jedoch hilfsweise eine Quotelung gemäß § 254 BGB, wobei der Mitverschuldensanteil des Klägers 30 % nicht übersteigen darf.

Beweis: Schlichtungsvorschlag des Ombudsmanns (Anlage K10)

III. Außergerichtliche Bemühungen

Vor Klageerhebung hat der Kläger umfangreiche außergerichtliche Bemühungen unternommen, die sämtlich erfolglos geblieben sind:

1. Der Kläger wandte sich am 28. Mai 2025, 12:15 Uhr per E-Mail an die Beklagte und meldete den Schaden (Anlage K3).
2. Die Beklagte wies die Erstattungsansprüche mit Schreiben vom 2. Juni 2025 unter Verweis auf grobe Fahrlässigkeit zurück (Anlage K4).
3. Der Kläger legte am 3. Juni 2025, 09:45 Uhr Beschwerde ein (Anlage K5).
4. Die Beklagte bestätigte am 5. Juni 2025 die Ablehnung als „abschließend“ (Anlage K6).
5. Der Prozessbevollmächtigte des Klägers forderte die Beklagte mit Schreiben vom 10. Juni 2025 unter Fristsetzung von 14 Tagen zur Erstattung auf (Anlage K7).
6. Die Beklagte wies die Forderung am 20. Juni 2025 vollumfänglich zurück und lehnte auch einen Vergleich ab (Anlage K8).
7. Am 1. Juli 2025 wurde ein Schlichtungsverfahren beim Kundenbeschwerdestelle beim Deutschen Sparkassen- und Giroverband e.V. beantragt (Anlage K9).
8. Der Schlichter Dr. h.c. Wolfgang Reiter empfahl am 15. August 2025 eine Erstattung von 70 % (8.606,50 €). Die Beklagte lehnte diesen Schlichtungsvorschlag ab. Das Verfahren ist gescheitert (Anlage K10).

IV. Zuständigkeit und Zulässigkeit

1. **Sachliche Zuständigkeit:** Das Landgericht Berlin ist gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG sachlich zuständig, da der Streitwert 5.000,00 € übersteigt (Streitwert: 12.295,00 €).

2. **Örtliche Zuständigkeit:** Das Landgericht Berlin ist gemäß § 29 Abs. 1 ZPO örtlich zuständig (Erfüllungsort der Erstattungspflicht: Wohnsitz des Klägers in Berlin). Darüber hinaus hat die Beklagte ihren Sitz in Berlin (§ 17 Abs. 1 ZPO).

3. **Rechtsweg:** Der ordentliche Rechtsweg ist gemäß § 13 GVG eröffnet.

V. Zinsen und vorgerichtliche Rechtsanwaltskosten

Der Zinsanspruch folgt aus §§ 288 Abs. 1, 291 BGB. Der Erstattungsanspruch aus § 675u Abs. 2 BGB wird unverzüglich fällig. Spätestens seit dem 28. Mai 2025 – dem Tag des Schadenseintritts – schuldet die Beklagte Verzugszinsen.

Die vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.054,10 € sind als Verzugsschaden gemäß §§ 280 Abs. 1, 2, 286 BGB erstattungsfähig. Die Beklagte befand sich spätestens seit Ablauf der im Schreiben vom 10. Juni 2025 gesetzten 14-Tages-Frist in Verzug.

RA Dr. Marcus Brezelmann
Fachanwalt für Bank- und Kapitalmarktrecht

ANLAGENVERZEICHNIS

Anlage	Bezeichnung
K1	Girokontovertrag vom 12.09.2003
K2	Sonderbedingungen für das pushTAN-Verfahren
K3	E-Mail des Klägers an die Beklagte vom 28.05.2025
K4	Ablehnungsschreiben der Beklagten vom 02.06.2025
K5	E-Mail des Klägers vom 03.06.2025 (Beschwerde)
K6	Zweites Ablehnungsschreiben der Beklagten vom 05.06.2025
K7	Anwaltsschreiben an die Beklagte vom 10.06.2025
K8	Antwort der Beklagten auf das Anwaltsschreiben vom 20.06.2025
K9	Antrag an den Ombudsmann der Sparkassen vom 01.07.2025
K10	Schlichtungsvorschlag des Ombudsmanns vom 15.08.2025
K11	Screenshots Phishing-Vorfall (Displayanzeige, pushTAN-App, Push-Benachrichtigungen, Anrufliste)
K12	Kontoauszüge Nr. 10/2025 und 11/2025
K13	Bestätigung Strafanzeige LKA Berlin, Az.: LKA 24/250529/0847
K14	Eidesstattliche Versicherung des Klägers vom 05.06.2025
K15	Schriftliche Zeugenaussage Marina Vogt vom 04.06.2025

Anlage K1

Girokontovertrag vom 12.09.2003

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K2

Sonderbedingungen für das pushTAN-Verfahren

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K3

E-Mail des Klägers an die Beklagte vom 28.05.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K4

Ablehnungsschreiben der Beklagten vom 02.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K5

E-Mail des Klägers vom 03.06.2025 (Beschwerde)

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K6

Zweites Ablehnungsschreiben der Beklagten vom 05.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K7

Anwaltsschreiben an die Beklagte vom 10.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K8

Antwort der Beklagten auf das Anwaltsschreiben vom 20.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K9

Antrag an den Ombudsmann der Sparkassen vom 01.07.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K10

Schlichtungsvorschlag des Ombudsmanns vom 15.08.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K11

Screenshots Phishing-Vorfall (Displayanzeige, pushTAN-App, Push-Benachrichtigungen, Anrufliste)

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K12

Kontoauszüge Nr. 10/2025 und 11/2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K13

Bestätigung Strafanzeige LKA Berlin, Az.: LKA 24/250529/0847

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K14

Eidesstattliche Versicherung des Klägers vom 05.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)

Anlage K15

Schriftliche Zeugenaussage Marina Vogt vom 04.06.2025

zur Klageschrift vom 15. September 2025
in der Sache Peter Mayer ./ Sparkasse Berlin
Az.: 2025-B-0478

(Dokument als separate Anlage beigelegt)