

Arbeitsakte

Akte Phishing-Vorfall Mayer ./. Sparkasse Berlin

phishing-vorfall-mayer-sparkasse-berlin

Diese Datei bündelt alle Aktenstücke in einem Dokument. Die Einzeldateien liegen im Aktenordner ebenfalls vor.

Inhaltsverzeichnis

Teil	Inhalt
Teil 1	Aktenstücke (Markdown) (5)
Teil 2	CSV-Tabellen (2)
Teil 3	PDF-Anhänge (Originaldokumente) (24)

Aktenstücke (Markdown)

Datei: 00_aktenuebersicht.md

Aktenübersicht

Stammdaten

- Mandant: Peter Mayer
- Gegnerin: Sparkasse Berlin
- Aktenzeichen Mandat: 2025-B-0478
- späteres Gerichtsaktenzeichen: LG Berlin, 4 O 218/25
- Konto: DE89 1005 0000 0478 2395 42
- Schaden: 12.295,00 EUR
- Vorfall: 28.05.2025

Originalunterlagen

Nr.	Datei	Bedeutung
01	`01_Aktendeckblatt.pdf`	Stammdaten, Schaden, Aktenzeichen
02	`02_Vollmacht_und_Mandatsvertrag.pdf`	Mandat und Vollmacht
03	`03_Kontovertrag_und_AGB.pdf`	Kontovertrag und AGB
04	`04_Sonderbedingungen_pushTAN.pdf`	Pflichten und pushTAN-Regeln
05	`05_Aktennotiz_Erstkontakt.pdf`	Erstkontakt und Mandantenschilderung
06	`06_Email_Mayer_an_Sparkasse_280525.pdf`	erste Reklamation
07	`07_Ablehnungsschreiben_Sparkasse_020625.pdf`	erste Ablehnung Bank
08	`08_Email_Mayer_an_Sparkasse_030625.pdf`	Gegendarstellung Mandant
09	`09_Zweites_Ablehnungsschreiben_Sparkasse_050625.pdf`	endgültige Bankablehnung
10	`10_Email_Mayer_an_Freund_290525.pdf`	zeitnahe Sachverhaltsbericht
11	`11_Screenshots_Phishing.pdf`	Screenshots/Anrufanzeige

Nr.	Datei	Bedeutung
12	`12_Internes_Rechtsgutachten_Sparkasse.pdf`	Bankinterne Rechtsposition
13	`13_Anwaltsschreiben_an_Sparkasse_100625.pdf`	anwaltliche Aufforderung
14	`14_Antwort_Sparkasse_auf_Anwalt_200625.pdf`	Bankantwort
15	`15_Antrag_Ombudsmann_010725.pdf`	Schlichtungsantrag
16	`16_Schlichtungsvorschlag_Ombudsmann_150825.pdf`	70/30-Vorschlag
17	`17_Kontoauszuege.pdf`	Kontoauszüge/Schadenspositionen
18	`18_Strafanzeige_Bescheinigung.pdf`	Strafanzeige
19	`19_Eidesstattliche_Versicherung_Mayer.pdf`	Mandantenerklärung
20	`20_Zeugenaussage_Kollegin.pdf`	Zeugin zur Drucksituation
21	`21_Klageschrift_mit_Anlagen.pdf`	Klageentwurf/Klage
22	`22_Klageerwiderung_Sparkasse.pdf`	Verteidigung Bank
23	`23_Sicherheitshinweis_Sparkasse_150125.pdf`	frühere Sicherheitshinweise
24	`24_Technisches_Protokoll_TAN.pdf`	TAN-/IP-/Device-Protokoll

Kernproblem

Der Mandant gab im Rahmen eines Spoofing-Anrufs eine pushTAN weiter. Die Bank beruft sich auf grobe Fahrlässigkeit. Die Mandantenseite muss zeigen, dass keine Autorisierung der konkreten Zahlungen vorlag und dass der Bankeinwand aus § 675v BGB wegen Täuschungslage, App-Dialog und auffälliger Banklogs nicht durchgreift.

Datei: 04_erstbewertung_675u_675v.md

Erstbewertung § 675u / § 675v BGB

Kurzfazit

Der Fall ist anspruchsvoll, aber klagefähig. Der Mandant hat gute Argumente für einen nicht autorisierten Zahlungsvorgang, weil er nach seiner Darstellung keinen konkreten Zahlungsauftrag an die Empfänger freigeben wollte, sondern in einem durch Call-ID-Spoofing erzeugten Sicherheitsnarrativ handelte. Der zentrale Angriffspunkt der Bank bleibt aber erheblich: Die TAN wurde telefonisch weitergegeben und die Bank behauptet Warnhinweise sowie eine starke Kundenauthentifizierung.

§ 675u BGB

Für den Mandanten sprechen:

- keine bewusste Freigabe der konkreten Empfänger und Beträge,
- Call-ID-Spoofing mit offizieller Banknummer,
- angeblicher Sicherheitsvorgang,
- möglicher Sammel-/Batch-Charakter der Freigabe,
- sehr schnelle Transaktionskette.

Offen bleibt:

- exakter App-Dialog,
- konkrete Darstellung von Betrag und Empfänger,
- technische Transaktionsbindung.

Ampel: **Grün/Gelb**.

§ 675v BGB

Für die Bank sprechen:

- TAN wurde am Telefon genannt,
- vorherige allgemeine Sicherheitshinweise,
- berufliche Erfahrung des Mandanten,
- bankseitiger Vortrag zu eindeutiger Freigabe.

Für den Mandanten sprechen:

- professionelle Täuschung,
- Spoofing der Servicenummer,
- Drucksituation,
- schnelle Sperre,
- fremde/riskante IP und möglicher Standortbruch,
- bankseitige Monitoringfrage.

Ampel: **Gelb mit hohem Prozessrisiko**.

Sofort nächste Schritte

1. Banklogs und App-Dialog vollständig anfordern.
2. Mandantenerklärung um zeitlichen Ablauf und subjektive Wahrnehmung des App-Diialogs ergänzen.
3. Zeugin zur Drucksituation und zum unmittelbaren Verhalten sichern.
4. Technisches Protokoll mit IP-/Device-Bruch als Bankpflicht-/Monitoringthema ausbauen.
5. Klage nicht nur auf "Phishing", sondern auf fehlende konkrete Autorisierung und unzureichenden Nachweis stützen.

Datei: 05_grobe_fahrlaessigkeit_ampel.md

Grobe-Fahrlässigkeit-Ampel Mayer ./ Sparkasse

Rot aus Mandantensicht

- TAN wurde am Telefon weitergegeben.
- Bank kann sich auf allgemeine Sicherheitsinformationen berufen.
- Mandant ist rechtsnah berufserfahren.
- Klageerwiderung behauptet klare App-Anzeige mit Transaktionsfreigabe.

Grün aus Mandantensicht

- Caller-ID-Spoofing mit offizieller Banknummer.
- Täuschung als akuter Sicherheitsvorfall.
- Zeitdruck und Autoritätsgefälle.
- Sperre innerhalb kurzer Zeit.
- fremde IP/Tor-Exit-Node im technischen Protokoll.
- manuelle Bankprüfung erst nach Abschluss der Vorgänge.

Gelbe Kernfragen

- War die pushTAN-Anzeige objektiv klar genug?
- Konnte der Mandant erkennen, dass er konkrete Zahlungen freigab?
- Reichen allgemeine Warnhinweise von Januar für grobe Fahrlässigkeit im Mai?
- Hätte die Bank bei Score 72 und Schwelle 75 plus Tor-/Geräteauffälligkeit eskalieren müssen?

Arbeitshypothese

Der Fall sollte nicht als "TAN genannt, also verloren" behandelt werden. Ebenso wenig ist er ein sicherer Erstattungsfall. Die beste Linie ist: konkrete Autorisierung bestreiten, Bankbeweis nach § 675w BGB angreifen, § 675v BGB mit den besonderen Täuschungs- und Monitoringumständen entschärfen.

Datei: 06_bankpflichten_und_tech_logs.md

Bankpflichten und technische Logs

Auffälligkeiten aus der Akte

- TAN-Generierung vom registrierten iPhone.
- TAN-Einsatz/Online-Banking-Aktion aus fremder Umgebung mit Tor-Hinweis.
- sehr kurze Transaktionskette.
- Apple-Pay-/Händlertransaktionen kurz nach Überweisungen.
- Risikoscore 72 bei interner Schwelle 75.

- manuelle Review erst nach Durchführung.

Prüfungsfragen

1. Welche App-Anzeige sah der Mandant exakt?
2. War die TAN dynamisch mit Betrag und Empfänger verknüpft?
3. Wurde ein neuer Empfänger angelegt?
4. Gab es Limitänderungen?
5. War die Bank technisch in der Lage, den Orts-/IP-Wechsel zu erkennen?
6. Warum löste Score 72 keine Rückfrage aus?
7. Warum wurde bei schneller Sequenz und Kontoleerung nicht angehalten?
8. Wurden Rückholungen/Recalls unverzüglich versucht?

Beweisanforderung

Die Bank sollte nicht nur pauschal "starke Kundenauthentifizierung" behaupten dürfen. Anzufordern sind die konkreten Protokolle, die zeigen, was authentifiziert wurde, was autorisiert wurde und warum das Monitoring die Vorgänge passieren ließ.

Datei: 07_ombudsmann_und_klagepfad.md

Ombudsmann und Klagepfad

Ombudsmann

Der Schlichtungsvorschlag sieht eine Quote 70/30 zugunsten des Mandanten vor:

- Zahlung Bank: 8.606,50 EUR
- Eigenanteil Mandant: 3.688,50 EUR

Das spricht dafür, dass der Fall auch neutral nicht als klarer Bank- oder Kundenfall bewertet wurde. Die Ablehnung durch die Bank kann im Prozess taktisch erwähnt werden, ersetzt aber keine Anspruchsbegründung.

Klagepfad

Die Klage muss vier Dinge leisten:

1. konkrete Autorisierung bestreiten,
2. Bankbeweis nach § 675w BGB konkret angreifen,
3. grobe Fahrlässigkeit nicht verschweigen, sondern erklären,
4. technische Auffälligkeiten als Monitoring-/Pflichtenthema verwerten.

Risiken

- Gericht kann TAN-Weitergabe als grob fahrlässig ansehen.
- Wenn der App-Dialog klar Betrag und Empfänger zeigte, wird der Fall deutlich schwächer.

- Allgemeine Sicherheitswarnungen sind nicht entscheidend, aber gefährlich.
- Der Alternativantrag auf Quote kann sinnvoll sein, darf aber den Hauptanspruch nicht verwässern.

Nächster sinnvoller Schriftsatz

Ein Schriftsatz sollte die Klageerwiderung anhand einer Vier-Spalten-Tabelle beantworten:

Bankbehauptung	Mandantenposition	Beweis	rechtliche Folge
----------------	-------------------	--------	------------------

CSV-Tabellen

Datei: 02_transaktionsmatrix.csv

Zeitpunkt	Zahlungsart	Empfaenger_oder_Haendler	Betrag_EUR	Quelle	Anmerkung
2025-05-28 11:17	Ueberweisung	Digital Services GmbH	4500.00	17_Kontoauszuege.pdf	streitige Online-Banking-Transaktion
2025-05-28 11:17	Ueberweisung	TechPay Solutions	3200.00	17_Kontoauszuege.pdf	streitige Online-Banking-Transaktion
2025-05-28 11:18	Lastschriftrueckgabe	Miete	1850.00	17_Kontoauszuege.pdf	Rueckgabe als Schaden erfasst
2025-05-28 11:18	Lastschriftrueckgabe	Versicherungen gesamt	645.00	17_Kontoauszuege.pdf	Rueckgabe als Schaden erfasst
2025-05-28 11:19	Apple Pay	MediaMarkt Muenchen	849.00	17_Kontoauszuege.pdf	Wallet-/Kartenvorgang
2025-05-28 11:19	Apple Pay	Saturn Stuttgart	599.00	17_Kontoauszuege.pdf	Wallet-/Kartenvorgang
2025-05-28 11:20	Apple Pay	Expert Muenchen	652.00	17_Kontoauszuege.pdf	Wallet-/Kartenvorgang

Datei: 03_beweis_und_log_matrix.csv

Beweisfrage	Vorhandener_Beleg	Offene_Anforderung	Bewertung
Konkreter App-Freigabetext	11_Screenshots_Phishing.pdf und Parteivortrag	Vollständiger serverseitiger Freigabetext mit Layout und Parametern	GELB
TAN-Generierung und TAN-Einsatz	24_Technisches_Protokoll_TAN.pdf	Vollständige TAN-Session inklusive Transaktionsbindung	GELB
IP-Wechsel und Tor-Hinweis	24_Technisches_Protokoll_TAN.pdf	Geo-/Risk-Engine und Monitoringentscheidung	GRUEN fuer Mandant
Zeitnahe Sperre	06_Email_Mayer_an_Sparkasse_280525.pdf und Sperrzeiten	Hotline-/Sperrnotrufprotokoll	GRUEN fuer Mandant
Sicherheitswarnungen	23_Sicherheitshinweis_Sparkasse_150125.pdf	Zustellung und konkrete Wahrnehmung durch Mandant	GELB
Grobe Fahrlässigkeit	07/09/14/22 Bankunterlagen	konkrete App-Anzeige und Warnwirkung im Moment der TAN	GELB bis ROT
Bankmonitoring	24_Technisches_Protokoll_TAN.pdf	Risikoscore 72/Schwelle 75 und manuelle Review-Akte	GELB fuer Mandant
Schaden	17_Kontoauszuege.pdf	Rueckholungsversuche und endgültige Valuta	GRUEN

PDF-Anhang: originale/01_Aktendeckblatt.pdf

Datei: 01_Aktendeckblatt.pdf

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

MANDATSSTAMMBLATT

Aktenzeichen: 2025-B-0478

Sache: Mayer ./ Sparkasse Berlin

Sachgebiet: Bank- und Kapitalmarktrecht / Zahlungsdiensterecht

I. Mandantendaten

Name:	Peter Mayer
Geburtsdatum:	14. März 1971
Anschrift:	Lietzenburger Straße 74, 10719 Berlin
Telefon (Festnetz):	+49 30 882 74 91
Telefon (Mobil):	+49 170 448 23 56
E-Mail:	peter.mayer1971@gmail.com
Beruf:	Rechtsanwaltsfachangestellter
Arbeitgeber:	Kanzlei Dr. Schneider & Partner, Berlin
Familienstand:	ledig
Steuerliche ID:	57 821 034 219

II. Gegner

Bezeichnung:	Sparkasse Berlin
Anschrift:	Alexanderplatz 2, 10178 Berlin
Kundennummer:	478-239-561
Konto-IBAN:	DE89 1005 0000 0478 2395 42

III. Streitgegenstand

Erstattungsanspruch gemäß § 675u BGB wegen nicht autorisierter Zahlungsvorgänge infolge eines Phishing-/Spoofing-Angriffs (sog. Call-ID-Spoofing mit Social Engineering). Schadenshöhe: 12,295.00 € zzgl. Nebenforderungen.

IV. Streitwert und Gebühren

Vorläufiger Streitwert: 12,295.00 €

Gerichtsgebühren (3,0 Gebühr): 798,00 €

Rechtsanwaltsgebühren (1,3 Verfahrensgebühr + 1,2 Terminsgebühr): 2.077,94 € zzgl. USt.

V. Fristen und Termine

Mandatserteilung:	3. Juni 2025
Frist Ombudsmann:	4 Wochen ab 05.06.2025 = 03.07.2025
Klageeinreichung:	15. September 2025
Klagezustellung:	29. September 2025
Klageerwiderungsfrist:	10.11.2025 (verlängert)

VI. Bearbeiter

Federführung: RA Dr. Marcus Brezelmann

Sachbearbeitung: RAin Julia Eichenwald (Ref.)

Angelegt am: 3. Juni 2025

gez. RA Dr. Marcus Brezelmann

PDF-Anhang: originale/02_Vollmacht_und_Mandatsvertrag.pdf

Datei: 02_Vollmacht_und_Mandatsvertrag.pdf

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

VOLLMACHT

Hiermit erteile ich, **Peter Mayer**, geb. am 14. März 1971, wohnhaft Lietzenburger Straße 74, 10719 Berlin,

der Kanzlei **Kanzlei Brezelmann & Partner**, Kurfürstendamm 195, 10707 Berlin, namentlich **RA Dr. Marcus Brezelmann** sowie dessen Sozien und mit ihm verbundenen Rechtsanwälten

Vollmacht

mich in der Angelegenheit

Peter Mayer ./ Sparkasse Berlin

wegen Erstattung nicht autorisierter Zahlungsvorgänge

Streitwert: 12,295.00 €

zu vertreten. Die Vollmacht erstreckt sich auf alle mit dieser Angelegenheit zusammenhängenden Verfahren und Rechtsstreitigkeiten, einschließlich:

1. Außergerichtliche Vertretung und Korrespondenz mit dem Gegner und Dritten
2. Vertretung in Schlichtungs- und Mediationsverfahren, insbesondere vor dem Ombudsmann der Sparkassen
3. Erhebung und Zustellung von Klagen, Einlegung und Zurücknahme von Rechtsmitteln
4. Vertretung vor allen Gerichten aller Instanzen und Rechtszüge
5. Abschluss von Vergleichen und Empfangnahme von Geldern
6. Erteilung und Widerruf von Untervollmachten
7. Erhebung von Widerklagen und Anschlussrechtsmitteln
8. Vertretung in Zwangsvollstreckungsverfahren
9. Akteneinsicht und Abholung von Dokumenten bei Behörden und Gerichten

Die Vollmacht gilt im Innenverhältnis auch über den Tod des Vollmachtgebers hinaus (§ 672 BGB). Ein Widerruf ist jederzeit möglich.

Berlin, den 3. Juni 2025

Peter Mayer

(Mandant)

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

MANDATSVERTRAG

(Geschäftsbesorgungsvertrag gemäß §§ 611, 675 BGB)

zwischen

Peter Mayer, Lietzenburger Straße 74, 10719 Berlin
— nachfolgend „Mandant“ —

und

Kanzlei Brezelmann & Partner, Kurfürstendamm 195, 10707 Berlin
vertreten durch RA Dr. Marcus Brezelmann
— nachfolgend „Kanzlei“ —

§ 1 Mandatsgegenstand

(1) Der Mandant beauftragt die Kanzlei mit der rechtlichen Beratung und Vertretung in der Angelegenheit „Peter Mayer ./ Sparkasse Berlin“ wegen Erstattung nicht autorisierter Zahlungsvorgänge (Phishing-Schaden) in Höhe von 12,295.00 € nebst Nebenforderungen.

(2) Der Auftrag umfasst die außergerichtliche Geltendmachung, die Durchführung eines Schlichtungsverfahrens beim Ombudsmann der Sparkassen sowie ggf. die gerichtliche Durchsetzung der Ansprüche in erster und zweiter Instanz.

§ 2 Vergütung

(1) Die Vergütung richtet sich nach dem Rechtsanwaltsvergütungsgesetz (RVG) in der jeweils geltenden Fassung. Maßgeblicher Gegenstandswert ist der Betrag der geltend gemachten Forderung.

(2) Neben den gesetzlichen Gebühren werden Auslagen gemäß VV RVG Nr. 7000 ff. berechnet. Die Umsatzsteuer wird gesondert ausgewiesen.

(3) Ein Vorschuss in Höhe einer 1,3-Geschäftsgebühr gemäß Nr. 2300 VV RVG auf den Gegenstandswert von 12,295.00 € wird mit Mandatserteilung fällig.

§ 3 Pflichten der Kanzlei

(1) Die Kanzlei verpflichtet sich zur sorgfältigen und gewissenhaften Bearbeitung des Mandats unter Beachtung der geltenden Berufspflichten (BRAO, BORA, CCBE).

(2) Der Mandant wird über wesentliche Verfahrensschritte, Fristen und Termine unverzüglich informiert.

§ 4 Pflichten des Mandanten

(1) Der Mandant verpflichtet sich zur vollständigen und wahrheitsgemäßen Sachverhaltsschilderung sowie zur zeitnahen Übermittlung aller verfahrensrelevanten Unterlagen.

(2) Adressänderungen und sonstige Änderungen persönlicher Daten sind der Kanzlei unverzüglich mitzuteilen.

§ 5 Kündigung

Das Mandatsverhältnis kann von beiden Seiten jederzeit ohne Angabe von Gründen gekündigt werden (§ 627 BGB). Die Vergütung für bis dahin erbrachte Leistungen bleibt hiervon unberührt.

§ 6 Datenschutz

Die Verarbeitung personenbezogener Daten erfolgt im Einklang mit der DSGVO und dem BDSG. Eine gesonderte Datenschutzhinweisung gemäß Art. 13 DSGVO wurde dem Mandanten ausgehändigt.

§ 7 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Abbedingung dieser Schriftformklausel.

(2) Sollte eine Bestimmung dieses Vertrages unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

(3) Es gilt deutsches Recht. Gerichtsstand ist Berlin.

Berlin, den 3. Juni 2025

Peter Mayer
(Mandant)

RA Dr. Marcus Brezelmann
(Kanzlei)

PDF-Anhang: originale/03_Kontovertrag_und_AGB.pdf

Datei: 03_Kontovertrag_und_AGB.pdf

GIROKONTOVERTRAG

(Zahlungsdiensterahmenvertrag gemäß §§ 675f ff. BGB)

Kontonummer: IBAN DE89 1005 0000 0478 2395 42

BIC: BELADEBEXXX

Kontoinhaberin/Kontoinhaber: Peter Mayer

Kundennummer: 478-239-561

Kontoeröffnung: 12. September 2003

Kontomodell: Sparkassen-Giro Komfort

zwischen

Sparkasse Berlin, Alexanderplatz 2, 10178 Berlin

— nachfolgend „Sparkasse“ —

und

Peter Mayer, Lietzenburger Straße 74, 10719 Berlin

— nachfolgend „Kunde“ —

§ 1 Vertragsgegenstand

(1) Die Sparkasse führt für den Kunden ein Girokonto (Zahlungskonto) zur Abwicklung des bargeldlosen Zahlungsverkehrs. Der Vertrag wird als Zahlungsdiensterahmenvertrag im Sinne des § 675f Abs. 2 BGB geschlossen.

(2) Es gelten die beigefügten Allgemeinen Geschäftsbedingungen der Sparkasse, die Sonderbedingungen für den Überweisungsverkehr, die Sonderbedingungen für das Online-Banking sowie die Sonderbedingungen für das pushTAN-Verfahren.

§ 2 Kontoführung

(1) Über das Konto können Überweisungen, Lastschriften, Daueraufträge, Kartenzahlungen sowie sonstige im Zahlungsverkehr übliche Transaktionen abgewickelt werden.

(2) Dem Kunden wird ein Dispositionskredit in Höhe von 3.500,00 € eingeräumt. Der Zinssatz für die Inanspruchnahme beträgt derzeit 12,43 % p.a.

§ 3 Authentifizierungsverfahren

(1) Für die Autorisierung von Zahlungsvorgängen im Online-Banking nutzt der Kunde das pushTAN-Verfahren. Die hierzu geltenden Sonderbedingungen sind Bestandteil dieses Vertrages.

(2) Das pushTAN-Verfahren erfüllt die Anforderungen an die starke Kundenauthentifizierung gemäß Art. 97 der Richtlinie (EU) 2015/2366 (PSD2) i.V.m. § 55 ZAG.

§ 4 Entgelte

- (1) Monatliche Kontoführungsgebühr: 4,90 €
- (2) Beleghafte Überweisungen: 1,50 € je Auftrag
- (3) Online-Überweisungen: 0,00 €
- (4) Debitkarte (Sparkassen-Card): 6,00 € p.a.
- (5) Kreditkarte (Sparkassen-Kreditkarte Classic): 30,00 € p.a.

§ 5 Haftung bei nicht autorisierten Zahlungsvorgängen

(1) Im Falle eines nicht autorisierten Zahlungsvorgangs hat die Sparkasse dem Kunden den Zahlungsbetrag unverzüglich zu erstatten und das Konto wieder auf den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte (§ 675u Abs. 2 BGB).

(2) Abweichend von Absatz 1 ist der Kunde der Sparkasse zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Kunde ihn durch vorsätzliches oder grob fahrlässiges Verhalten herbeigeführt hat (§ 675v Abs. 3 Nr. 2 BGB).

- (3) Grobe Fahrlässigkeit des Kunden kann insbesondere vorliegen, wenn er
- a) die personalisierten Sicherheitsmerkmale (PIN, TAN) einer anderen Person mitgeteilt hat,
 - b) den Verlust, Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments nicht unverzüglich angezeigt hat, nachdem er hiervon Kenntnis erlangt hat,
 - c) die personalisierten Sicherheitsmerkmale ungesichert aufbewahrt hat.

§ 6 Sorgfaltspflichten des Kunden

(1) Der Kunde hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von den personalisierten Sicherheitsmerkmalen (insbesondere PIN und TAN) erlangt.

(2) TANs dürfen nur für die Autorisierung von Zahlungsvorgängen oder sonstigen in den Online-Banking-Bedingungen vorgesehenen Aufträgen verwendet werden. Die Sparkasse wird den Kunden niemals telefonisch, per E-Mail oder per SMS zur Mitteilung von TANs, PINs oder Passwörtern auffordern.

§ 7 Anzeige- und Sorgfaltspflichten

(1) Stellt der Kunde fest, dass ein Zahlungsvorgang nicht autorisiert oder fehlerhaft ausgeführt wurde, hat er die Sparkasse unverzüglich zu unterrichten (§ 676b Abs. 1 BGB).

(2) Ansprüche und Einwendungen nach § 676b Abs. 2 BGB sind ausgeschlossen, wenn der Kunde die Sparkasse nicht spätestens 13 Monate nach dem Tag der Belastung unterrichtet hat.

§ 8 Laufzeit und Kündigung

- (1) Der Vertrag wird auf unbestimmte Zeit geschlossen.
- (2) Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Kündigungsfrist kündigen.
- (3) Die Sparkasse kann den Vertrag mit einer Frist von mindestens zwei Monaten kündigen.

Berlin, den 12. September 2003

Peter Mayer
(Kunde)

Sparkasse Berlin
(Institut)

ALLGEMEINE GESCHÄFTSBEDINGUNGEN

der Sparkasse Berlin
Stand: 1. Januar 2025

1. Geltungsbereich und Änderungen dieser Geschäftsbedingungen

- (1) Diese Allgemeinen Geschäftsbedingungen gelten für die gesamte Geschäftsverbindung zwischen dem Kunden und der Sparkasse.
- (2) Änderungen dieser Geschäftsbedingungen werden dem Kunden spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Kunde mit der Sparkasse einen elektronischen Kommunikationsweg vereinbart, können die Änderungen auch auf diesem Wege angeboten werden.

2. Bankgeheimnis und Datenschutz

- (1) Die Sparkasse ist zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet, von denen sie Kenntnis erlangt (Bankgeheimnis). Die Sparkasse darf Kundendaten nur dann weitergeben, wenn gesetzliche Bestimmungen dies gebieten oder der Kunde eingewilligt hat.
- (2) Die Verarbeitung personenbezogener Daten erfolgt gemäß den Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

3. Haftung der Sparkasse

- (1) Bei der Erfüllung ihrer Verpflichtungen haftet die Sparkasse für jedes Verschulden ihrer Mitarbeiter und der Personen, die sie zur Erfüllung ihrer Verpflichtungen hinzuzieht.
- (2) Hat der Kunde durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Sparkasse und Kunde den Schaden zu tragen haben.

8. Mitwirkungspflichten des Kunden

- (1) Der Kunde hat für die Richtigkeit und Vollständigkeit der von ihm gegenüber der Sparkasse abgegebenen Erklärungen und eingereichten Unterlagen zu sorgen.
- (2) Der Kunde hat der Sparkasse unverzüglich Änderungen seiner Identifikationsdaten (Name, Adresse, Legitimationsdokumente) mitzuteilen.

11. Besondere Regeln für den Zahlungsverkehr

- (1) Die Sparkasse führt Zahlungsaufträge des Kunden aus, sofern diese ordnungsgemäß erteilt und durch die vereinbarten Authentifizierungsverfahren autorisiert wurden.
- (2) Der Kunde darf die personalisierten Sicherheitsmerkmale (insbesondere PIN, TAN) nicht an Dritte weitergeben. Er hat sicherzustellen, dass keine andere Person Kenntnis von den Sicherheitsmerkmalen erlangt. Die Sparkasse wird den Kunden niemals telefonisch, per E-Mail oder per SMS zur Preisgabe seiner personalisierten Sicherheitsmerkmale auffordern.**
- (3) Erkennt der Kunde den Verlust oder den Diebstahl seines Zahlungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung, so hat er dies der Sparkasse unverzüglich anzuzeigen (Sperranzeige).

15. Haftung bei nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgängen

- (1) Bei nicht autorisierten Zahlungsvorgängen hat die Sparkasse gegen den Kunden keinen Anspruch auf Erstattung ihrer Aufwendungen. Sie ist verpflichtet, dem Kunden den Zahlungsbetrag unverzüglich zu erstatten (§ 675u Abs. 2 BGB).
- (2) Abweichend von Absatz 1 haftet der Kunde für den gesamten Schaden aus nicht autorisierten Zahlungsvorgängen, wenn er diese durch vorsätzliche oder grob fahrlässige Verletzung seiner Sorgfaltspflichten nach Nr. 11 dieser Bedingungen ermöglicht hat (§ 675v Abs. 3 Nr. 2 BGB).
- (3) Solange der Kunde die Sperranzeige nach Nr. 11 Abs. 3 nicht abgegeben hat, haftet er für Schäden aus nicht autorisierten Zahlungsvorgängen bis zu einem Betrag von 50,00 € (§ 675v Abs. 1 BGB), es sei denn, der Kunde hat den Eintritt des Schadens nicht zu vertreten oder die Sparkasse hat eine starke Kundenauthentifizierung nach § 55 ZAG nicht verlangt.

20. Außergerichtliche Streitschlichtung

- (1) Für die Beilegung von Streitigkeiten mit der Sparkasse kann der Kunde die bei der Deutschen Bundesbank eingerichtete Schlichtungsstelle oder den Ombudsmann der deutschen Sparkassen anrufen.
- (2) Die Adresse des Ombudsmanns der Sparkassen lautet: Kundenbeschwerdestelle beim Deutschen Sparkassen- und Giroverband e.V., Charlottenstraße 47, 10117 Berlin.

PDF-Anhang: originale/04_Sonderbedingungen_pushTAN.pdf

Datei: 04_Sonderbedingungen_pushTAN.pdf

SONDERBEDINGUNGEN

für das pushTAN-Verfahren der Sparkasse Berlin

Stand: 1. Januar 2025

1. Gegenstand und Anwendungsbereich

(1) Diese Sonderbedingungen regeln die Nutzung des pushTAN-Verfahrens als Authentifizierungsinstrument im Online-Banking der Sparkasse Berlin.

(2) Das pushTAN-Verfahren dient der Autorisierung von Zahlungsvorgängen und sonstigen Aufträgen im Sinne des § 675j Abs. 1 BGB. Es erfüllt die Anforderungen der starken Kundenauthentifizierung gemäß Art. 97 der Richtlinie (EU) 2015/2366 (PSD2) i.V.m. § 55 ZAG.

2. Funktionsweise

(1) Beim pushTAN-Verfahren wird die TAN in der SparkassenApp auf dem registrierten Mobilgerät des Kunden generiert und angezeigt.

(2) Vor der TAN-Generierung werden dem Kunden die wesentlichen Daten des zu autorisierenden Vorgangs angezeigt (insbesondere Empfänger, Betrag, Verwendungszweck bei Überweisungen; Art des Auftrags bei sonstigen Vorgängen).

(3) Die TAN ist nur für den angezeigten Vorgang gültig und verfällt nach 5 Minuten.

3. Sorgfaltspflichten des Kunden

(1) Der Kunde hat das Mobilgerät, auf dem die SparkassenApp installiert ist, vor dem Zugriff Dritter zu schützen. Der Zugang zur SparkassenApp ist durch ein sicheres Passwort, eine PIN oder ein biometrisches Merkmal zu sichern.

(2) Der Kunde darf die TAN keinem Dritten mitteilen oder sonst zugänglich machen. Die TAN darf ausschließlich über die von der Sparkasse bereitgestellte Eingabemaske im Online-Banking eingegeben werden. Eine telefonische, mündliche oder schriftliche Weitergabe der TAN an Dritte ist unter keinen Umständen zulässig.

(3) Der Kunde hat vor Bestätigung der TAN die in der SparkassenApp angezeigten Auftragsdaten sorgfältig zu prüfen. Stimmen die angezeigten Daten nicht mit dem beabsichtigten Auftrag überein, ist der Vorgang abzubrechen.

(4) Der Kunde hat die SparkassenApp stets auf dem aktuellen Stand zu halten und Sicherheitsupdates unverzüglich zu installieren.

(5) Der Kunde darf das Mobilgerät nicht in einer Weise verändern (z.B. Jailbreak, Root), die die Sicherheit der SparkassenApp beeinträchtigen könnte.

4. Sperrmöglichkeiten

(1) Der Kunde kann das pushTAN-Verfahren jederzeit sperren lassen, indem er die Sparkasse über den Sperr-Notruf (116 116) oder über die Hotline der Sparkasse Berlin kontaktiert.

(2) Die Sparkasse ist berechtigt, das pushTAN-Verfahren zu sperren, wenn Tatsachen die Annahme rechtfertigen, dass das Verfahren missbräuchlich genutzt wird oder die Sicherheit des Verfahrens nicht mehr gewährleistet ist.

5. Haftung

(1) Die Haftung bei nicht autorisierten Zahlungsvorgängen richtet sich nach den gesetzlichen Bestimmungen (§§ 675u, 675v BGB) sowie den Allgemeinen Geschäftsbedingungen der Sparkasse.

(2) Der Kunde haftet für Schäden, die durch eine schuldhafte Verletzung der in Ziffer 3 genannten Sorgfaltspflichten entstehen.

(3) Insbesondere bei telefonischer Weitergabe der TAN an Dritte liegt in der Regel grobe Fahrlässigkeit im Sinne des § 675v Abs. 3 Nr. 2 BGB vor.

6. Änderungen der Sonderbedingungen

(1) Änderungen dieser Sonderbedingungen werden dem Kunden spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten.

(2) Die Zustimmung des Kunden gilt als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat.

7. Schlussbestimmungen

(1) Diese Sonderbedingungen ergänzen die Allgemeinen Geschäftsbedingungen der Sparkasse sowie die Bedingungen für das Online-Banking.

(2) Bei Widersprüchen zwischen diesen Sonderbedingungen und den Allgemeinen Geschäftsbedingungen gehen diese Sonderbedingungen vor.

(3) Stand: 1. Januar 2025.

Der Kunde bestätigt, die vorstehenden Sonderbedingungen erhalten und zur Kenntnis genommen zu haben.

Berlin, den 5. März 2024 (Umstellung auf pushTAN)

Peter Mayer

Sparkasse Berlin

PDF-Anhang: originale/05_Aktennotiz_Erstkontakt.pdf

Datei: 05_Aktennotiz_Erstkontakt.pdf

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

AKTENNOTIZ

Datum:	3. Juni 2025
Bearbeiter:	RA Dr. Marcus Brezelmann
Aktenzeichen:	2025-B-0478
Mandant:	Peter Mayer
Betreff:	Telefonischer Erstkontakt – Phishing-Schaden Sparkasse Berlin

Herr Peter Mayer (54 Jahre, Rechtsanwaltsfachangestellter bei Kollegen Dr. Schneider & Partner) rief heute um 14:30 Uhr in erheblicher Aufregung an.

Sachverhaltsschilderung des Mandanten:

Am 28. Mai 2025, gegen 11:15 Uhr, erhielt Herr Mayer einen Anruf auf seinem Mobiltelefon. Die angezeigte Nummer war ihm bekannt – es handelte sich scheinbar um die Servicenummer der Sparkasse Berlin (030-869869869). Der Anrufer stellte sich als „Thomas Bergmann vom Sicherheitsteam der Sparkasse Berlin" vor. Die Stimme klang professionell und vertrauenswürdig.

Der Anrufer teilte mit, dass auf dem Konto von Herrn Mayer (Girokonto Nr. XXXX-XXXX-42) verdächtige Aktivitäten festgestellt worden seien. Konkret seien mehrere Abbuchungsversuche aus dem Ausland registriert worden. Um das Konto zu schützen, müsse es vorübergehend gesperrt werden. Hierzu benötige man zur Verifizierung eine aktuelle TAN.

Herr Mayer generierte daraufhin über seine SparkassenApp eine TAN (pushTAN-Verfahren) mit der Anzeige „Freigabe für Sicherheitssperre". Diese TAN (487923) übermittelte er telefonisch. Der Anrufer bedankte sich höflich und versicherte, das Konto sei nun gesichert.

Innerhalb von weniger als 90 Sekunden nach Beendigung des Telefonats erhielt Herr Mayer Push-Nachrichten über folgende Transaktionen:

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

Gesamtschaden: 12,295.00 €

Kontosaldo nach Vorfall: -245,00 € (Dispositionscredit)

Herr Mayer kontaktierte umgehend die Sparkasse (28.5., 11:45 Uhr), Sperrnotruf wurde veranlasst. Strafanzeige bei der Polizei Berlin erfolgte am 29. Mai 2025 (Az. LKA 24/250529/0847).

Die Sparkasse lehnt bisher jegliche Schadensregulierung ab mit Verweis auf grobe Fahrlässigkeit bei TAN-Weitergabe.

Erste rechtliche Einschätzung:

Prüfung von Schadensersatzansprüchen aus § 675u BGB, § 280 Abs. 1 BGB i.V.m. Zahlungsdiensterahmenvertrag. Mitverschulden gem. § 254 BGB zu prüfen, aber Täuschungsintensität zu berücksichtigen (Spoofing der Telefonnummer, Social Engineering). Starke Argumente gegen grobe Fahrlässigkeit: professionelle Täuschung, gefälschte Rufnummer, irreführende TAN-Anzeige in der App. Neuere Rechtsprechung (LG Köln, Urt. v. 08.01.2024 – 15 O 267/23) tendiert bei solchen Fällen zugunsten der Kunden.

gez. RA Dr. Marcus Brezelmann

PDF-Anhang: originale/06_Email_Mayer_an_Sparkasse_280525.pdf

Datei: 06_Email_Mayer_an_Sparkasse_280525.pdf

E-MAIL-AUSDRUCK

Von: peter.mayer1971@gmail.com

An: service@sparkasse-berlin.de

Datum: 28. Mai 2025, 12:15 Uhr

Betreff: DRINGEND – Mein Konto wurde leergeräumt! Kontonummer XXXX-42

Sehr geehrte Damen und Herren,

ich bin seit über 20 Jahren Kunde bei Ihnen und mir ist gerade etwas Schreckliches passiert!

Vor einer Stunde hat mich jemand von Ihrer Sicherheitsabteilung angerufen (Herr Bergmann hieß er), die Nummer war auch Ihre normale Servicenummer. Er sagte, mein Konto müsste wegen verdächtiger Aktivitäten gesperrt werden und ich solle eine TAN durchgeben zur Bestätigung. Das habe ich gemacht – ich dachte ja, das ist wirklich die Sparkasse!

Keine zwei Minuten später war mein ganzes Konto leer! Über 12.000 Euro weg! Alles abgebucht, Lastschriften zurückgegeben, sogar Apple Pay wurde aktiviert und damit wurde in München eingekauft – ich war heute noch gar nicht in München, ich sitze hier in Berlin in meinem Büro!

Das kann doch nicht sein! Ihre Telefonnummer wurde angezeigt, wie soll ich denn wissen, dass das Betrüger sind? Ich habe sofort die Sperrhotline angerufen und meine Karten sperren lassen, aber das Geld ist schon weg.

Bitte kümmern Sie sich SOFORT darum! Ich brauche das Geld, die Miete wurde zurückgebucht, die Versicherungen auch, ich stehe jetzt im Minus!

Meine Kundennummer ist 478-239-561, das betroffene Konto ist das Girokonto mit der Endung -42.

Ich erwarte umgehend eine Rückmeldung!

Mit freundlichen Grüßen

Peter Mayer

P.S.: Ich habe auch schon versucht, in der Filiale anzurufen, aber da konnte mir niemand helfen und hat mich an die Hotline verwiesen. Das ist doch ein Alptraum!

PDF-Anhang: originale/07_Ablehnungsschreiben_Sparkasse_020625.p

Datei: 07_Ablehnungsschreiben_Sparkasse_020625.pdf

Abteilung Zahlungsverkehr/Schadensbearbeitung
Sachbearbeiter: Assessor jur. Thomas Krüger
Telefon: 030-869869-4421

Herrn
Peter Mayer
Lietzenburger Straße 74, 10719 Berlin

Ihr Zeichen: E-Mail vom 28.05.2025
Unser Zeichen: SB-2025/KR-44782
Kundennummer: 478-239-561
Datum: 2. Juni 2025

**Betreff: Ihre Schadensmeldung vom 28.05.2025; Girokonto IBAN DE89 1005 0000 0478 2395 42
hier: Ablehnung der Erstattungsansprüche**

Sehr geehrter Herr Mayer,

wir beziehen uns auf Ihre elektronische Mitteilung vom 28.05.2025 betreffend nicht autorisierte Zahlungsvorgänge auf vorbezeichnetem Zahlungskonto.

Nach eingehender Prüfung des Sachverhalts unter Berücksichtigung der technischen Protokolldaten sowie der einschlägigen rechtlichen Bestimmungen müssen wir Ihre Erstattungsansprüche zurückweisen.

I. Sachverhalt

Nach Ihrer Darstellung haben Sie am 28.05.2025 telefonisch eine mittels pushTAN-Verfahren generierte Transaktionsnummer an einen vermeintlichen Mitarbeiter unseres Hauses übermittelt. In der Folge wurden diverse Zahlungsvorgänge über Ihr Konto abgewickelt.

II. Rechtliche Würdigung

Gemäß § 675j Abs. 1 S. 1 BGB ist für die Autorisierung eines Zahlungsvorgangs erforderlich, dass der Zahler gegenüber dem Zahlungsdienstleister die Zustimmung zur Ausführung erteilt. Diese Zustimmung erfolgt im Rahmen des zwischen Ihnen und unserem Haus vereinbarten pushTAN-Verfahrens durch Eingabe der generierten TAN.

Die streitgegenständlichen Zahlungsvorgänge wurden ordnungsgemäß unter Verwendung einer gültigen, von Ihrem registrierten Endgerät generierten TAN autorisiert. Die technische Authentifizierung erfolgte korrekt gemäß Art. 4 Nr. 30 i.V.m. Art. 97 der Richtlinie (EU) 2015/2366 (PSD2) unter Anwendung der starken Kundenauthentifizierung.

Nach § 675v Abs. 2 BGB trifft den Zahler die Haftung für nicht autorisierte Zahlungsvorgänge in voller Höhe, wenn er diese durch vorsätzliches oder grob fahrlässiges Verhalten ermöglicht hat. Insbesondere liegt grobe Fahrlässigkeit vor bei Verletzung der Pflichten aus § 675l BGB i.V.m. Ziffer 11.1 unserer Allgemeinen Geschäftsbedingungen sowie Ziffer 3.2 der Sonderbedingungen für das pushTAN-Verfahren.

Die Weitergabe einer TAN an Dritte stellt eine evidente Verletzung der Sorgfaltspflichten dar. In Ziffer 3.2 der Sonderbedingungen heißt es ausdrücklich: „Der Kunde darf die TAN keinem Dritten mitteilen

oder sonst zugänglich machen.“ Ferner wurden Sie mehrfach, zuletzt mit Schreiben vom 15.01.2025, über aktuelle Phishing-Methoden informiert mit dem ausdrücklichen Hinweis, dass Mitarbeiter der Sparkasse niemals telefonisch nach TANs fragen.

Der Bundesgerichtshof hat in ständiger Rechtsprechung (vgl. BGH, Urt. v. 26.01.2016 – XI ZR 91/14; Urt. v. 29.11.2016 – XI ZR 429/15) judiziert, dass die Preisgabe von Authentifizierungselementen regelmäßig als grob fahrlässig zu qualifizieren ist.

III. Ergebnis

Eine Erstattungspflicht unsererseits gemäß § 675u BGB scheidet aus. Sie haben durch die Weitergabe der TAN grob fahrlässig gehandelt und tragen daher den entstandenen Schaden in vollem Umfang selbst (§ 675v Abs. 2 BGB).

Ergänzend weisen wir darauf hin, dass die Rückbuchung der autorisierten Lastschriften aufgrund Kontoüberziehung nach § 675x Abs. 2 BGB erfolgte und insoweit rechtmäßig war.

Mit freundlichen Grüßen

Sparkasse Berlin

i.A. Assessor jur. Thomas Krüger
Abteilung Zahlungsverkehr

i.V. Sabine Hoffmann
Prokuristin · Leiterin Schadensbearbeitung

Hinweis: Gegen diese Entscheidung können Sie binnen 4 Wochen ab Zugang Beschwerde beim Ombudsmann des Deutschen Sparkassen- und Giroverbandes einlegen.

PDF-Anhang: originale/08_Email_Mayer_an_Sparkasse_030625.pdf

Datei: 08_Email_Mayer_an_Sparkasse_030625.pdf

E-MAIL-AUSDRUCK

Von: peter.mayer1971@gmail.com

An: service@sparkasse-berlin.de; thomas.krueger@sparkasse-berlin.de

Datum: 3. Juni 2025, 09:45 Uhr

Betreff: Re: Ihr Schreiben SB-2025/KR-44782 – Das kann doch nicht Ihr Ernst sein!

Sehr geehrter Herr Krüger, sehr geehrte Frau Hoffmann,

ich habe Ihr Schreiben vom 2. Juni erhalten und bin ehrlich gesagt fassungslos!

Grob fahrlässig soll ich gehandelt haben? Die haben IHRE Telefonnummer angezeigt! Woher soll ich denn wissen, dass man Telefonnummern fälschen kann? Ich bin Rechtsanwaltsfachangestellter, kein IT-Experte!

Sie schreiben, ich hätte Ihre Warnungen ignoriert – ja, ich bekomme jeden Monat fünf Briefe von Ihnen mit irgendwelcher Werbung, wer soll das alles lesen? Und wenn wirklich Ihre Nummer auf meinem Display steht, dann denke ich doch, dass Sie das sind!

Der Anrufer wusste meinen Namen, meine Kontonummer (die letzten Ziffern jedenfalls) und hat sehr professionell geklungen. Er hat gesagt, es gäbe verdächtige Abbuchungen aus Rumänien und er müsste das Konto SOFORT sperren, damit kein größerer Schaden entsteht. Was hätte ich denn machen sollen?

Außerdem: In der pushTAN-App stand „Freigabe für Sicherheitssperre“ – das klang doch genau nach dem, was der Mann am Telefon gesagt hat! Da stand nichts von einer Überweisung!

12.000 Euro sind für mich sehr viel Geld! Ich arbeite seit 25 Jahren hart für mein Geld und bin seit über 20 Jahren treuer Kunde bei Ihnen. Ist das wirklich Ihre Art, mit langjährigen Kunden umzugehen?

Ich bitte Sie dringend, die Sache nochmal zu prüfen. Das kann doch nicht sein, dass ich auf allem sitzen bleibe, nur weil Kriminelle immer raffinierter werden!

Mit freundlichen Grüßen

Peter Mayer

P.S.: Ich werde mir anwaltlichen Rat einholen. Das lasse ich so nicht auf mir sitzen!

PDF-Anhang: originale/09_Zweites_Ablehnungsschreiben_Sparkasse_

Datei: 09_Zweites_Ablehnungsschreiben_Sparkasse_050625.pdf

Abteilung Zahlungsverkehr/Schadensbearbeitung
Direktor Dr. jur. Friedrich Steinberg
Telefon: 030-869869-4001

Herrn
Peter Mayer
Lietzenburger Straße 74, 10719 Berlin

Ihr Zeichen: E-Mail vom 03.06.2025
Unser Zeichen: SB-2025/ST-44782-2
Kundennummer: 478-239-561
Datum: 5. Juni 2025

Betreff: Ihre Beschwerde vom 03.06.2025; Bestätigung der Ablehnung

Bezug: Unser Schreiben vom 2. Juni 2025, Az. SB-2025/KR-44782

Sehr geehrter Herr Mayer,

Ihre erneute Eingabe vom 03.06.2025 wurde mir zur abschließenden Entscheidung vorgelegt. Nach nochmaliger eingehender Prüfung unter Würdigung Ihrer ergänzenden Ausführungen muss ich die Entscheidung meiner Fachabteilung vollumfänglich bestätigen.

I. Ergänzende Feststellungen zum Sachverhalt

Die forensische Analyse der Systemprotokolle ergab folgende Erkenntnisse:

- Die TAN-Generierung erfolgte am 28.05.2025 um 11:16:42 Uhr über Ihr registriertes Mobilgerät (iPhone 13, Geräte-ID bei uns hinterlegt).
- Der in der pushTAN-App angezeigte Text lautete vollständig: „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“. Dieser Text wird systemseitig bei Sammelaufträgen generiert.
- Die TAN wurde um 11:17:14 Uhr im Online-Banking-System eingegeben, IP-Adresse 185.220.XXX.XXX (Tor-Exit-Node).

II. Rechtliche Bewertung unter Berücksichtigung Ihrer Einwände

Zur behaupteten Unkenntnis über Call-ID-Spoofing:

Die Möglichkeit der Rufnummernmanipulation ist spätestens seit dem Inkrafttreten des § 66k TKG allgemein bekannt. Der BGH (Urt. v. 19.03.2019 – XI ZR 355/18) hat ausgeführt, dass von einem durchschnittlichen Bankkunden im digitalen Zahlungsverkehr ein Mindestmaß an Sensibilisierung für Betrugsmaschen erwartet werden kann. Ihre berufliche Tätigkeit im Rechtsbereich lässt sogar ein überdurchschnittliches Problembewusstsein erwarten.

Zur Informationspflicht:

Gemäß § 675d Abs. 1 BGB i.V.m. Art. 248 §§ 1-16 EGBGB haben wir unseren Informationspflichten vollumfänglich genügt. Die quartalsweisen Sicherheitshinweise (nachweislich zugestellt am 15.01.2025, 15.10.2024, 15.07.2024 und 15.04.2024) enthielten jeweils den prägnanten Warnhinweis: „Die Sparkasse wird Sie niemals telefonisch, per E-Mail oder SMS zur Eingabe von TANs, PINs oder

Passwörtern auffordern.“

Zum Vertrauenstatbestand:

Das OLG Frankfurt (Urt. v. 27.02.2020 – 17 U 42/19) hat klargestellt, dass allein die Anzeige einer bekannten Rufnummer keinen schützenswerten Vertrauenstatbestand begründet, wenn elementare Sicherheitsregeln missachtet werden. Die telefonische Weitergabe einer TAN stellt eine solche elementare Pflichtverletzung dar.

Zur Täuschungshandlung:

Zwar erkennen wir an, dass Sie Opfer einer elaborierten Täuschung wurden. Jedoch hat das OLG München (Urt. v. 14.01.2021 – 17 U 3651/20) judiziert, dass selbst bei sophistizierten Social-Engineering-Attacken die grobe Fahrlässigkeit nicht entfällt, wenn – wie hier – gegen eindeutige, mehrfach kommunizierte Sicherheitsanweisungen verstoßen wird.

Zur Formulierung in der pushTAN-App:

Der vollständige Text „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“ hätte bei pflichtgemäßer Sorgfalt (§ 276 Abs. 2 BGB) Anlass zu erhöhter Vorsicht geben müssen. Der Zusatz „Transaktionsfreigabe“ ist eindeutig.

III. Abschließende Bewertung

Die Haftungsverteilung des § 675v BGB folgt dem Prinzip der Risikosphären. Die Geheimhaltung der Authentifizierungselemente liegt in Ihrer alleinigen Risikosphäre. Durch die Preisgabe der TAN haben Sie die Ihnen obliegende Sorgfaltspflicht in einem Maße verletzt, das deutlich unter dem Verhalten eines durchschnittlich sorgfältigen Bankkunden liegt.

Eine Erstattungspflicht nach § 675u BGB scheidet daher definitiv aus. Auch Ansprüche aus § 280 Abs. 1 BGB wegen Verletzung von Schutzpflichten sind nicht gegeben, da unser Sicherheitssystem ordnungsgemäß funktioniert hat und die Transaktion technisch korrekt autorisiert wurde.

IV. Hinweise

Wir bedauern aufrichtig, dass Sie Opfer einer Straftat wurden, und haben den Sachverhalt unsererseits gemäß § 11 GwG an die Zentralstelle für Verdachtsmeldungen gemeldet.

Sie haben die Möglichkeit, binnen 4 Wochen ab Zugang dieses Schreibens ein Schlichtungsverfahren beim Ombudsmann der deutschen Sparkassen einzuleiten (www.dsgv.de/schlichtungsstelle).

Unabhängig davon können Sie zivilrechtliche Ansprüche gegen die derzeit unbekannten Täter geltend machen. Die Staatsanwaltschaft Berlin führt nach unserer Kenntnis entsprechende Ermittlungen.

Diese Entscheidung ist innerhalb unseres Hauses abschließend.

Mit freundlichen Grüßen

Sparkasse Berlin

Dr. jur. Friedrich Steinberg
Direktor · Leiter Recht und Compliance

Anlagen:

- Technisches Protokoll TAN-Verwendung (anonymisiert)
- Auszug Sonderbedingungen pushTAN-Verfahren
- Kopie Sicherheitshinweis vom 15.01.2025

PDF-Anhang: originale/10_Email_Mayer_an_Freund_290525.pdf

Datei: 10_Email_Mayer_an_Freund_290525.pdf

E-MAIL-AUSDRUCK

Von: peter.mayer1971@gmail.com
An: juergen.roth82@web.de
Datum: 29. Mai 2025, 22:17 Uhr
Betreff: Du wirst nicht glauben was mir passiert ist...

Hallo Jürgen,

ich muss dir was erzählen, mir ist gestern was Unfassbares passiert. Ich sitze immer noch total unter Schock.

Gestern Vormittag, so gegen Viertel nach elf, klingelt mein Handy. Auf dem Display steht die Nummer von der Sparkasse – du weißt ja, ich bin da schon ewig Kunde. Der Typ am Telefon stellt sich als Thomas Bergmann vor, Sicherheitsteam Sparkasse Berlin. Klang total seriös, professionell, keine Hintergrundgeräusche oder so.

Er sagt, auf meinem Konto wären verdächtige Aktivitäten festgestellt worden, irgendwelche Abbuchungsversuche aus Rumänien. Das Konto müsste sofort gesperrt werden, damit kein größerer Schaden entsteht. Dafür bräuchte er eine TAN von mir zur Verifizierung. Ich dachte natürlich: Okay, die Sparkasse ruft an, auf dem Display steht die richtige Nummer, der kennt meinen Namen und meine Kontonummer – das muss echt sein.

Also hab ich die App aufgemacht und eine TAN generiert. In der App stand auch was von „Sicherheitssperre“ – passte ja genau zu dem, was er gesagt hat. Die TAN hab ich ihm dann durchgegeben.

Jürgen, nicht mal zwei Minuten später kriege ich Push-Nachrichten auf mein Handy: 4.500 Euro überwiesen, 3.200 Euro überwiesen, Lastschriften zurückgebucht, Apple Pay aktiviert – und dann noch Einkäufe in München und Stuttgart! Ich war die ganze Zeit hier in Berlin im Büro!

Insgesamt sind über 12.000 Euro weg. ZWÖLFTAUSEND! Mein komplettes Konto ist leer, ich bin sogar im Minus. Die Miete wurde zurückgebucht, die Versicherungen auch. Ich hab sofort bei der Sparkasse angerufen und alles sperren lassen, aber das Geld war schon weg.

Heute war ich bei der Polizei, Anzeige erstattet. Die meinten, das wäre „Call-ID-Spoofing“, da kann man wohl Telefonnummern fälschen. Hab ich vorher noch nie von gehört! Hast du davon mal gehört? Ich fühl mich so dumm...

Die Sparkasse will natürlich nichts erstatten, die sagen, ich wäre selbst schuld. Aber woher soll ich denn wissen, dass das nicht wirklich die Sparkasse war? Deren eigene Nummer stand auf meinem Handy!

Ich überleg jetzt, mir einen Anwalt zu nehmen. So kann das doch nicht laufen. Was meinst du?

Ruf mich mal an, wenn du Zeit hast. Brauch jemanden zum Reden.

Grüße

Peter

Von: juergen.roth82@web.de
An: peter.mayer1971@gmail.com
Datum: 30. Mai 2025, 08:42 Uhr
Betreff: Re: Du wirst nicht glauben was mir passiert ist...

Alter Peter,

das ist ja der absolute Hammer! 12.000 Euro – das ist doch fast dein ganzes Ersparnis?! Das tut mir so leid für dich.

Ich hab tatsächlich mal was über dieses Nummer-Fälschen gelesen, das war vor ein paar Monaten in der Tagesschau. Die Betrüger werden immer dreister. Aber ehrlich: Wenn auf meinem Handy die Sparkassen-Nummer angezeigt wird, würde ich auch denken, dass die das wirklich sind. Das ist doch kein Fehler von dir!

Auf jeden Fall Anwalt nehmen! Da gibt es doch Fachanwälte für Bankrecht. Mein Kollege Stefan hatte mal was Ähnliches mit seiner Volksbank, der hat sich an so eine spezialisierte Kanzlei gewandt und am Ende fast alles zurückbekommen.

Ruf mich heute Abend an, dann können wir in Ruhe reden. Kopf hoch!

Jürgen

PDF-Anhang: originale/11_Screenshots_Phishing.pdf

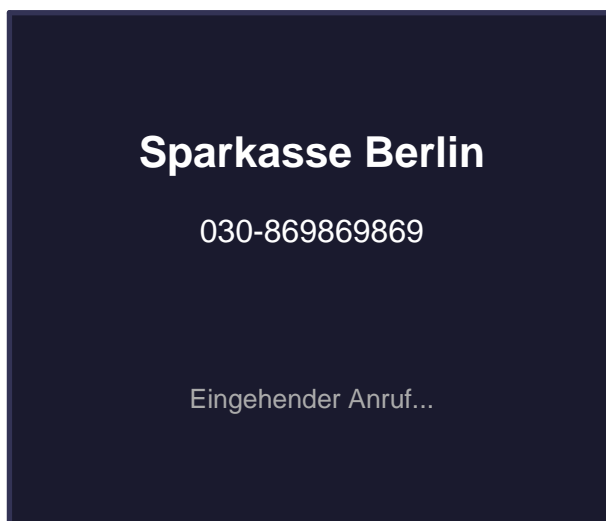
Datei: 11_Screenshots_Phishing.pdf

SCREENSHOTS / BILDSCHIRMFOTOS

zum Phishing-Vorfall vom 28. Mai 2025
Mandant: Peter Mayer · Az.: 2025-B-0478

Screenshot 1: Eingehender Anruf – Displayanzeige

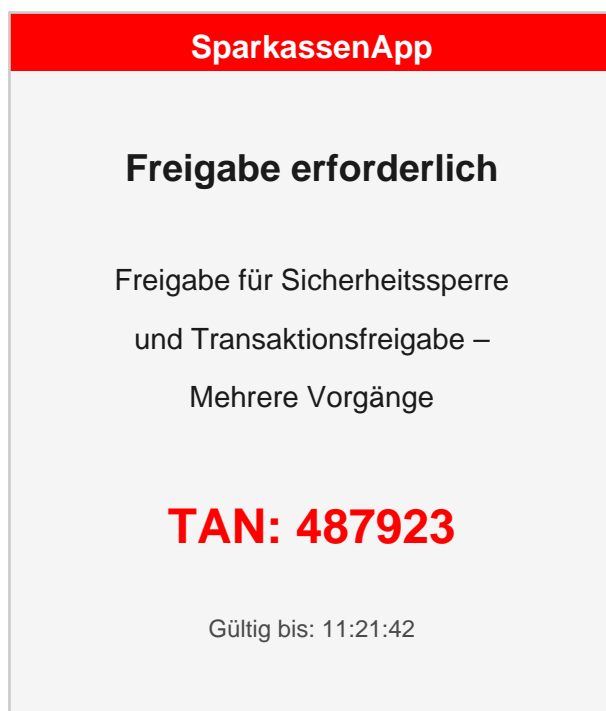
Aufgenommen am 28.05.2025, ca. 11:15 Uhr (rekonstruiert aus Anrufliste)



Anmerkung: Die angezeigte Rufnummer entspricht der offiziellen Servicenummer der Sparkasse Berlin. Die Täter verwendeten sog. Call-ID-Spoofing.

Screenshot 2: pushTAN-App – Freigabeanzeige

Aufgenommen am 28.05.2025, 11:16 Uhr (rekonstruiert)



Anmerkung: Die Formulierung „Freigabe für Sicherheitssperre“ ist irreführend. Der Zusatz „und Transaktionsfreigabe – Mehrere Vorgänge“ ist auf dem Mobilgerät leicht zu übersehen.

Screenshot 3: Push-Benachrichtigungen nach TAN-Eingabe

Aufgenommen am 28.05.2025, ab 11:18 Uhr

Uhrzeit	Absender	Benachrichtigung
11:17:22	Sparkasse Berlin	Überweisung 4.500,00 € an Digital Services GmbH ausgeführt
11:17:24	Sparkasse Berlin	Überweisung 3.200,00 € an TechPay Solutions ausgeführt
11:17:31	Sparkasse Berlin	Lastschrift Miete 1.850,00 € zurückgegeben – Deckung fehlt
11:17:33	Sparkasse Berlin	Lastschriften Versicherungen 645,00 € zurückgegeben
11:17:45	Apple Wallet	Neue Karte zu Apple Pay hinzugefügt: Sparkassen-Card ****42
11:18:02	Apple Pay	Zahlung 849,00 € bei MediaMarkt München genehmigt
11:18:15	Apple Pay	Zahlung 599,00 € bei Saturn Stuttgart genehmigt
11:18:28	Apple Pay	Zahlung 652,00 € bei Expert München genehmigt

Anmerkung: Sämtliche betrügerischen Transaktionen wurden innerhalb von ca. 70 Sekunden nach TAN-Eingabe durchgeführt (automatisiertes Angriffsskript).

Screenshot 4: Anrufliste des Mobiltelefons

Exportiert am 29.05.2025

Datum/Uhrzeit	Nummer	Richtung	Dauer
28.05.2025 11:15	030-869869869	Eingehend	1 Min 48 Sek
28.05.2025 11:45	116 116 (Sperr-Notruf)	Ausgehend	4 Min 12 Sek
28.05.2025 11:52	030-869869869	Ausgehend	12 Min 34 Sek
28.05.2025 14:30	+49 30 889 23 400	Ausgehend	22 Min 07 Sek

Der eingehende Anruf um 11:15 Uhr zeigt die Sparkassen-Servicenummer an. Der Sperr-Notruf um 11:45 Uhr belegt die unverzügliche Reaktion.

PDF-Anhang: originale/12_Internes_Rechtsgutachten_Sparkasse.pdf

Datei: 12_Internes_Rechtsgutachten_Sparkasse.pdf

INTERNES RECHTSGUTACHTEN

— VERTRAULICH — NUR FÜR DEN INTERNEN DIENSTGEBRAUCH —

Aktenzeichen:	SB-2025/KR-44782 / Gutachten-Nr. RG-2025/0612
Erstellt von:	Abt. Recht und Compliance
Verfasser:	Dr. jur. Friedrich Steinberg
Mitwirkung:	Assessor jur. Thomas Krüger
Datum:	1. Juni 2025
Gegenstand:	Schadensfall Peter Mayer – Phishing/Social Engineering
Schadenshöhe:	12,295.00 €

A. Sachverhalt

Am 28. Mai 2025 gegen 11:15 Uhr wurde der Kunde Peter Mayer (Kundennummer: 478-239-561) Opfer eines Phishing-Angriffs mittels Call-ID-Spoofing und Social Engineering. Der Angreifer gab sich als Mitarbeiter „Thomas Bergmann“ des Sicherheitsteams der Sparkasse Berlin aus und verwendete die manipulierte Rufnummer 030-869869869.

Der Kunde generierte auf Aufforderung eine TAN über das pushTAN-Verfahren und teilte diese telefonisch mit. Die TAN wurde anschließend zur Autorisierung mehrerer betrügerischer Zahlungsvorgänge verwendet.

Technische Feststellungen:

- TAN-Generierung: 28.05.2025, 11:16:42 Uhr, Gerät: iPhone 13 (registriertes Endgerät)
- TAN-Eingabe: 28.05.2025, 11:17:14 Uhr, IP: 185.220.XXX.XXX (Tor-Exit-Node, NL)
- App-Anzeige: „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“
- Transaktionen: 2 Überweisungen, 2 Lastschriftrückgaben, Apple Pay-Aktivierung, 3 Apple Pay-Käufe
- Gesamtschaden: 12.295,00 €
- Sperranzeige des Kunden: 28.05.2025, 11:45 Uhr (ca. 28 Minuten nach TAN-Eingabe)

B. Fragestellung

Zu prüfen ist, ob die Sparkasse Berlin dem Kunden gemäß § 675u BGB zur Erstattung des Schadens verpflichtet ist oder ob dem Kunden grobe Fahrlässigkeit im Sinne des § 675v Abs. 3 Nr. 2 BGB zur Last fällt.

C. Rechtliche Würdigung

I. Nicht autorisierter Zahlungsvorgang (§ 675u BGB)

Ein Zahlungsvorgang ist autorisiert, wenn der Zahler dem Zahlungsvorgang zugestimmt hat (§ 675j Abs. 1 S. 1 BGB). Die TAN wurde zwar auf dem Endgerät des Kunden generiert, jedoch durch einen

Dritten in das Online-Banking-System eingegeben (IP-Adresse: Tor-Exit-Node).

Ergebnis: Die Zahlungsvorgänge sind **nicht autorisiert** im Sinne des § 675j BGB. Der Kunde hat den Zahlungen nicht zugestimmt; er wollte eine „Sicherheitssperre“ veranlassen, nicht Überweisungen tätigen. Die grundsätzliche Erstattungspflicht nach § 675u Abs. 2 BGB ist gegeben.

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

Die Erstattungspflicht entfällt, wenn der Zahler den Schaden durch grob fahrlässige Verletzung seiner Sorgfaltspflichten herbeigeführt hat. Grobe Fahrlässigkeit liegt vor, wenn die im Verkehr erforderliche Sorgfalt in besonders schwerem Maße verletzt wird (BGH, Urt. v. 26.01.2016 – XI ZR 91/14, Rn. 72).

1. Für grobe Fahrlässigkeit sprechende Umstände:

a) **Telefonische TAN-Weitergabe:** Die Weitergabe einer TAN an Dritte stellt eine zentrale Verletzung der Sorgfaltspflichten aus § 675l BGB und Ziffer 3.2 der Sonderbedingungen pushTAN dar. Die Rechtsprechung wertet dies regelmäßig als grob fahrlässig (BGH, Urt. v. 26.01.2016 – XI ZR 91/14; OLG München, Urt. v. 14.01.2021 – 17 U 3651/20).

b) **Mehrfache Warnhinweise:** Der Kunde wurde quartalsweise über Phishing-Gefahren informiert, zuletzt am 15.01.2025.

c) **App-Anzeige:** Der vollständige Anzeigetext enthielt den Zusatz „Transaktionsfreigabe – Mehrere Vorgänge“, der bei sorgfältiger Lektüre hätte auffallen müssen.

d) **Berufliche Vorbildung:** Der Kunde ist als Rechtsanwaltsfachangestellter beruflich mit rechtlichen Vorgängen befasst.

2. Gegen grobe Fahrlässigkeit sprechende Umstände:

[Anmerkung: Folgende Gegenargumente werden bei gerichtlicher Auseinandersetzung voraussichtlich vorgebracht:]

a) **Hohe Täuschungsintensität:** Call-ID-Spoofing ist eine technisch anspruchsvolle Methode. Das LG Köln (Urt. v. 08.01.2024 – 15 O 267/23) hat in einem vergleichbaren Fall die grobe Fahrlässigkeit verneint.

b) **Irreführende App-Anzeige:** Die primäre Anzeige „Freigabe für Sicherheitssperre“ korrespondierte mit der Erklärung des Anrufers. Die Sparkasse könnte eine Mitverantwortung für die unklare Formulierung tragen.

c) **Drucksituation:** Der Anrufer erzeugte eine akute Drucksituation. Das AG München (Urt. v. 05.12.2023 – 132 C 49/23) hat in solchen Fällen die Schwelle zur groben Fahrlässigkeit erhöht.

d) **Beweislast:** Die Beweislast für grobe Fahrlässigkeit liegt gemäß § 675v Abs. 4 BGB beim Zahlungsdienstleister (BGH, Urt. v. 26.01.2016 – XI ZR 91/14, Rn. 75).

III. Eigene Pflichtverletzung der Sparkasse

a) **Transaktionsüberwachung:** Das TMS hat die ungewöhnlichen Transaktionen nicht rechtzeitig identifiziert. Zwei Überweisungen in Höhe von insgesamt 7.700 € an bisher nicht bekannte Empfänger sowie eine Apple-Pay-Aktivierung aus einer TOR-IP-Adresse hätten Anomalien auslösen müssen.

b) **App-Gestaltung:** Die Formulierung „Freigabe für Sicherheitssperre“ ist objektiv irreführend. Eine klarere Bezeichnung (z.B. „Überweisung an Digital Services GmbH: 4.500,00 €“) wäre technisch möglich und nach Art. 97 Abs. 2 PSD2 geschuldet gewesen.

D. Risikoeinschätzung für den Rechtsstreit

Prozessrisiko: MITTEL BIS HOCH

Die Rechtslage ist nicht eindeutig. Während die ältere Rechtsprechung tendenziell zugunsten der Institute entschied, zeigt die neuere Rechtsprechung der Instanzgerichte eine zunehmende Sensibilisierung für die Raffinesse moderner Phishing-Methoden. Insbesondere die unklare App-Anzeige und die fehlende Anomalie-Erkennung könnten dem Gericht Anlass geben, die grobe Fahrlässigkeit zu verneinen oder zumindest ein Mitverschulden der Sparkasse anzunehmen.

Empfehlung: Ablehnung der Erstattung aufrechterhalten, um keine Präzedenzwirkung zu entfalten. Im Falle einer Klage Vergleichsbereitschaft auf Basis 50-70 % prüfen.

E. Ergebnis und Empfehlung

1. Der Phishing-Angriff ist als authentischer Betrugsfall zu werten.
2. Ablehnung der Erstattung auf Vorwurf der groben Fahrlässigkeit vertretbar, birgt aber erhebliche Prozessrisiken.
3. Interne Schwachstellen (App-Formulierung, TMS-Reaktionszeit) sind der Gegenseite nicht offenzulegen, aber im Prozessrisiko einzupreisen.
4. Empfehlung: Außergerichtliche Erstattung ablehnen. Bei Klageerhebung: Vergleichsbereitschaft auf Basis 50-70 % signalisieren.

Dr. jur. Friedrich Steinberg
Direktor · Leiter Recht und Compliance

— Dieses Dokument ist vertraulich und ausschließlich für den internen Dienstgebrauch bestimmt. —

PDF-Anhang: originale/13_Anwaltsschreiben_an_Sparkasse_100625.pdf

Datei: 13_Anwaltsschreiben_an_Sparkasse_100625.pdf

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

Sparkasse Berlin
Abteilung Zahlungsverkehr/Schadensbearbeitung
Alexanderplatz 2, 10178 Berlin

Ihr Zeichen: SB-2025/KR-44782

Unser Zeichen: 2025-B-0478

Sachbearbeiter: RA Dr. Marcus Brezelmann

Datum: 10. Juni 2025

Betreff: Nicht autorisierte Zahlungsvorgänge vom 28. Mai 2025; Girokonto IBAN DE89 1005 0000 0478 2395 42

hier: Aufforderung zur Erstattung gemäß § 675u BGB

In Sachen: Peter Mayer ./ Sparkasse Berlin

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit zeigen wir an, dass uns Herr Peter Mayer, wohnhaft Lietzenburger Straße 74, 10719 Berlin, mit der Wahrnehmung seiner rechtlichen Interessen beauftragt hat. Ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Namens und in Vollmacht unseres Mandanten fordern wir Sie hiermit auf, den durch nicht autorisierte Zahlungsvorgänge vom 28. Mai 2025 entstandenen Schaden in Höhe von

12.295,00 € (in Worten: zwölftausendzweihundertfünfundneunzig Euro)

zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 28. Mai 2025 (§§ 288 Abs. 1, 291 BGB) binnen

14 Tagen ab Zugang dieses Schreibens

auf das Konto unseres Mandanten, IBAN DE89 1005 0000 0478 2395 42, zu erstatten.

I. Sachverhalt

Am 28. Mai 2025 gegen 11:15 Uhr erhielt unser Mandant einen Telefonanruf. Auf seinem Mobiltelefon wurde die offizielle Servicenummer Ihres Hauses (030-869869869) angezeigt. Der Anrufer stellte sich als Mitarbeiter des Sicherheitsteams der Sparkasse Berlin vor und behauptete, es seien verdächtige Abbuchungsversuche aus Rumänien festgestellt worden. Das Konto müsse dringend gesperrt werden.

Der Anrufer kannte den Namen unseres Mandanten sowie Teile seiner Kontodaten und erzeugte eine akute psychologische Drucksituation. Die in der pushTAN-App angezeigte Bezeichnung lautete „Freigabe für Sicherheitssperre“ – eine Formulierung, die exakt der Behauptung des Anrufers entsprach. Unser Mandant generierte daraufhin eine TAN und teilte diese dem Anrufer mit.

In der Folge wurden innerhalb weniger Minuten mehrere betrügerische Transaktionen durchgeführt, deren Gesamtschaden sich auf 12.295,00 € beläuft. Unser Mandant hat unverzüglich den Sperr-Notruf 116 116 kontaktiert und Strafanzeige beim LKA Berlin erstattet (Az.: LKA 24/250529/0847).

II. Rechtliche Würdigung

1. Nicht autorisierte Zahlungsvorgänge (§ 675j BGB)

Die streitgegenständlichen Zahlungsvorgänge sind nicht autorisiert im Sinne des § 675j Abs. 1 S. 1 BGB. Unser Mandant hat zu keinem Zeitpunkt die Zustimmung zur Ausführung von Überweisungen oder zur Aktivierung von Apple Pay erteilt. Er wollte ausschließlich eine „Sicherheitssperre“ seines Kontos veranlassen. Ein Autorisierungswille lag nicht vor. Die TAN wurde vielmehr durch arglistige Täuschung erschlichen.

Ihr Haus ist daher gemäß § 675u Abs. 2 BGB verpflichtet, das Zahlungskonto unseres Mandanten in den Zustand zu versetzen, in dem es sich ohne die nicht autorisierten Zahlungsvorgänge befunden hätte.

2. Keine grobe Fahrlässigkeit (§ 675v Abs. 3 Nr. 2 BGB)

Der Einwand grober Fahrlässigkeit greift im vorliegenden Fall nicht durch:

a) Hohe Täuschungsintensität durch Call-ID-Spoofing: Die Täter verwendeten eine technisch anspruchsvolle Methode zur Manipulation der Rufnummernanzeige. Die Anzeige der offiziellen Sparkassen-Servicenummer auf dem Display unseres Mandanten begründete ein berechtigtes Vertrauen in die Identität des Anrufers. Das LG Köln hat in seinem Urteil vom 08.01.2024 (Az. 15 O 267/23) in einem vergleichbaren Fall die grobe Fahrlässigkeit verneint, da Call-ID-Spoofing für den durchschnittlichen Verbraucher nicht erkennbar ist.

b) Irreführende Anzeige in der pushTAN-App: Die primäre Anzeige „Freigabe für Sicherheitssperre“ korrespondierte exakt mit der vom Anrufer 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.

c) Psychologische Drucksituation: Der Anrufer erzeugte bewusst eine akute Stresssituation durch die Behauptung, es drohten unmittelbar weitere Schäden. Unter solchen Umständen ist die Schwelle zur groben Fahrlässigkeit erhöht (vgl. AG München, Urt. v. 05.12.2023 – 132 C 49/23).

d) Kenntnis persönlicher Daten: Der Anrufer verfügte über den Namen und Kontodaten unseres Mandanten. Dies verstärkte den Anschein der Legitimation erheblich.

3. Pflichtverletzungen Ihres Hauses

a) Unzureichende Transaktionsüberwachung: Zwei Überweisungen in Höhe von insgesamt 7.700,00 € an bisher unbekannte Empfänger, eine Apple-Pay-Aktivierung von einer Tor-Exit-Node-IP-Adresse sowie drei kontaktlose Zahlungen in München und Stuttgart – während der Kontoinhaber in Berlin ansässig ist – hätten im Transaktionsmonitoring Anomalien auslösen müssen. Eine Echtzeitintervention unterblieb.

b) Irreführende App-Gestaltung: Die Formulierung in der pushTAN-App ist geeignet, Nutzer über den wahren Charakter der freigegebenen Transaktion in die Irre zu führen. Nach Art. 97 Abs. 2 der Zahlungsdiensterichtlinie (PSD2) ist der Zahlungsdienstleister verpflichtet, dem Nutzer eindeutige Transaktionsinformationen anzuzeigen. Eine Anzeige wie „Überweisung an Digital Services GmbH: 4.500,00 €“ wäre technisch möglich und rechtlich geschuldet gewesen.

III. Fristsetzung und weitere Maßnahmen

Wir fordern Sie letztmalig auf, den Betrag von **12.295,00 €** nebst Zinsen binnen **14 Tagen** ab Zugang dieses Schreibens zu erstatten.

Sollte eine fristgerechte Zahlung nicht erfolgen, werden wir – ohne weitere Ankündigung – zunächst ein Schlichtungsverfahren beim Ombudsmann der deutschen Sparkassen (Kundenbeschwerdestelle beim DSGVO) einleiten und sodann gerichtliche Schritte ergreifen.

Die Kosten der anwaltlichen Inanspruchnahme in Höhe einer 1,3-Geschäftsgebühr gemäß Nr. 2300 VV RVG zuzüglich Auslagenpauschale und Umsatzsteuer werden wir Ihnen gesondert in Rechnung stellen.

Mit freundlichen Grüßen

RA Dr. Marcus Brezelmann
Fachanwalt für Bank- und Kapitalmarktrecht

Anlagen:

- Vollmacht (Kopie)
- Strafanzeige LKA Berlin, Az.: LKA 24/250529/0847
- Screenshots Phishing-Vorfall
- Kontoauszüge

PDF-Anhang: originale/14_Antwort_Sparkasse_auf_Anwalt_200625.pdf

Datei: 14_Antwort_Sparkasse_auf_Anwalt_200625.pdf

Abteilung Recht und Compliance
Direktor Dr. jur. Friedrich Steinberg
Telefon: 030-869869-4001

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

Ihr Zeichen: 2025-B-0478
Unser Zeichen: SB-2025/ST-44782-2
Kundennummer: 478-239-561
Datum: 20. Juni 2025

Betreff: Ihr Schreiben vom 10. Juni 2025; Schadensfall Peter Mayer

hier: Zurückweisung der Erstattungsforderung

Sehr geehrter Herr Dr. Brezelmann,

wir bestätigen den Eingang Ihres Schreibens vom 10. Juni 2025 und nehmen hierzu wie folgt Stellung:

I. Zur Autorisierung

Die streitgegenständlichen Zahlungsvorgänge wurden unter Verwendung einer gültigen, vom registrierten Endgerät Ihres Mandanten generierten TAN autorisiert. Die technische Authentifizierung mittels starker Kundenauthentifizierung (Art. 97 PSD2) war ordnungsgemäß. Der Umstand, dass die TAN aufgrund einer Täuschungshandlung eines Dritten preisgegeben wurde, beseitigt nicht die technisch korrekte Autorisierung.

II. Grobe Fahrlässigkeit Ihres Mandanten

Ihr Mandant hat gegen seine vertraglichen und gesetzlichen Sorgfaltspflichten in grob fahrlässiger Weise verstoßen:

- a)** Die telefonische Weitergabe einer TAN an Dritte stellt nach ständiger Rechtsprechung des Bundesgerichtshofs eine grobe Fahrlässigkeit dar (BGH, Urt. v. 26.01.2016 – XI ZR 91/14, Rn. 72 ff.; BGH, Urt. v. 29.11.2016 – XI ZR 429/15). An dieser Beurteilung ändert auch das Vorliegen einer sophistizierten Täuschungshandlung grundsätzlich nichts.
- b)** Gemäß Ziffer 3.2 der zwischen Ihrem Mandanten und unserem Haus vereinbarten Sonderbedingungen für das pushTAN-Verfahren ist die TAN streng geheim zu halten und darf Dritten unter keinen Umständen mitgeteilt werden. Diese Pflicht ist absolut und unterliegt keinen Ausnahmen.
- c)** Ihr Mandant wurde quartalsweise, zuletzt am 15.01.2025, mit dem ausdrücklichen Hinweis informiert: „Die Sparkasse wird Sie niemals telefonisch, per E-Mail oder SMS zur Eingabe von TANs, PINs oder Passwörtern auffordern.“ Trotz dieser eindeutigen Warnung hat Ihr Mandant eine TAN telefonisch weitergegeben.

III. Zu Ihren weiteren Argumenten

Zum Call-ID-Spoofing: Die Möglichkeit der Rufnummernmanipulation ist spätestens seit Inkrafttreten des § 66k TKG allgemein bekannt. Das OLG Frankfurt (Urt. v. 27.02.2020 – 17 U 42/19) hat

klargestellt, dass allein die Anzeige einer bekannten Rufnummer keinen schützenswerten Vertrauenstatbestand begründet.

Zur App-Anzeige: Der vollständige Anzeigetext lautete „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“. Der Zusatz „Transaktionsfreigabe“ ist eindeutig und hätte bei pflichtgemäßer Sorgfalt (§ 276 Abs. 2 BGB) Anlass zur Vorsicht geben müssen.

Zum Transaktionsmonitoring: Unser Transaktions-Monitoring-System entspricht den aufsichtsrechtlichen Anforderungen. Die Tatsache, dass die Transaktionen technisch korrekt autorisiert wurden, begründete aus Systemsicht keinen Anomalieverdacht.

IV. Ergebnis

Wir weisen die Erstattungsforderung Ihres Mandanten vollumfänglich zurück. Ein Erstattungsanspruch gemäß § 675u BGB ist durch die grobe Fahrlässigkeit Ihres Mandanten nach § 675v Abs. 3 Nr. 2 BGB ausgeschlossen.

Einen Vergleich können wir nicht anbieten. Wir sehen einer gerichtlichen Überprüfung mit Zuversicht entgegen.

Ihrem Mandanten steht es frei, ein Schlichtungsverfahren beim Ombudsmann der deutschen Sparkassen einzuleiten (Kundenbeschwerdestelle beim DSGVO, Charlottenstraße 47, 10117 Berlin). Wir weisen darauf hin, dass der Schlichtungsspruch für beide Seiten nicht bindend ist.

Mit freundlichen Grüßen

Sparkasse Berlin

Dr. jur. Friedrich Steinberg
Direktor · Leiter Recht und Compliance

PDF-Anhang: originale/15_Antrag_Ombudsmann_010725.pdf

Datei: 15_Antrag_Ombudsmann_010725.pdf

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

Kundenbeschwerdestelle beim Deutschen Sparkassen- und Giroverband e.V.
Charlottenstraße 47, 10117 Berlin

Unser Zeichen: 2025-B-0478

Sachbearbeiter: RA Dr. Marcus Brezelmann

Datum: 1. Juli 2025

Antrag auf Durchführung eines Schlichtungsverfahrens

Peter Mayer ./ Sparkasse Berlin

Streitwert: 12.295,00 €

Sehr geehrte Damen und Herren,

namens und in Vollmacht unseres Mandanten Peter Mayer, Lietzenburger Straße 74, 10719 Berlin, beantragen wir hiermit die Durchführung eines Schlichtungsverfahrens gemäß § 14 Abs. 1 des Unterlassungsklagengesetzes (UKlaG) i.V.m. der Verfahrensordnung der Kundenbeschwerdestelle beim DSGV.

I. Beteiligte

Beschwerdeführer: Peter Mayer, Lietzenburger Straße 74, 10719 Berlin, vertreten durch Kanzlei Brezelmann & Partner, Kurfürstendamm 195, 10707 Berlin

Beschwerdegegnerin: Sparkasse Berlin, Alexanderplatz 2, 10178 Berlin

II. Gegenstand der Beschwerde

Unser Mandant begehrt die Erstattung von 12.295,00 € nebst Zinsen wegen nicht autorisierter Zahlungsvorgänge gemäß § 675u BGB.

III. Sachverhalt

Am 28. Mai 2025 gegen 11:15 Uhr wurde unser Mandant Opfer eines sogenannten Call-ID-Spoofing-Angriffs. Ein unbekannter Täter rief unseren Mandanten unter der gefälschten Servicenummer der Sparkasse Berlin (030-869869869) an und gab sich als Mitarbeiter des Sicherheitsteams aus.

Der Anrufer behauptete, es seien verdächtige Abbuchungsversuche aus Rumänien festgestellt worden und das Konto müsse sofort gesperrt werden. Er kannte den Namen und Kontodaten unseres Mandanten. Unter diesem Vorwand bewog er unseren Mandanten, eine pushTAN zu generieren und telefonisch mitzuteilen. Die App zeigte als Beschreibung „Freigabe für Sicherheitssperre“ an.

Mit der erschlichenen TAN wurden folgende betrügerische Transaktionen durchgeführt:

- Überweisung an Digital Services GmbH: 4,500.00 €
- Überweisung an TechPay Solutions: 3,200.00 €
- Lastschriftrückgabe Miete: 1,850.00 €

- Lastschriftrückgabe Versicherungen (gesamt): 645.00 €
- Apple Pay Transaktionen (Elektronikfachgeschäfte München/Stuttgart): 2,100.00 €

Gesamtschaden: 12,295.00 €

Unser Mandant erstattete am 29. Mai 2025 Strafanzeige beim LKA Berlin (Az.: LKA 24/250529/0847).

IV. Bisherige Korrespondenz

- 28. Mai 2025, 12:15 Uhr: E-Mail des Mandanten an die Sparkasse Berlin (Schadensmeldung)
- 2. Juni 2025: Erstes Ablehnungsschreiben der Sparkasse Berlin (Az.: SB-2025/KR-44782)
- 3. Juni 2025, 09:45 Uhr: Beschwerde des Mandanten
- 5. Juni 2025: Zweites Ablehnungsschreiben der Sparkasse Berlin (Az.: SB-2025/ST-44782-2), Entscheidung als abschließend erklärt
- 10. Juni 2025: Anwaltsschreiben mit Zahlungsaufforderung und Fristsetzung (Az.: 2025-B-0478)
- 20. Juni 2025: Ablehnungsschreiben der Sparkasse Berlin an die Kanzlei (Az.: SB-2025/ST-44782-2)

V. Rechtliche Begründung

Der Erstattungsanspruch unseres Mandanten ergibt sich aus § 675u Abs. 2 BGB. Die Zahlungsvorgänge waren nicht autorisiert im Sinne des § 675j BGB, da unser Mandant zu keinem Zeitpunkt den Willen hatte, Überweisungen zu tätigen oder Apple Pay zu aktivieren.

Der Einwand grober Fahrlässigkeit gemäß § 675v Abs. 3 Nr. 2 BGB greift nicht durch. Die Täuschung mittels Call-ID-Spoofing war technisch anspruchsvoll und für einen durchschnittlichen Verbraucher nicht erkennbar (vgl. LG Köln, Urt. v. 08.01.2024 – 15 O 267/23). Die irreführende Formulierung in der pushTAN-App („Freigabe für Sicherheitssperre“) hat maßgeblich zur Täuschung beigetragen. Zudem hat die Sparkasse Berlin gegen ihre Pflichten aus Art. 97 PSD2 (eindeutige Transaktionsinformation) und § 675f Abs. 2 BGB (Transaktionsüberwachung) verstoßen.

VI. Antrag

Wir beantragen, die Sparkasse Berlin im Wege der Schlichtung dazu anzuhalten, unserem Mandanten den Betrag von 12.295,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 28. Mai 2025 zu erstatten.

Mit freundlichen Grüßen

RA Dr. Marcus Brezelmann
Fachanwalt für Bank- und Kapitalmarktrecht

Anlagen:

- Vollmacht (Kopie)
- Gesamte Korrespondenz (chronologisch)

- Screenshots Phishing-Vorfall
- Strafanzeige LKA Berlin, Az.: LKA 24/250529/0847
- Kontoauszüge

PDF-Anhang: originale/16_Schlichtungsvorschlag_Ombudsmann_1508

Datei: 16_Schlichtungsvorschlag_Ombudsmann_150825.pdf

Kundenbeschwerdestelle

beim Deutschen Sparkassen- und Giroverband e.V.

Charlottenstraße 47, 10117 Berlin · Tel.: +49 30 20 225-0 · www.dsgv.de/schlichtungsstelle

SCHLICHTUNGSVORSCHLAG

gemäß § 10 der Verfahrensordnung der Kundenbeschwerdestelle beim DSGV

Aktenzeichen:	S-2025/07-0891
Beschwerdeführer:	Peter Mayer, vertreten durch Kanzlei Brezelmann & Partner
Beschwerdegegnerin:	Sparkasse Berlin
Schlichter:	Schlichter Dr. h.c. Wolfgang Reiter
Datum:	15. August 2025
Streitwert:	12.295,00 €

I. Sachverhalt

Der Beschwerdeführer unterhielt bei der Beschwerdegegnerin ein Girokonto (IBAN DE89 1005 0000 0478 2395 42). Am 28. Mai 2025 wurde er Opfer eines Phishing-Angriffs mittels Call-ID-Spoofing. Ein unbekannter Täter kontaktierte ihn unter der manipulierten Servicenummer der Beschwerdegegnerin und veranlasste ihn unter Vorspiegelung einer Kontosperrung zur Generierung und telefonischen Mitteilung einer pushTAN. In der Folge wurden nicht autorisierte Transaktionen in Höhe von insgesamt 12.295,00 € durchgeführt.

Die pushTAN-App zeigte die Transaktion als „Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“ an. Der Beschwerdeführer erstattete unverzüglich Strafanzeige und kontaktierte den Sperr-Notruf.

Die Beschwerdegegnerin lehnte die Erstattung unter Verweis auf grobe Fahrlässigkeit des Beschwerdeführers (§ 675v Abs. 3 Nr. 2 BGB) ab. Auch nach anwaltlicher Zahlungsaufforderung hielt die Beschwerdegegnerin an ihrer Position fest.

II. Standpunkte der Beteiligten

Standpunkt des Beschwerdeführers:

Der Beschwerdeführer macht geltend, dass die Zahlungsvorgänge nicht autorisiert waren (§ 675u BGB) und ihm keine grobe Fahrlässigkeit vorgeworfen werden könne. Die Täuschung mittels Call-ID-Spoofing sei technisch anspruchsvoll und für ihn nicht erkennbar gewesen. Die irreführende Anzeige in der pushTAN-App habe maßgeblich zur Täuschung beigetragen. Er verweist auf LG Köln, 15 O 267/23.

Standpunkt der Beschwerdegegnerin:

Die Beschwerdegegnerin verweist auf die ständige Rechtsprechung des BGH (XI ZR 91/14), wonach die TAN-Weitergabe regelmäßig grobe Fahrlässigkeit darstelle. Der Beschwerdeführer sei mehrfach über Phishing-Gefahren informiert worden. Der vollständige App-Text habe auch „Transaktionsfreigabe“ enthalten.

III. Würdigung

Nach Prüfung des Sachverhalts und der vorgelegten Unterlagen gelangt der Schlichter zu folgender Einschätzung:

1. Die Zahlungsvorgänge sind nicht autorisiert im Sinne des § 675j BGB. Der Beschwerdeführer wollte keine Überweisungen tätigen, sondern eine Sicherheitssperre veranlassen. Die grundsätzliche Erstattungspflicht nach § 675u Abs. 2 BGB ist gegeben.

2. Die Frage der groben Fahrlässigkeit (§ 675v Abs. 3 Nr. 2 BGB) ist im vorliegenden Fall nicht eindeutig zu beantworten:

- Einerseits stellt die telefonische TAN-Weitergabe grundsätzlich eine erhebliche Sorgfaltspflichtverletzung dar. Die Sonderbedingungen untersagen dies ausdrücklich.
- Andererseits ist die Qualität der Täuschung im vorliegenden Fall außergewöhnlich hoch: Die Rufnummernmanipulation, die Kenntnis persönlicher Daten und die irreführende App-Anzeige bildeten ein geschlossenes Täuschungsbild.
- Insbesondere die Formulierung „Freigabe für Sicherheitssperre“ in der pushTAN-App erscheint geeignet, auch einen sorgfältigen Verbraucher irrezuführen. Die Beschwerdegegnerin trägt insoweit eine Mitverantwortung für die unklare Gestaltung ihrer Sicherheitselemente.

3. Die neuere Instanzrechtsprechung (LG Köln, 15 O 267/23; AG München, 132 C 49/23) tendiert in vergleichbaren Fällen dazu, die grobe Fahrlässigkeit bei qualifizierten Spoofing-Angriffen zu verneinen oder zumindest ein erhebliches Mitverschulden des Zahlungsdienstleisters anzunehmen.

IV. Schlichtungsvorschlag

Unter Berücksichtigung der vorstehenden Erwägungen sowie des Umstands, dass beide Seiten berechtigte Argumente vorbringen, schlägt der Schlichter folgende Einigung vor:

Die Sparkasse Berlin erstattet dem Beschwerdeführer 70 % des entstandenen Schadens, mithin einen Betrag von 8.606,50 € (in Worten: achttausendsechshundertsechs Euro und fünfzig Cent).

Die verbleibenden 30 % (3.688,50 €) trägt der Beschwerdeführer als Eigenanteil. Dieser Eigenanteil trägt dem Umstand Rechnung, dass die TAN-Weitergabe trotz der Täuschung eine objektive Sorgfaltspflichtverletzung darstellt.

Der Vorschlag berücksichtigt, dass die grobe Fahrlässigkeit angesichts der Qualität des Angriffs und der irreführenden App-Gestaltung nicht eindeutig feststellbar ist. Die Quotelung 70/30 spiegelt die Verursachungsbeiträge beider Seiten angemessen wider.

V. Hinweise

Dieser Schlichtungsvorschlag ist gemäß § 11 der Verfahrensordnung für beide Parteien **nicht bindend**. Die Beteiligten können den Vorschlag annehmen oder ablehnen. Das Recht zur Klageerhebung bleibt unberührt.

Die Beteiligten werden gebeten, ihre Entscheidung **binnen vier Wochen** ab Zugang dieses Vorschlags schriftlich mitzuteilen.

Schlichter Dr. h.c. Wolfgang Reiter
Schlichter

Vermerk:

Die Sparkasse Berlin hat den Schlichtungsvorschlag mit Schreiben vom 22. August 2025 abgelehnt. Begründung: „Die vorgeschlagene Quotelung widerspricht der ständigen Rechtsprechung des BGH zur groben Fahrlässigkeit bei TAN-Weitergabe. Eine Erstattung – auch anteilig – kommt nicht in Betracht.“

Der Beschwerdeführer hat den Vorschlag mit Schreiben vom 20. August 2025 angenommen.

Das Schlichtungsverfahren ist damit gescheitert. Dem Beschwerdeführer steht der Rechtsweg offen.

PDF-Anhang: originale/17_Kontoauszuege.pdf

Datei: 17_Kontoauszuege.pdf

KONTOAUSZUG

Kontoinhaber: Peter Mayer
IBAN: DE89 1005 0000 0478 2395 42
BIC: BELADEBEXX
Kontoauszug Nr.: 10/2025
Auszugsdatum: 27. Mai 2025
Blatt: 1 von 1

Alter Saldo per 30.04.2025: 13.085,00 €

Buchungstag	Wertstellung	Vorgang	Betrag (€)
01.05.2025	01.05.2025	Lastschrift – Miete Hausverwaltung Kreuzberg GmbH	-1.850,00
05.05.2025	05.05.2025	Lastschrift – DEVK Versicherungen	-285,00
05.05.2025	05.05.2025	Lastschrift – HUK-COBURG Haftpflicht	-45,00
05.05.2025	05.05.2025	Lastschrift – Techniker Krankenkasse	-315,00
07.05.2025	07.05.2025	Kartenzahlung – REWE Lietzenburger Str.	-47,82
12.05.2025	12.05.2025	Lastschrift – Vattenfall Strom	-89,00
12.05.2025	12.05.2025	Lastschrift – GASAG Erdgas	-62,50
15.05.2025	15.05.2025	Kartenzahlung – Lidl Filiale 1847	-38,65
19.05.2025	19.05.2025	Kartenzahlung – dm-drogerie markt	-23,40
22.05.2025	22.05.2025	Überweisung – GEZ Beitragsservice	-55,08
25.05.2025	25.05.2025	Gehalt – Kanzlei Dr. Schneider & Partner	+3.200,00
26.05.2025	26.05.2025	Kartenzahlung – EDEKA Ku'damm	-33,55

Neuer Saldo per 27.05.2025: 12.540,00 €

Verfügbarer Betrag: 12.540,00 € (eingerichteter Dispositionskredit: 3.000,00 €)

KONTOAUSZUG

Kontoinhaber: Peter Mayer
IBAN: DE89 1005 0000 0478 2395 42
BIC: BELADEBEXX
Kontoauszug Nr.: 11/2025
Auszugsdatum: 29. Mai 2025
Blatt: 1 von 1

Alter Saldo per 27.05.2025: 12.540,00 €

Buchungstag	Wertstellung	Vorgang	Betrag (€)
28.05.2025	28.05.2025	Überweisung – Digital Services GmbH, LT12 3456 7890	-4.500,00
28.05.2025	28.05.2025	Überweisung – TechPay Solutions, EE98 7654 3210	-3.200,00
28.05.2025	28.05.2025	Lastschriftrückgabe – Miete (mangels Deckung)	-1.850,00
28.05.2025	28.05.2025	Lastschriftrückgabe – DEVK Versicherungen	-285,00
28.05.2025	28.05.2025	Lastschriftrückgabe – HUK-COBURG	-45,00
28.05.2025	28.05.2025	Lastschriftrückgabe – Techniker Krankenkasse	-315,00
28.05.2025	28.05.2025	Apple Pay – MediaMarkt München	-849,00
28.05.2025	28.05.2025	Apple Pay – Saturn Stuttgart	-599,00
28.05.2025	28.05.2025	Apple Pay – Expert München	-652,00
29.05.2025	29.05.2025	Kontosperre – Verfügungssperre Betrugsfall	0,00

Neuer Saldo per 29.05.2025: -245,00 €

ACHTUNG: Konto im Soll! Verfügungssperre aktiv seit 29.05.2025.

Hinweis: Die mit „Lastschriftrückgabe“ gekennzeichneten Positionen betreffen regelmäßige Lastschriften, die aufgrund fehlender Kontodeckung nach den betrügerischen Überweisungen zurückgegeben wurden.

PDF-Anhang: originale/18_Strafanzeige_Bescheinigung.pdf

Datei: 18_Strafanzeige_Bescheinigung.pdf

Der Polizeipräsident in Berlin

Landeskriminalamt

Dezernat 24 – Cybercrime

Tempelhofer Damm 12, 12101 Berlin · Tel.: 030 4664-924200 · Fax: 030 4664-924299

Herrn

Peter Mayer

Lietzenburger Straße 74, 10719 Berlin

Unser Zeichen: LKA 24/250529/0847

Sachbearbeiterin: KHK'in Sandra Petersen

Datum: 29. Mai 2025

ANZEIGENBESTÄTIGUNG

Bestätigung über die Erstattung einer Strafanzeige

Sehr geehrter Herr Mayer,

hiermit bestätigen wir, dass Sie am 29. Mai 2025 bei der nachstehend bezeichneten Dienststelle Strafanzeige erstattet haben.

I. Angaben zur Anzeige

Aktenzeichen:	LKA 24/250529/0847
Dienststelle:	Landeskriminalamt Berlin, Dezernat 24 – Cybercrime
Anzeigenerstatter:	Peter Mayer, geb. 14. März 1971
Anschrift:	Lietzenburger Straße 74, 10719 Berlin
Aufnahmedatum:	29. Mai 2025
Sachbearbeiterin:	KHK'in Sandra Petersen
Tatzeit:	28. Mai 2025, 11:15 Uhr
Tatort:	Internet / Telekommunikation (Call-ID-Spoofing)
Schadenshöhe:	12.295,00 €

II. Angezeigte Straftaten

- **Computerbetrug** gemäß § 263a Abs. 1 StGB – Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unbefugte Verwendung von Daten
- **Ausspähen von Daten** gemäß § 202a Abs. 1 StGB – Verschaffung des Zugangs zu Daten, die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung
- **Fälschung beweisrelevanter Daten** gemäß § 269 Abs. 1 StGB – Speicherung und Veränderung beweisrelevanter Daten zur Täuschung im Rechtsverkehr (Manipulation der Rufnummernanzeige / Call-ID-Spoofing)

III. Sachverhalt (Kurzfassung)

Der Anzeigenerstatter wurde am 28. Mai 2025 gegen 11:15 Uhr von einer unbekannten Person unter Verwendung der manipulierten Rufnummer 030-869869869 (Sparkasse Berlin) angerufen. Der Täter gab sich als Mitarbeiter des Sicherheitsteams der Sparkasse Berlin aus und veranlasste den Anzeigenerstatter unter dem Vorwand einer dringenden Kontosperrung zur Generierung und telefonischen Mitteilung einer pushTAN.

Mit der erlangten TAN wurden mehrere nicht autorisierte Transaktionen durchgeführt (2 Überweisungen, Apple-Pay-Aktivierung, 3 kontaktlose Zahlungen). Der Gesamtschaden beläuft sich auf 12.295,00 €.

IV. Ermittlungsstand

Die Ermittlungen wurden aufgenommen und dauern an. Es wird darauf hingewiesen, dass:

- Die Empfängerkonten (IBAN LT, IBAN EE) über die internationale Rechtshilfe ermittelt werden
- Die IP-Adresse 185.220.XXX.XXX als Tor-Exit-Node identifiziert wurde, was die Rückverfolgung erschwert
- Eine Zusammenführung mit weiteren gleichgelagerten Verfahren geprüft wird

V. Hinweise

Diese Bestätigung dient als Nachweis der Anzeigenerstattung gegenüber Dritten (insbesondere Banken, Versicherungen, Rechtsanwälte). Über den Fortgang des Verfahrens werden Sie schriftlich unterrichtet.

Sachdienliche Hinweise richten Sie bitte unter Angabe des Aktenzeichens LKA 24/250529/0847 an die oben genannte Dienststelle.

Im Auftrag

KHK'in Sandra Petersen
Kriminalhauptkommissarin
LKA Berlin, Dezernat 24 – Cybercrime

Dienstsiegel

PDF-Anhang: originale/19_Eidesstattliche_Versicherung_Mayer.pdf

Datei: 19_Eidesstattliche_Versicherung_Mayer.pdf

EIDESSTATTLICHE VERSICHERUNG

gemäß § 156 StGB, § 294 ZPO

Name:	Peter Mayer
Geburtsdatum:	14. März 1971
Anschrift:	Lietzenburger Straße 74, 10719 Berlin
Beruf:	Rechtsanwaltsfachangestellter
Personalausweis-Nr.:	T82K47F215 (gültig bis 13.03.2031)

Ich versichere an Eides statt:

1. Ich bin Inhaber des Girokontos bei der Sparkasse Berlin mit der IBAN DE89 1005 0000 0478 2395 42 (Kundennummer: 478-239-561). Ich bin seit über 20 Jahren Kunde der Sparkasse Berlin und nutze das pushTAN-Verfahren seit dessen Einführung.
2. Am 28. Mai 2025, einem Mittwoch, befand ich mich an meinem Arbeitsplatz bei der Kanzlei Dr. Schneider & Partner, Berlin. Gegen 11:15 Uhr erhielt ich einen Anruf auf meinem Mobiltelefon (Nummer: +49 170 448 23 56). Auf dem Display wurde die Nummer 030-869869869 angezeigt. Diese Nummer kannte ich als die offizielle Servicenummer der Sparkasse Berlin.
3. Der Anrufer stellte sich als „Thomas Bergmann vom Sicherheitsteam der Sparkasse Berlin“ vor. Er sprach professionell, höflich und ohne Akzent. Er nannte meinen vollständigen Namen und die letzten Ziffern meiner Kontonummer. Er teilte mir mit, es seien verdächtige Abbuchungsversuche aus Rumänien festgestellt worden und mein Konto müsse dringend gesperrt werden, um größeren Schaden abzuwenden.
4. Der Anrufer bat mich, zur Verifizierung meiner Identität und zur Durchführung der Kontosperrung eine pushTAN zu generieren. Ich öffnete die pushTAN-App auf meinem iPhone 13. In der App wurde die Aufforderung angezeigt als: „Freigabe für Sicherheitssperre“. Diese Beschreibung entsprach exakt dem, was der Anrufer als Zweck der Maßnahme angegeben hatte. Ich generierte daraufhin die TAN.
5. Die in der App angezeigte TAN lautete 487923. Ich teilte diese TAN dem Anrufer telefonisch mit. Der Anrufer bedankte sich und sagte, die Sperre werde nun aktiviert. Das Gespräch dauerte insgesamt etwa 1 Minute und 48 Sekunden.
6. Innerhalb von weniger als 90 Sekunden nach Mitteilung der TAN erhielt ich mehrere Push-Benachrichtigungen auf meinem Mobiltelefon:
 - 11:17:22 Uhr: Überweisung 4.500,00 € an Digital Services GmbH
 - 11:17:24 Uhr: Überweisung 3.200,00 € an TechPay Solutions
 - 11:17:31 Uhr: Lastschriftrückgabe Miete 1.850,00 €
 - 11:17:33 Uhr: Lastschriftrückgabe Versicherungen 645,00 €
 - 11:17:45 Uhr: Apple Pay aktiviert (Sparkassen-Card ****42)
 - 11:18:02 Uhr: Apple Pay Zahlung 849,00 € MediaMarkt München
 - 11:18:15 Uhr: Apple Pay Zahlung 599,00 € Saturn Stuttgart
 - 11:18:28 Uhr: Apple Pay Zahlung 652,00 € Expert München

7. Ich habe sofort erkannt, dass ich Opfer eines Betrugs geworden bin. Ich habe unverzüglich den Sperr-Notruf 116 116 angerufen. Dieser Anruf erfolgte um 11:45 Uhr. Die Karten- und Kontosperre wurde bestätigt. Anschließend rief ich die Sparkasse Berlin unter der Nummer 030-869869869 an und meldete den Vorfall.

8. Am 29. Mai 2025 habe ich beim Landeskriminalamt Berlin, Dezernat 24 – Cybercrime Strafanzeige erstattet (Az.: LKA 24/250529/0847).

9. Ich erkläre ausdrücklich: Ich habe zu keinem Zeitpunkt die Absicht gehabt, Überweisungen zu tätigen, Apple Pay zu aktivieren oder sonstige Zahlungsvorgänge freizugeben. Ich wollte ausschließlich mein Konto sperren lassen, um es vor den angeblichen verdächtigen Abbuchungen aus Rumänien zu schützen.

10. Mir war zum Zeitpunkt des Vorfalls nicht bekannt, dass Telefonnummern gefälscht werden können (sogenanntes „Call-ID-Spoofing“). Ich hatte von dieser Möglichkeit zuvor noch nie gehört. Ich bin von Beruf Rechtsanwaltsfachangestellter und nicht im Bereich der Informationstechnologie tätig.

11. Der Gesamtschaden beläuft sich auf 12.295,00 €. Dieses Geld stellt einen wesentlichen Teil meiner Ersparnisse dar.

Mir ist bekannt, dass die vorsätzliche Abgabe einer falschen Versicherung an Eides statt gemäß § 156 StGB mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft wird.

Berlin, den 5. Juni 2025

Peter Mayer

BEGLAUBIGUNGSVERMERK

Die vorstehende eidesstattliche Versicherung wurde am 5. Juni 2025 vor mir, Notar Dr. Heinrich Kramer, Kanzlei Kurfürstendamm 112, 10711 Berlin, von Herrn Peter Mayer, ausgewiesen durch gültigen Personalausweis (Nr. T82K47F215), persönlich abgegeben.

Ich habe den Erklärenden über die Bedeutung der eidesstattlichen Versicherung und die strafrechtlichen Folgen einer falschen Versicherung an Eides statt belehrt.

Berlin, den 5. Juni 2025

Notar Dr. Heinrich Kramer
UR-Nr. 387/2025

(Dienstsiegel)

PDF-Anhang: originale/20_Zeugenaussage_Kollegin.pdf

Datei: 20_Zeugenaussage_Kollegin.pdf

SCHRIFTLICHE ZEUGENAUSSAGE

gemäß § 377 Abs. 3 ZPO

Name: Marina Vogt
Geburtsdatum: 22. September 1983
Anschrift: Fasanenstraße 31, 10719 Berlin
Beruf: Rechtsanwaltsfachangestellte
Arbeitgeber: Kanzlei Dr. Schneider & Partner, Berlin
Verhältnis zum Betroffenen: Arbeitskollegin seit 2017

Bezug: Vorfall vom 28. Mai 2025 betreffend Peter Mayer

Ich, Marina Vogt, erkläre nach bestem Wissen und Gewissen Folgendes:

I. Zur Person und zum Arbeitsumfeld

Ich bin seit dem 1. März 2017 als Rechtsanwaltsfachangestellte bei der Kanzlei Dr. Schneider & Partner, Berlin tätig. Mein Arbeitsplatz befindet sich im selben Büro wie der von Herrn Peter Mayer. Unsere Schreibtische stehen nebeneinander, in einem Abstand von etwa zwei Metern. Ich arbeite seit nunmehr acht Jahren mit Herrn Mayer zusammen.

II. Beobachtungen am 28. Mai 2025

Am Mittwoch, den 28. Mai 2025, war ich wie gewöhnlich an meinem Arbeitsplatz. Gegen 11:15 Uhr hörte ich, wie das Mobiltelefon von Herrn Mayer klingelte. Er nahm das Gespräch an.

Ich konnte während des Telefonats folgende Äußerungen von Herrn Mayer hören:

- „Ja, Herr Bergmann, guten Tag.“
- „Aus Rumänien? Das kann nicht sein, da habe ich keine Geschäfte.“
- „Ja natürlich, bitte sperren Sie das sofort!“
- „Ja, ich öffne die App... Moment...“
- „Die TAN lautet vier-acht-sieben-neun-zwei-drei.“
- „Gut, vielen Dank, Herr Bergmann.“

Während des Telefonats wirkte Herr Mayer besorgt, aber nicht misstrauisch. Er schien den Anrufer für einen echten Sparkassen-Mitarbeiter zu halten. Das Gespräch dauerte schätzungsweise knapp zwei Minuten.

III. Beobachtungen unmittelbar nach dem Telefonat

Etwa ein bis zwei Minuten nach Beendigung des Telefonats bemerkte ich, dass Herr Mayer plötzlich sehr unruhig wurde. Er starrte auf sein Mobiltelefon und sein Gesicht wurde blass. Ich hörte mehrfach den Benachrichtigungston seines Telefons.

Dann rief er laut aus: „Das kann nicht sein, das Geld ist weg!“ Er war sichtlich schockiert und zitterte. Er versuchte sofort, eine Nummer anzurufen – wie ich später erfuhr, den Sperr-Notruf 116 116.

In den folgenden Minuten war er völlig aufgelöst. Er erzählte mir unter Tränen, was passiert war – dass jemand sich als Sparkassen-Mitarbeiter ausgegeben und sein gesamtes Konto leergräumt habe. Ich half ihm dabei, die Hotline der Sparkasse zu erreichen, und bot ihm ein Glas Wasser an.

IV. Persönliche Einschätzung zu Herrn Mayer

Ich arbeite seit acht Jahren eng mit Herrn Mayer zusammen. Ich kenne ihn als äußerst gewissenhaften und sorgfältigen Kollegen. In unserer beruflichen Zusammenarbeit hat er sich stets als zuverlässig und verantwortungsbewusst erwiesen.

Herr Mayer ist kein leichtgläubiger oder unbedachter Mensch. Dass er dem Anrufer vertraut hat, führe ich allein darauf zurück, dass die Sparkassen-Nummer auf seinem Display angezeigt wurde und der Anrufer äußerst überzeugend auftrat. Ich bin überzeugt, dass die meisten Menschen in dieser Situation genauso reagiert hätten.

Mir ist bekannt, dass ich als Zeugin zur wahrheitsgemäßen Aussage verpflichtet bin und eine falsche uneidliche Aussage gemäß § 153 StGB strafbar ist.

Berlin, den 4. Juni 2025

Marina Vogt

PDF-Anhang: originale/21_Klageschrift_mit_Anlagen.pdf

Datei: 21_Klageschrift_mit_Anlagen.pdf

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)

PDF-Anhang: originale/22_Klageerwiderung_Sparkasse.pdf

Datei: 22_Klageerwiderung_Sparkasse.pdf

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)

PDF-Anhang: originale/23_Sicherheitshinweis_Sparkasse_150125.pdf

Datei: 23_Sicherheitshinweis_Sparkasse_150125.pdf

WICHTIGER SICHERHEITSHINWEIS

für alle Kundinnen und Kunden der Sparkasse Berlin

Datum: 15. Januar 2025

Sehr geehrte Kundin, sehr geehrter Kunde,

die Sicherheit Ihrer Finanzen hat für uns höchste Priorität. Aktuell beobachten wir eine Zunahme betrügerischer Aktivitäten, die darauf abzielen, an Ihre vertraulichen Bankdaten zu gelangen. Wir möchten Sie daher über die gängigsten Betrugsmaschen informieren und Ihnen Tipps zum Schutz geben.

1. Telefonbetrug („Vishing“ / Call-ID-Spoofing)

Betrüger rufen bei Kundinnen und Kunden an und geben sich als Sparkassen-Mitarbeiter aus. Dabei verwenden sie eine Technik namens „Call-ID-Spoofing“, mit der sie die angezeigte Rufnummer manipulieren können. Auf Ihrem Telefondisplay erscheint dann die echte Sparkassen-Nummer, obwohl der Anruf tatsächlich von Kriminellen stammt.

Die Anrufer behaupten typischerweise, es gäbe verdächtige Kontobewegungen oder Sicherheitsprobleme. Sie fordern Sie auf, eine TAN zu generieren und telefonisch mitzuteilen – angeblich zur „Verifizierung“ oder „Kontosperre“.

2. Phishing-E-Mails

Betrügerische E-Mails, die täuschend echt aussehen, fordern Sie auf, über einen Link Ihre Zugangsdaten einzugeben. Achten Sie auf: unpersönliche Anrede, Rechtschreibfehler, dringliche Aufforderungen, verdächtige Absenderadressen.

3. SMS-Phishing („Smishing“)

Sie erhalten eine SMS, die angeblich von der Sparkasse stammt, mit der Aufforderung, einen Link anzuklicken. Dieser führt zu einer gefälschten Webseite.

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

So schützen Sie sich:

- Geben Sie **niemals** TANs, PINs oder Passwörter am Telefon, per E-Mail oder SMS weiter – auch nicht an vermeintliche Sparkassen-Mitarbeiter.
- Vertrauen Sie **nicht** der angezeigten Rufnummer. Telefonnummern können gefälscht werden.

- Legen Sie bei verdächtigen Anrufen auf und rufen Sie uns über die Ihnen bekannte Nummer zurück: 030-869869869.
- Prüfen Sie bei jeder TAN-Freigabe in der App **genau**, welche Transaktion Sie freigeben. Lesen Sie den **vollständigen** Anzeigetext.
- Klicken Sie **nicht** auf Links in E-Mails oder SMS, die Sie zur Eingabe von Zugangsdaten auffordern.
- Sperren Sie im Notfall Ihr Konto sofort über den Sperr-Notruf **116 116** (kostenlos, rund um die Uhr).

Bei Fragen oder Verdächtigungen wenden Sie sich bitte an Ihre Filiale oder unseren Kundenservice unter 030-869869869.

Mit freundlichen Grüßen

Ihre Sparkasse Berlin

*Dieser Sicherheitshinweis wird quartalweise an alle Kundinnen und Kunden versandt. Letzter Versand: 15. Oktober 2024.
Sparkasse Berlin · Alexanderplatz 2, 10178 Berlin · BLZ 100 500 00*

PDF-Anhang: originale/24_Technisches_Protokoll_TAN.pdf

Datei: 24_Technisches_Protokoll_TAN.pdf

TECHNISCHES PROTOKOLL

TAN-Verwendung und Transaktionslog

— Anonymisierte Version — Anlage zum Schreiben vom 5. Juni 2025 —

Aktenzeichen: SB-2025/KR-44782
Kunde: Peter Mayer (Kd.-Nr. 478-239-561)
IBAN: DE89 1005 0000 0478 2395 42
Erstellungsdatum: 28. Mai 2025
Erstellt durch: Abt. IT-Sicherheit / Betrugsprevention

1. Geräteregistrierung pushTAN

Parameter	Wert
Gerätetyp:	Apple iPhone 13
Betriebssystem:	iOS 17.4.1
pushTAN-App-Version:	3.8.2 (Build 4891)
Registrierungsdatum:	05. März 2024, 14:22:18 Uhr
Geräte-ID (intern):	DEV-478239-A7F2B
Registrierungs-IP:	91.64.XXX.XXX (Telekom Deutschland)
Aktivierungsmethode:	Aktivierungsbrief + Erstanmeldung Filiale
Letzte App-Aktualisierung:	12. Mai 2025

2. TAN-Generierung und -Eingabe am 28. Mai 2025

Parameter	Wert
TAN-Generierung:	28.05.2025, 11:16:42.317 Uhr (UTC+2)
TAN-Wert:	487923
TAN-Gültigkeitsdauer:	300 Sekunden (bis 11:21:42 Uhr)
App-Anzeigetext:	„Freigabe für Sicherheitssperre und Transaktionsfreigabe – Mehrere Vorgänge“
TAN-Typ:	Sammelauftrag (Batch-TAN)
Generierungs-IP:	91.64.XXX.XXX (Telekom Deutschland / Mobilfunk)
TAN-Eingabe:	28.05.2025, 11:17:14.892 Uhr (UTC+2)
Eingabe-IP:	185.220.XXX.XXX
IP-Klassifikation:	Tor-Exit-Node (NL – Niederlande)
User-Agent:	Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0

Session-ID:	SES-28052025-XXX-A4F7
Login-Zeitpunkt:	28.05.2025, 11:14:33 Uhr
Login-Methode:	Online-Banking (Benutzername + PIN)
2FA-Status:	TAN erfolgreich validiert

Hinweis: Die IP-Adresse der TAN-Generierung (Mobilfunknetz) und die IP-Adresse der TAN-Eingabe (Tor-Exit-Node) stimmen nicht überein. Dies deutet darauf hin, dass die TAN nicht vom selben Gerät/Netzwerk eingegeben wurde, das sie generiert hat.

3. Ausgeführte Transaktionen (chronologisch)

Zeit (UTC+2)	Typ	Details	Betrag
11:17:22.104	Überweisung	Digital Services GmbH IBAN LT12 3456 7890 1234 5678 Verw.zweck: INV-2025-4471	4.500,00 €
11:17:24.318	Überweisung	TechPay Solutions IBAN EE98 7654 3210 9876 5432 Verw.zweck: ORDER-88291	3.200,00 €
11:17:31.547	LS-Rückgabe	Hausverwaltung Kreuzberg GmbH Miete Juni 2025 – mangels Deckung	1.850,00 €
11:17:33.221	LS-Rückgabe	DEVK / HUK / TK Versicherungen 3 Lastschriften – mangels Deckung	645,00 €
11:17:45.892	Apple Pay	Kartenaktivierung Sparkassen-Card ****42 Gerät: iPhone (unbekannt) IP: 185.220.XXX.XXX	–
11:18:02.113	Apple Pay	MediaMarkt München-Stachus Kontaktlose Zahlung	849,00 €
11:18:15.447	Apple Pay	Saturn Stuttgart-Mitte Kontaktlose Zahlung	599,00 €
11:18:28.891	Apple Pay	Expert München-Pasing Kontaktlose Zahlung	652,00 €

Gesamtschadenssumme: 12.295,00 €

Zeitspanne von erster Transaktion bis letzter Transaktion: 66,787 Sekunden. Dies deutet auf ein automatisiertes Angriffsskript hin.

4. Kontosperrung

Parameter	Wert
Sperr-Notruf (116 116):	28.05.2025, 11:45:00 Uhr
Kartensperrung bestätigt:	28.05.2025, 11:47:12 Uhr
Online-Banking-Sperrung:	28.05.2025, 11:48:03 Uhr
Anruf Sparkasse-Hotline:	28.05.2025, 11:52:00 Uhr
Vollständige Kontosperrung:	28.05.2025, 12:04:18 Uhr

Erstellung: Abt. IT-Sicherheit, Sparkasse Berlin
Geprüft: Assessor jur. Thomas Krüger, Abt. Zahlungsverkehr
Freigabe: Dr. jur. Friedrich Steinberg, Direktor Recht und Compliance

— Dieses Protokoll wurde anonymisiert. Vollständige IP-Adressen, Geräte-IDs und Session-Daten sind in der nicht anonymisierten Fassung enthalten (nur für den internen Dienstgebrauch). —