

Phishing, Pharming & Co. in der Hausratversicherung

Leistungsversprechen, aktuelle Rechtsprechung und Tipps für die Schadenbearbeitung

Inhalt

Sechs Abschnitte – vom Fall über das Bedingungsmerk bis in die Schadenpraxis

A

Einstieg und Relevanz

B

Technische Erscheinungsformen

C

Leistungsversprechen & Klauselarchitektur

D

Rechtliche Einordnung & AVB-Auslegung

E

Aktuelle Rechtsprechung

F

Schadenbearbeitung in der Praxis

A

Einstieg und Relevanz

Ein Fall vom Kleinanzeigenmarkt – und die Frage, die er aufwirft



Der Fall

Vier Schritte von der Kontaktaufnahme bis zur offenen Deckungsfrage

01

Der Fall

Eine Frau bietet auf einer Kleinanzeigenplattform gebrauchte Waren zum Verkauf an. Ein vermeintlicher Käufer meldet sich und erklärt, die Zahlung könne erst nach einer Verifizierung freigegeben werden.

02

Die Falle

Sie erhält eine SMS mit einem Link, der sie auf eine täuschend echte, gefälschte Website führt. Dort gibt sie ihre Karten- und Kontodaten ein und bestätigt anschließend einen Code in ihrer Banking-App – in der Überzeugung, einen legitimen Verifizierungsschritt durchzuführen.

03

Der Schaden

Ihr Konto wird mit mehreren tausend Euro belastet. Die Bank erstattet den Betrag nur teilweise zurück, da sie der Ansicht ist, die Kontoinhaberin habe den Zahlungsvorgang selbst autorisiert.

04

Die entscheidende Frage

Handelt es sich um einen versicherten Phishing-Schaden in der Hausratversicherung – oder nur um eine nicht gedeckte digitale Zahlungstransaktion, die auf einem Irrtum der Versicherungsnehmerin beruht?

Leitthese

”

Die Antwort ergibt sich nicht aus der allgemeinen Verwendung des Wortes „Phishing“.

Maßgeblich ist, was die spezifischen Versicherungsbedingungen versprechen und wie sich der tatsächliche Geschehensablauf in dieses Leistungsversprechen einfügt.

Gerade bei SMS-Angriffen, dem Einrichten digitaler Karten und der anschließenden Nutzung im stationären Handel können technische und rechtliche Kategorien auseinanderdriften.



Warum das Thema in der Hausratversicherung angekommen ist

Von der Sachversicherung zum Baustein für reine Vermögensschäden

1

Traditionelle Deckung

Die Hausratversicherung ist traditionell auf Schäden am beweglichen Eigentum des Versicherungsnehmers zugeschnitten.

2

Neues Risiko-Feld

Mit Online-Banking, mobilem Bezahlen und digitalen Marktplätzen hat sich jedoch ein neues Risiko-Feld entwickelt.

3

Reaktion der Versicherer

Versicherer reagieren mit Internetschutz-, Onlineschutz- oder Digitalschutz-Bausteinen, die herkömmliche Hausratversicherungen ergänzen.

Kein Rundum-Schutz

Diese Bausteine sind keine automatische, vollumfassende Cyber-Versicherung. Sie erweitern den ursprünglichen Schutz der Sachversicherung um bestimmte, vertraglich definierte reine Vermögensschäden.

Was offen bleibt

Die Reichweite entscheidet sich im einzelnen Bedingungsmerk

4

Umfang

Diese Bausteine sind keine automatische, vollumfassende Cyber-Versicherung. Sie erweitern den ursprünglichen Schutz der Sachversicherung um bestimmte, vertraglich definierte reine Vermögensschäden.

5

Offene Fragen

Welche digitalen Angriffe erfasst sind, wie der Zahlungsprozess ausgestaltet sein muss und welche Daten als Zugangsdaten gelten, bleiben Fragen der jeweiligen Tarifgeneration und Bedingungsmerk-Version.



B

Technische Erscheinungsformen

Phishing, Pharming und die Tatsachen, auf die es ankommt



Die gängigsten Erscheinungsformen

Technische Kategorien des Cyber-Betrugs

1

Phishing

Täuschungsversuche zum Erlangen sensibler Daten per gefälschter Kommunikation. Smishing nutzt SMS, Vishing Anrufe und Skimming manipuliert Hardware an Geldautomaten oder POS-Terminals.

2

Pharming

Nutzer werden unbemerkt auf gefälschte Websites umgeleitet – selbst bei korrekter Adresseingabe. Typischerweise durch Manipulation von DNS-Servern oder der Hosts-Datei des Zielsystems.

3

Zu prüfende Tatsachen

Es sind die konkreten Details des Angriffs und die Art der Datenkompromittierung maßgeblich – einschließlich Tathergang und Kausalitätsprüfung.



Die entscheidenden Tatsachen

Sechs Feststellungen, ohne die keine Deckungsprüfung trägt

01

Das Kommunikationsmittel

Welcher Kanal wurde für den Angriff genutzt (E-Mail, SMS, Messenger, Telefon)?

02

Die technische Angriffshandlung

War es ein Link auf eine gefälschte Seite oder eine technische Umleitung des korrekten Aufrufs?

03

Die konkret erlangten Daten

Welche Daten wurden tatsächlich erlangt (Zugangsdaten, PIN/TAN, App-Freigabe, IBAN, Kartendaten)?

04

Die Art und der Ort der Zahlung

War es eine Überweisung, Onlinezahlung, Kartenzahlung, Lastschrift oder stationärer Einkauf?

05

Der unmittelbare Kausalverlauf

Welche Handlung führte unmittelbar zur Belastung des Kontos?

06

Die Vorstellung des Versicherungsnehmers

Wollte der Versicherungsnehmer eine Zahlung ausführen oder eine Verifizierung/Freischaltung?

Die bloße Feststellung „es war ein Phishing-Angriff“ ersetzt diese Tatsachenfeststellungen nicht.

C

Leistungsversprechen & Klauselarchitektur

Was die Bedingungswerke tatsächlich versprechen



Klauselbeispiel 1

Enge Fassung: Zugangsdaten zum Onlinebanking

Versichert sind Vermögensschäden des Versicherungsnehmers oder einer mit ihm in häuslicher Gemeinschaft lebenden Person durch den Missbrauch von Zugangsdaten für das private Onlinebanking, die durch Phishing erlangt worden sind.

Phishing ist eine Betrugsmethode, bei der der Täter sich ausschließlich mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten des Versicherungsnehmers oder einer mit ihm in häuslicher Gemeinschaft lebenden Person beschafft, um diese Daten zu missbrauchen.

Ersetzt wird der durch den Phishingangriff verursachte Vermögensschaden in Höhe des abgebuchten Betrags vom privaten Konto. Mehrere Buchungen stellen einen Vermögensschaden dar, wenn sie durch einen Phishingangriff verursacht worden sind. Das gilt auch, wenn der Täter mehrere Zugangs- oder Identifikationsdaten erlangt hat.

Versichert ist der Missbrauch von Zugangsdaten für das private Onlinebanking – erlangt ausschließlich über gefälschte E-Mails.

Klauselbeispiel 2

Phishing als Verfahren

Phishing im Sinn dieser Regelung ist ein Verfahren, bei dem Täter sich mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten verschaffen, wobei die Täter typischerweise ein durch die Täuschung über die tatsächliche Identität erlangtes Vertrauensverhältnis ausnutzen. Mit den gewonnenen Daten nehmen die Täter unter der Identität des Inhabers im Online-Verkehr unerlaubte Handlungen vor.

Die Klausel beschreibt den Tathergang: gefälschte E-Mails, ein erschlichesenes Vertrauensverhältnis und Handlungen unter fremder Identität.

Klauselbeispiel 3

Weite Fassung: Kontodaten samt PIN und TAN

Phishing liegt vor, wenn Dritte mit Hilfe gefälschter E-Mails Kontodaten sowie dazugehörige PIN, TANs und Passwörter von dem Versicherungsnehmer oder der mit ihm in häuslicher Gemeinschaft lebenden Personen zu erlangen versuchen. Ziel dieser gefälschten E-Mails ist es, mit den gewonnenen Daten auf gefälschten Internetseiten von Banken unerlaubte Handlungen vorzunehmen.

Hier genügt, dass Dritte über gefälschte E-Mails Kontodaten nebst PIN, TANs und Passwörtern erlangen, um damit unerlaubte Handlungen vorzunehmen.

Die fünf Bausteine der Deckung

Jede Klausel beantwortet diese fünf Fragen anders

1

Wer ist geschützt?

Manche Klauseln nennen nur den Versicherungsnehmer, andere beziehen Personen ein, die mit ihm in häuslicher Gemeinschaft leben.

2

Welche Konten sind erfasst?

Girokonten, Depots, Kredit- oder Bankkarten und virtuelle Konten mit Zahlungsfunktion können unterschiedlich behandelt werden.

3

Das Angriffsmittel

E-Mails, elektronische Nachrichten, gefälschte Webseiten, sonstige Täuschungshandlungen.

4

Die erlangten Daten

Zugangsdaten, Identifikationsdaten, PIN, TAN und Passwörter sind nicht gleichbedeutend mit IBAN, Kartenummer oder den üblichen Daten einer Kartenzahlung.

5

Der Schadenmechanismus

Einige Bedingungen versichern ungewollte Zahlungen vom Konto. Andere knüpfen an Überweisungen, Kartendaten im Internet oder unbefugte Nutzung virtueller Konten an. Die Begriffe „Belastung“, „Zahlung“ und „Überweisung“ dürfen nicht gleichgesetzt werden.

D

Rechtliche Einordnung & AVB-Auslegung

Drei Maßstäbe: Verständnishorizont, Transparenzkontrolle, Kausalität



I. Der Maßstab der Auslegung

Wie ein durchschnittlicher Versicherungsnehmer die Bedingung verstehen muss – Wortlaut zuerst, aber nicht allein

”

Bei der Auslegung von AVB kommt es darauf an, wie ein durchschnittlicher Versicherungsnehmer ohne versicherungsrechtliche Spezialkenntnisse die Bestimmung bei verständiger Würdigung, aufmerksamer Durchsicht und Berücksichtigung des erkennbaren Sinnzusammenhangs verstehen muss.

Ausgangspunkt ist der Wortlaut; einzubeziehen sind aber auch Systematik, Zweck und die berechtigten Erwartungen an den Versicherungsschutz.

BGH, 19.09.2007 – IV ZR 136/06

Wortlaut

Ausgangspunkt jeder Auslegung

Systematik & Zweck

Der Sinnzusammenhang des Klauselwerks

Erwartung

Berechtigte Erwartung an den Schutz

II. Transparenzkontrolle möglich?

Abgrenzung Primäre Leistungsbeschreibung vs. Risikobegrenzung

Primäre Leistungsbeschreibung

Sie bestimmt, welches Risiko der Versicherer überhaupt übernimmt. Sie legt den Gegenstand der Hauptleistung fest.

Risikobegrenzung

Sie nimmt aus einem bereits versprochenen Schutz einzelne Fälle wieder heraus und engt den zugesagten Umfang ein.

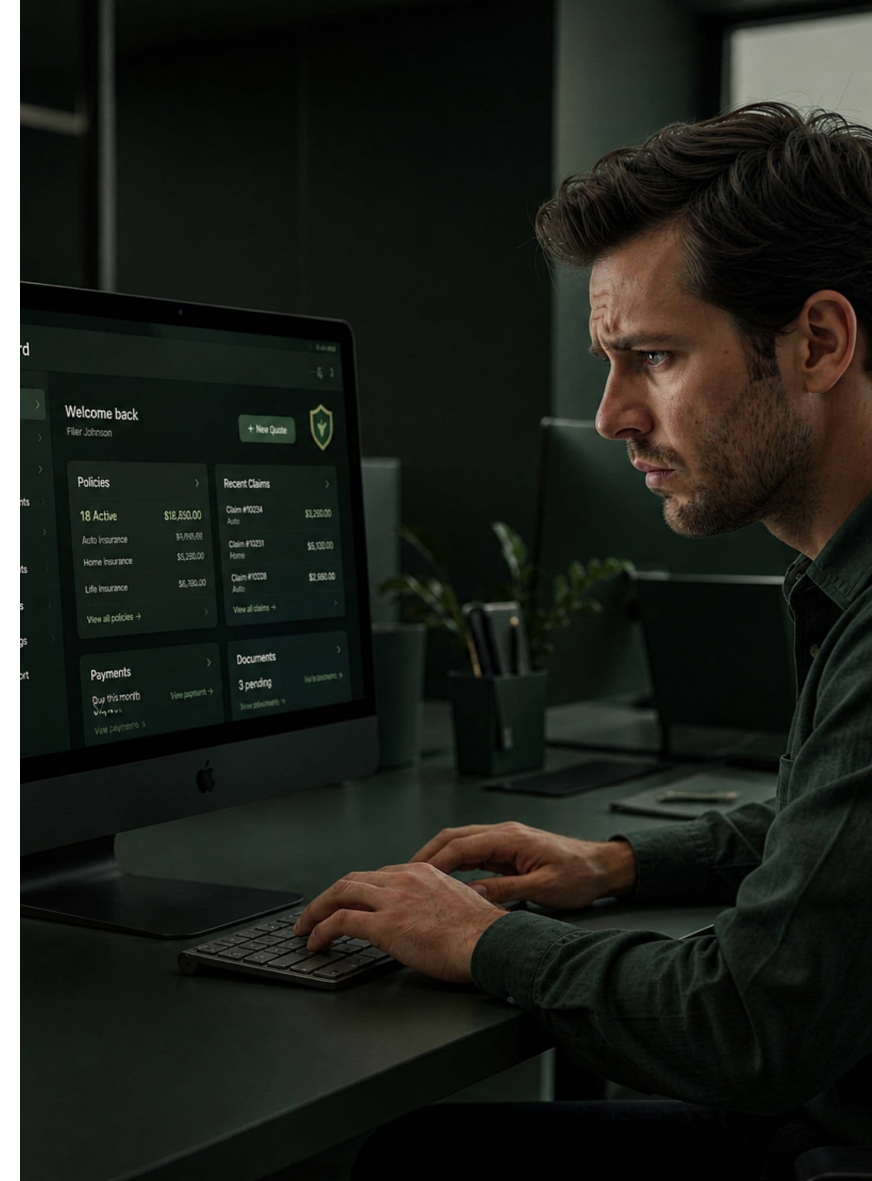
Primäre Leistungsbeschreibungen sind der Transparenzkontrolle nicht zugänglich

III. Kausalität und Zielvorstellung

Die Vorstellung des Handelnden wird zum Tatbestandsmerkmal

Viele Klauseln verlangen nicht nur, dass Daten erlangt wurden. Sie knüpfen zusätzlich daran an, dass der Versicherungsnehmer im Glauben an die Echtheit einer Seite einen Zahlungsvorgang ausführt oder dass die erlangten Daten unmittelbar für eine Überweisung verwendet werden sollen.

Dann ist die Zielvorstellung des Versicherungsnehmers ein relevantes Tatbestandsmerkmal.



E

Aktuelle Rechtsprechung

Vier Entscheidungen aus 2024 und 2025



Vier Entscheidungen im Überblick

In allen vier Fällen blieb die Klage ohne Erfolg – jeweils aus anderem Grund

LG Hamburg

12.12.2024 · 332 O 187/23

5.600 €

Streitwert

SMS statt gefälschter E-Mail; keine Zahlung, sondern Verifizierung

LG Bielefeld

25.09.2025 · 22 S 81/25

4.644,62 €

Streitwert

SMS ist keine E-Mail; digitale Girocard ist kein Zahlungsvorgang

AG Bernau

04.12.2025 · 10 C 212/25

1.968,55 €

Streitwert

IBAN und Kartendaten sind keine Onlinebanking-Zugangsdaten

LG Berlin II

27.05.2025 · 24 O 250/24

6.151,96 €

Streitwert

Mobile-Pay im stationären Handel ist keine Überweisung

Kleinanzeigen, SMS und ein Verifizierungsschritt

Fall 1

LG Hamburg · Urteil vom 12.12.2024, Az. 332 O 187/23

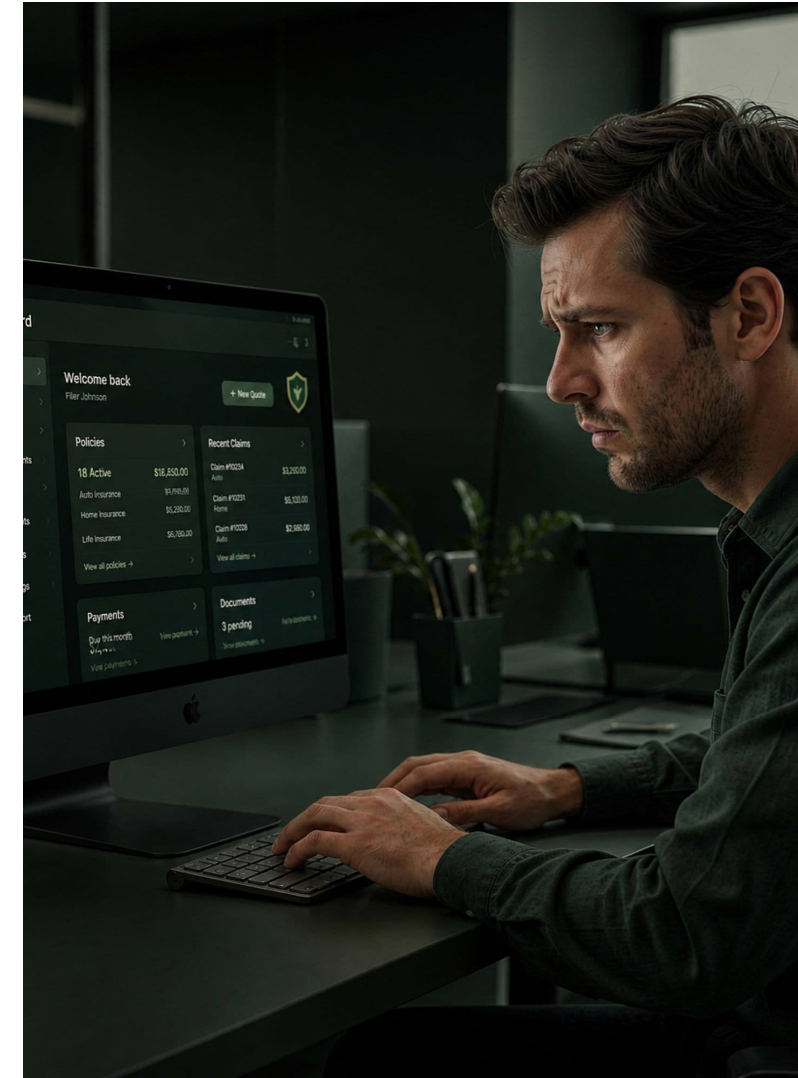
Sachverhalt

Das Landgericht Hamburg hatte über eine Hausratversicherung mit mitversichertem Internetschutz zu entscheiden. Die Versicherungsnehmerin war über eine Kleinanzeigenplattform kontaktiert worden.

Nach dem Erhalt einer SMS mit Link gelangte sie auf eine gefälschte Internetseite, gab dort ihre Karten- und Bankdaten ein und verwendete einen Verifikationscode, um ein angebliches Bezahlungssystem für die Kleinanzeigenplattform freizuschalten. Ihr Konto wurde mit 5.600 EUR belastet.

5.600 €

Belastung des Kontos



Auszug aus den streitgegenständlichen AVB

Fall 1

LG Hamburg · 332 O 187/23

Versicherte Gefahren: „Phishing“ und „Pharming“ – Was ist das genau?

”

„Phishing“: Dritte gelangen über eine gefälschte E-Mail an die Zugangs- und Identifikationsdaten zu Ihrem Konto.

„Pharming“: Dritte ahmen den Internetauftritt Ihres Geldinstituts/Online-Bezahldienstes nach und leiten dadurch Ihre Anfrage auf eine betrügerische Seite um. Sie führen im Glauben an die Echtheit der Seite Zahlungsvorgänge aus.

Zwei Tatbestandsmerkmale entscheiden: die gefälschte E-Mail – und der ausgeführte Zahlungsvorgang.

Die Entscheidung

Fall 1

LG Hamburg · 12.12.2024 – 332 O 187/23

Phishing verneint

Der Angriff erfolgte über eine SMS und nicht über eine gefälschte E-Mail. Die Klausel sei hinreichend klar und leicht verständlich für den durchschnittlichen Versicherungsnehmer; der Versicherer sei grundsätzlich frei, den Umfang des Versicherungsschutzes zu bestimmen.

Pharming verneint

Die Klägerin habe die Daten und den Code nach ihrem eigenen Vorstellungsbild nicht eingegeben, um eine Zahlung auszuführen, sondern um ein Bezahlungssystem zu verifizieren oder freizuschalten. Die Eingabe habe daher keinen Zahlungsvorgang im Sinne der Klausel dargestellt.

Im Ergebnis: weder Phishing noch Pharming – der Schaden blieb beim Versicherungsnehmer.

LG Hamburg, 12.12.2024 – 332 O 187/23

Eine digitale Girocard für fremde Einkäufe

Fall 2

LG Bielefeld · Hinweisbeschluss vom 25.09.2025, Az. 22 S 81/25

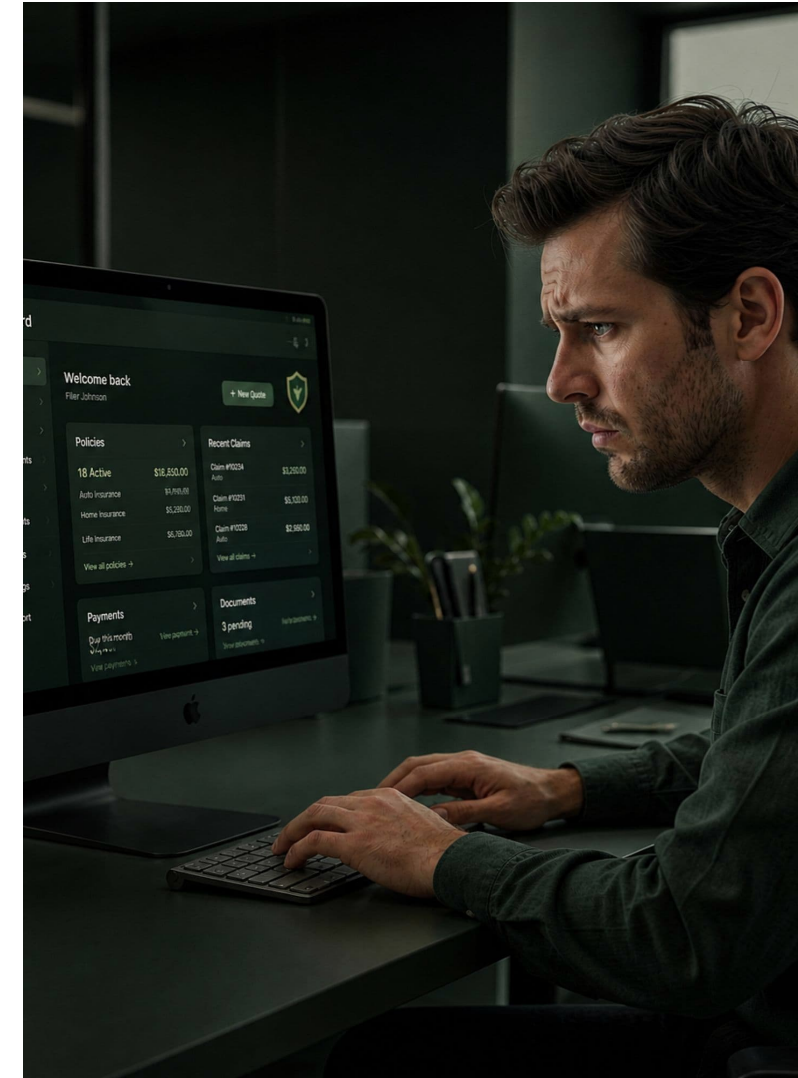
Sachverhalt

Der Kläger hatte eine SMS mit einem Link erhalten, die angeblich die Verlängerung seiner Registrierung für das Bank-Sicherheitsverfahren „VR-SecureGo plus“ betraf. Über die verlinkte, täuschend echt gestaltete Internetseite gab er seine Onlinebanking-Zugangsdaten ein und bestätigte anschließend in der SecureGo-App einen Auftrag.

Tatsächlich nutzten die Täter die Bestätigung, um für das Konto des Klägers eine digitale Girocard einzurichten. Mit dieser Karte tätigten sie später zahlreiche Einkäufe. Die Bank und der Versicherer lehnten eine Erstattung ab.

4.644,62 €

Belastung nach Schadensmeldung (zunächst 4.860,10 €)



Auszug aus den streitgegenständlichen AVB

Fall 2

LG Bielefeld · 22 S 81/25

„Phishing“ und „Pharming“:

”

„Phishing“: Dritte gelangen über eine gefälschte E-Mail an die Zugangs- und Identifikationsdaten zu Ihrem Konto.

„Pharming“: Dritte ahmen den Internetauftritt Ihres Geldinstituts/Online-Bezahldienstes nach und leiten dadurch Ihre Anfrage auf eine betrügerische Seite um. Sie führen im Glauben an die Echtheit der Seite Zahlungsvorgänge aus.

Wortgleich mit der Hamburger Klausel – und doch ein anderer Geschehensablauf.

Die Entscheidung – E-Mail und SMS

Fall 2

LG Bielefeld · 25.09.2025 – 22 S 81/25

Eine SMS ist keine E-Mail, sondern eine davon verschiedene Übermittlungsart

Das Gericht legte die Begriffe E-Mail und SMS nach dem Verständnis eines durchschnittlichen Versicherungsnehmers ohne versicherungsrechtliche Spezialkenntnisse aus. Nach Auffassung des Gerichts unterscheiden sich beide Nachrichtenformen unter anderem hinsichtlich Textumfang, möglicher Dateianhänge, typischer Verwendung und der Erkennbarkeit des Absenders.

Auch könne „E-Mail“ nicht als allgemeiner Oberbegriff für sämtliche elektronischen Nachrichten verstanden werden. E-Mail, SMS und Nachrichten über Messengerdienste seien vielmehr unterschiedliche Kommunikationsformen, die lediglich unter den Oberbegriff „elektronische Nachricht“ fallen könnten. Weil die Klausel ausdrücklich nur die gefälschte E-Mail nennt, war der SMS-basierte Angriff nicht als versichertes Phishing gedeckt.

Die Entscheidung – Pharming

Fall 2

LG Bielefeld · 25.09.2025 – 22 S 81/25

Die Bestätigung einer digitalen Girocard ist kein Zahlungsvorgang

Pharming lag nach der Entscheidung ebenfalls nicht vor. Erforderlich sei eine technische Umleitung des korrekten Aufrufs der Bankseite auf eine betrügerische Seite. Außerdem müsse der Versicherungsnehmer im Vertrauen auf deren Echtheit einen Zahlungsvorgang ausführen.

Die bloße Bestätigung der Einrichtung einer digitalen Girocard erfüllt das nicht. Die eigentlichen Einkäufe wurden erst später von den Tätern mit der digitalen Girocard vorgenommen. Die Bestätigung des Klägers führte daher nach der Bewertung des Gerichts nicht unmittelbar zu einem Zahlungsvorgang.

Chat, Kartendaten und eine Freigabe in der App

Fall 3

AG Bernau · Urteil vom 04.12.2025, Az. 10 C 212/25

Sachverhalt

Die Klägerin wollte auf einer Verkaufsplattform eine gebrauchte Babytrage veräußern. Ein vermeintlicher Kaufinteressent teilte ihr mit, dass es bei der Zahlung Probleme gebe und sie hierzu eine E-Mail der Plattform erhalten werde. Die Klägerin folgte den Anweisungen aus der E-Mail und gelangte darüber in einen Chat mit einem vermeintlichen Mitarbeiter der Plattform.

Im Chat gab sie ihre IBAN und ihre Kreditkartendaten an. Anschließend erhielt sie über ihre Sparkassen-App eine Freigabeaufforderung für eine Zahlung, die sie bestätigte. Der Betrag wurde anschließend von ihrem Girokonto eingezogen.

1.968,55 €

Belastung der Kreditkarte



Auszug aus den streitgegenständlichen AVB

Fall 3

AG Bernau · 10 C 212/25

”

Versichert sind Vermögensschäden des Versicherungsnehmers oder einer mit ihm in häuslicher Gemeinschaft lebenden Person durch den Missbrauch von Zugangsdaten für das private Onlinebanking, die durch Phishing erlangt worden sind.

Phishing ist eine Betrugsmethode, bei der der Täter sich ausschließlich mithilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten des Versicherungsnehmers oder einer mit ihm in häuslicher Gemeinschaft lebenden Person beschafft, um diese Daten zu missbrauchen.

Ersetzt wird der durch den Phishing-Angriff verursachte Vermögensschaden in Höhe des abgebuchten Betrages vom Privatkonto. Mehrere Buchungen stellen einen Vermögensschaden dar, wenn sie durch einen Phishing-Angriff verursacht worden sind.

Hier entscheidet nicht das Angriffsmittel, sondern die Art der preisgegebenen Daten.

Die Entscheidung – Kein Versicherungsfall

Fall 3

AG Bernau · 04.12.2025 – 10 C 212/25

Die Täter haben keine Zugangsdaten für das Onlinebanking erlangt

Das AG Bernau wies die Klage als unbegründet ab. Ein Versicherungsfall sei nicht eingetreten, weil die Täter keine vertraulichen Zugangsdaten für das private Onlinebanking erlangt oder missbraucht hätten.

Das Gericht ließ ausdrücklich offen, ob die Versicherungsbedingung eine Täuschung ausschließlich durch E-Mail voraussetzt oder ob auch eine Kommunikation in einem Chatraum ausreichen könnte. Entscheidend war bereits, dass die konkret preisgegebenen Daten nicht unter den versicherten Begriff der vertraulichen Zugangs- und Identifikationsdaten fielen.

Die Entscheidung – IBAN und Kartendaten

Fall 3

AG Bernau · 04.12.2025 – 10 C 212/25

IBAN und Kreditkartendaten sind keine vertraulichen Zugangsdaten

Nach der Auslegung des Gerichts sind IBAN und Kreditkartendaten typischerweise Daten, die im Zahlungsverkehr gegenüber Dritten angegeben werden müssen. Sie sind deshalb grundsätzlich nicht vertraulich und stellen keine Zugangsdaten zum privaten Onlinebanking dar.

Der Schaden wurde nach den Feststellungen des Gerichts auch nicht durch den Missbrauch von Onlinebanking-Zugangsdaten verursacht. Die Kreditkarte wurde vielmehr unter Verwendung der bei einer Kartenzahlung üblichen Daten belastet. Die eigentliche Zahlung wurde erst durch die von der Klägerin selbst vorgenommene Freigabe in der Sparkassen-App ermöglicht. Auch darin sah das Gericht keinen Missbrauch von Zugangsdaten zum Onlinebanking.

Mobile Pay an Tankstelle und Kasse

Fall 4

LG Berlin II · Urteil vom 27.05.2025, Az. 24 O 250/24

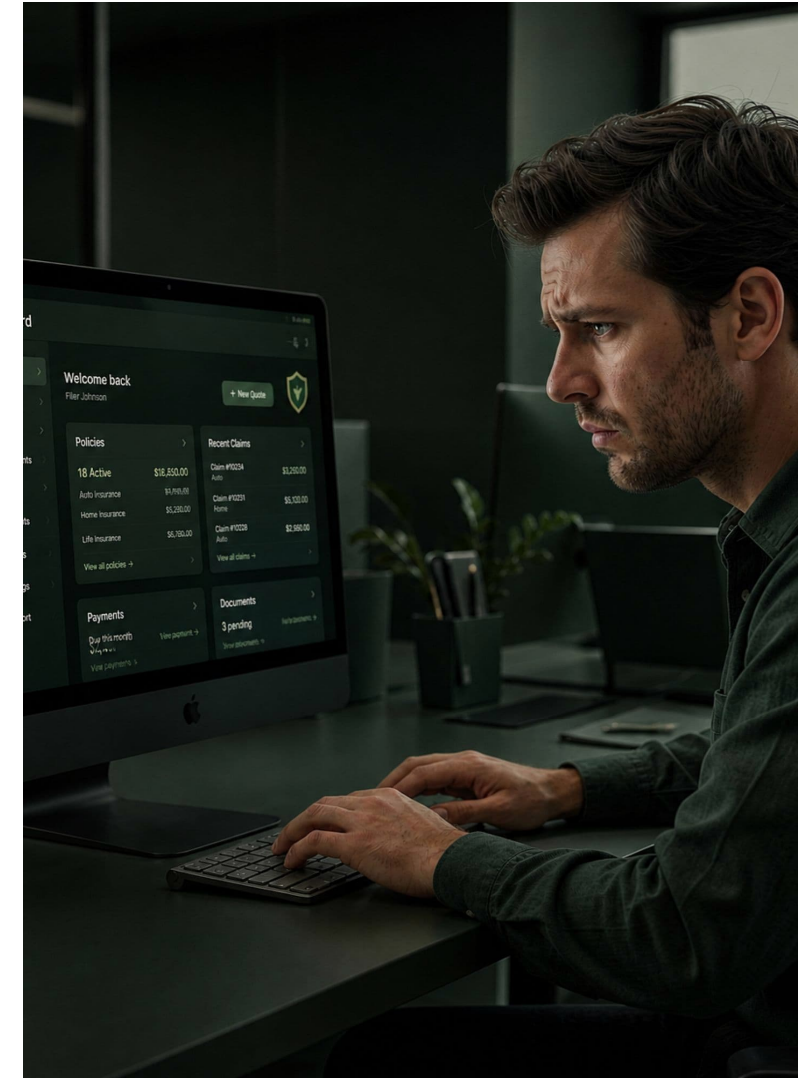
Sachverhalt

Die Klägerin verlangte Ersatz für 17 unberechtigte Zahlungsvorgänge, die Täter nach der Einrichtung und Freischaltung einer digitalen Karte zum Girokonto in einer Mobile-Pay-App bei Tankstellen, Supermärkten und anderen Einzelhändlern vorgenommen hatten.

Die Klägerin war zuvor durch eine SMS mit einem Link und einen anschließenden Anruf dazu gebracht worden, auf einer vermeintlichen Bankseite beziehungsweise im Zusammenhang mit ihrem Online-Banking Zugangsdaten preiszugeben. Sie hat aufgrund des Anrufs den Link in der App angeklickt. Ohne ihr Zutun sei dann durch die Täter eine Mobile-Pay-App freigeschaltet worden. Mit dieser bezahlten die Täter im stationären Handel.

6.151,96 €

17 unberechtigte Zahlungsvorgänge



Auszug aus den streitgegenständlichen AVB

Fall 4

LG Berlin II · 24 O 250/24

”

0991 Online- und Digitalschutz (Cyberklausel) – A. Vermögensschäden durch Onlinebanking- und Onlinezahlungs-Betrug

Versichert sind Vermögensschäden, sofern unberechtigte Dritte 1.1 sich im Internet Zugangs- und Identifikationsdaten zum privat genutzten Bankkonto a. des Versicherungsnehmers [...] verschafft haben und mit diesen Daten unberechtigter Weise Überweisungen vom Bankkonto vornehmen.

1.2 Daten von privat genutzten Kredit- oder Bankkarten sowie virtuellen Konten mit Zahlungsfunktion (z. B. PayPal) a. des Versicherungsnehmers [...] zur Bezahlung im Internet verwenden.

Versicherungsschutz besteht auch, wenn mit Hilfe gefälschter Webseiten und E-Mails Zugangsdaten sowie dazugehörige PIN, TANs und Passwörter vom Bankkonto des Versicherungsnehmers oder der mit ihm in häuslicher Gemeinschaft lebenden Personen erlangt werden (Phishing).

Die Entscheidung – Der Begriff der Überweisung

Fall 4

LG Berlin II · 27.05.2025 – 24 O 250/24

Überweisung heißt: Auftrag an die Bank, von Girokonto zu Girokonto

Der Begriff „Überweisung“ ist nach dem Verständnis eines durchschnittlichen Versicherungsnehmers auszulegen. Gemeint sei der Auftrag an eine Bank, einen bestimmten Geldbetrag von einem Girokonto auf ein anderes Girokonto zu übertragen. Auf die gesetzliche Definition in § 1 Abs. 22 ZAG komme es nicht an, weil ein durchschnittlicher Versicherungsnehmer diese Definition nicht vor Augen habe.

Der Begriff kann dabei nicht isoliert betrachtet werden, sondern muss den gesamten Klauselinhalt sowie die Regelungssystematik berücksichtigen. Ausweislich der Überschriften bietet die Klausel „Onlineschutz“ und erfasst Vermögensschäden „durch Onlinebanking-Betrug“. Ferner setzt der Wortlaut erkennbar voraus, dass die erlangten Zugangs- und Identifikationsdaten direkt verwendet werden, um von dem Bankkonto eine Überweisung zu veranlassen.

Die Entscheidung – Mobile Pay im Handel

Fall 4

LG Berlin II · 27.05.2025 – 24 O 250/24

Weder unmittelbare Überweisung noch Bezahlung im Internet

Die streitgegenständlichen Vorgänge seien keine unmittelbaren Überweisungen vom Bankkonto gewesen. Die Täter hätten zunächst eine Mobile-Pay-App eingerichtet und freigeschaltet. Erst anschließend sei diese App im analogen Handel eingesetzt worden. Zwar hätten die Bezahlvorgänge letztlich zu einer Belastung des Girokontos geführt; eine direkte Überweisung vom Bankkonto, wie sie die Klausel voraussetze, liege darin aber nicht.

Auch eine Bezahlung im Internet lag nach Auffassung des Gerichts nicht vor. Darunter verstehe ein durchschnittlicher Versicherungsnehmer einen direkten Zahlungsvorgang in einem Onlineshop oder eine sonstige online ausgeführte Zahlung. Zahlungen mit einer Mobile-Pay-App im stationären Handel seien davon nicht erfasst.

Die Klausel ist wirksam

Fall 4

LG Berlin II · 27.05.2025 – 24 O 250/24

Keine Inhaltskontrolle

Die Klausel ist als primäre Leistungsbeschreibung gemäß § 307 Abs. 3 Satz 1 BGB einer Inhaltskontrolle entzogen (hierzu BGH, Urteil vom 05.07.2023 – IV ZR 118/22, NJW-RR 2023, 1073 = r+s 2023, 666 Rn. 13).

Keine Aushöhlung

Durch das enge Verständnis wird der Versicherungsschutz nicht ausgehöhlt. Die Hausratversicherung deckt Schäden am Hausrat, mithin Sachsubstanzschäden. Mit der Erweiterung in Klausel 0991 werden zusätzlich reine Vermögensschäden bei bestimmten besonderen Gefahren abgedeckt – das erweitert das Schutzniveau.

Die enge Fassung ist zulässig – die Grenze zieht nicht das AGB-Recht, sondern der Wortlaut selbst.

Die gemeinsame Linie

Nicht jeder Onlinebetrug ist Phishing oder Pharming im Sinne der Versicherungsbedingungen.

Entscheidend ist der konkrete Wortlaut der AVB und der tatsächliche Schadenhergang.

Kein Urteil ist direkt auf andere Fälle übertragbar – stets individuelle Prüfung erforderlich.



F

Schadenbearbeitung in der Praxis

Vier Schritte für die Bearbeitung des nächsten Falls



Schadenbearbeitung in der Praxis

Vom Hergang über die Deckungs-Matrix bis zu den Obliegenheiten

1

Den Sachverhalt in Ereignisschritten aufnehmen

Erfassung des genauen Hergangs in chronologischer Reihenfolge.

2

Deckungs-Matrix anlegen

Abgleich des Schadens mit dem Leistungsversprechen der Versicherungsbedingungen.

3

Verhältnis zur Bank und zum Zahlungsdienstleister

Trennung von der Frage, ob die Bank oder der Zahlungsdienstleister haften.

4

Obliegenheiten und grobe Fahrlässigkeit

Anzeigepflichten, unverzügliche Kontosperrung. Nicht jede unvorsichtige Eingabe begründet eine grobe Fahrlässigkeit.

Vielen Dank

Fragen und Diskussion

Johannsen Rechtsanwälte

