Aktuelle Entwicklungen im Online-Banking

RiOLG Dr. Ole Böger, LL.M. (London)
Hanseatisches Oberlandesgericht in Bremen

Bankrechtstag 2025
Frankfurt, 27. Juni 2025

I. Aktuelle Relevanz von Betrugs- und Missbrauchsfällen im Online-Banking

Gegenstand des Vortrags: Nutzung des Online-Banking durch unbefugte Dritte/Betrugstäter zur Auslösung/Manipulation unbarer Zahlungsvorgänge

Steigende Fallzahlen:

- 90.000 Fälle des Betrugs mit Karten und Konten lt. Kriminalstatistik 2023
- Zuwachs von 14% seit 2022 und von 45% seit 2018 (Quelle: Handelsblatt)

Erhebliche Wahrnehmung in Medien und Fachöffentlichkeit:

- zB Stiftung Warentest, Verbraucherzentrale, pwc Payment Fraud Studie 2025

Vielzahl veröffentlichter Gerichtsentscheidungen aus jüngerer Zeit:

- Diskussion um Maßstäbe der Haftung von Zahlungsdienstleister und -nutzer

II. Überblick über wesentliche Betrugs- und Missbrauchsmaschen im Online-Banking

Phishing: Betrügerische E-Mail oder SMS verleiten Zahler, Links zu gefälschten Online-Banking-Seiten anzuklicken, wo Zugangsdaten von Dritten abgegriffen werden

Quishing: Zahler werden durch Scannen eines QR-Codes auf gefälschte Seite geleitet

Trojaner: Einschleusung von Schadsoftware auf den Rechner des Zahlers, die zB zur Vornahme von Zahlungen verleitet (Rücküberweisungstrojaner) oder Daten ausspäht

Pharming: (korrekter) Aufruf der Online-Banking-Seite durch Zahler führt zu einer gefälschten Website, entweder aufgrund eines kompromittierten DNS-Servers oder einer vorherigen Einschleusung eines Trojaners auf den Rechner des Zahlers

Social engineering: Betrügerischer Anrufe vermeintlicher Bankmitarbeiter, die – oftmals aufgrund vorheriger unbefugter Zugriffe – sich mit Kenntnis von Daten des Kontos des Zahlers legitimieren und den Zahler zur Freigabe von TANs u.a. verleiten

Man-in-the-middle-Angriff: Durch eingeschleuste Schadsoftware wird die Kommunikation des PC/Mobiltelefons des Zahlers mit dem Rechenzentrum der Bank kontrolliert und es werden Kundendaten abgefangen und Transaktionen manipuliert

Sim-Card Fraud: Mobiltelefonanbieter wird verleitet, die Telefonnummer des Zahlers auf neue SIM-Karte zu übertragen; TANs werden auf neues Mobilgerät gesandt

III. Wesentliche Gegenstände der Diskussion in der jüngeren Rechtsprechung

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

2. Insbesondere: Anfechtbarkeit der Autorisierung durch den Zahler

3. Ansprüche des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB aufgrund von Pflichtverletzungen des Zahlers

4. Insbesondere: Folgen der Nichtanwendung einer starken Kundenauthentifizierung nach § 675v Abs. 4 BGB

5. Ansprüche des Zahlungsdienstleisters aus § 122 BGB

6. Sorgfaltspflichtverletzungen des Zahlungsdienstleisters

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

a. Grundsätze

§ 675u S. 2 BGB: Bei nicht autorisierten Zahlungen hat der Zahlungsdienst-nutzer (Zahler) einen Anspruch gegen den Zahlungsdienstleister (ZDL) auf Erstattung und Wiedergutschrift des Zahlbetrags.

Beweislast: ZDL trägt Beweislast für (fehlende) Autorisierung durch Zahler

so jetzt ausdrückl. BGH, Urt.v. 5.3.24 – XI ZR 107/22, BGHZ 240, 23

- gegen früher teilw. vertretene Auffassung einer Beweislast des Zahlers

  so zB OLG Dresden, Urt. v. 21.6.18 – 8 U 1586/17; BeckOGK/M. Zimmermann § 675w Rn. 25 u.a.
- § 675w BGB [Pflicht des ZDL zum Nachweis der Authentifizierung bei bestrittener Autorisierung] als allg. Grundsatz der Beweislastverteilung
- Anschluss an Rspr. des EuGH, siehe EuGH Urt.v. 2.9.21 – C-337/20, CRCAM

Keine Autorisierung nach Anscheinsgesichtspunkten: bei der Erteilung einer Autorisierung kann die Erklärung eines nicht vertretungsberechtigten Dritten dem Zahler nicht nach Anscheinsgesichtspunkten zugerechnet werden,

so BGH, Urt.v. 17.11.20 – XI ZR 294/29, BGHZ 227, 343

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

b. Keine Autorisierung bei unstreitig durch unbefugten Dritten ausgelösten Zahlungen

Ist unstreitig ein Zahlungsvorgang nicht durch den Nutzer, sondern durch einen unbefugten Dritten ausgelöst worden, ist die Zahlung nicht autorisiert und es besteht ein **Erstattungsanspruch des Nutzers aus § 675u S. 2 BGB**

Relevant u.a. in folgenden Konstellationen:

- unstreitiger **Verlust des Zahlungsinstruments** nebst Sicherheitsmerkmalen
- **telefonische Übermittlung von TANs an angebl. Bankmitarbeiter** mit nachfolgender Auslösung der Zahlung durch unbefugten Dritten

  (siehe zB OLG Bremen, Bsl.v. 15.4.24 – 1 U 47/23; OLG Naumburg, Urt.v. 22.5.24 – 5 U 11/24)

  -> Hier nicht schon Autorisierung durch Zahler in Form der Übermittlung von TANs an angeblichen Bankmitarbeiter:
    - Mitteilung der TANs erfolgt nicht in vereinbarter Weise (§ 675j BGB)
    - keine Bevollmächtigung aus Rechtsscheinsgesichtspunkten

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

c. Insbesondere: Keine Autorisierung bei Auslösung von Zahlungen mittels unstreitig durch unbefugten Dritten eingerichteter Zahlungsinstrumente

Wesentliche Anwendungsfälle der vorstehenden Grundsätze:

Zahlungsauslösung mittels durch Dritten eingerichtes Zahlungsinstrument

zB unbefugte Einrichtung einer **Mobilfunk-Zweitkarte (SIM-Card-Fraud), Freischaltung weiterer Mobilgeräte mit darauf installierter pushTAN-App,**

zB OLG Karlsruhe, Urt.v. 19.11.24 – 17 U 127/22; OLG Naumburg, Urt.v. 30.10.24 – 5 U 35/24

oder von **digitalen Zahlungskarten** bzw. **mobilen Bezahldiensten (ApplePay)**

zB OLG Brandenburg, Urt.v. 15.1.25 – 4 U 32/24

LG Köln, Urt.v. 8.1.24 – 22 O 43/23; LG Heilbronn, Urt.v. 2.4.24 – Bm 6 O 378/23

- Zahlungsauslösung erfolgt durch unbefugten Dritten ohne Autorisierung des Zahlers
  -> **Anspruch gg ZDL nach § 675u S.2** auf Erstattung/Wiedergutschrift

- (uU täuschungsbedingte) Mitwirkung des Zahlers an Einrichtung des weiteren Zahlungsinstuments (zB Online-Freischaltung) begründet **keine Autorisierung späterer Zahlungsvorgänge durch Rechtsscheinsvollmacht**

  siehe OLG Brandenburg, aaO; OLG Naumburg, aaO

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

d. Autorisierung bei (täuschungsbedingter) Auslösung von Zahlungen durch den Zahler selbst

Wirksamkeit einer täuschungsbedingten Autorisierung durch den Zahler?

Bsp.: - Man-in-the-Middle-Angriff mit manipulierter Zahlungsdateneingabe
- Zahler wird telefonisch vorgetäuscht, mit Eingabe von TAN lediglich eine Rückbuchung o.ä. (statt einer Überweisung an einen Dritten) zu autorisieren

-> nach allg.M. ist Autorisierung nach obj. Empfängerhorizont auszulegen
bei täuschungsbedingt erteilter Autorisierung kommt es daher nicht auf die subj. Intention des Zahlers an, sondern auf den Erklärungswert gegenüber ZDL

so zB OLG Frankfurt, Bsl.v. 26.4.21 – 23 U 94/20; OLG Stuttgart, Urt.v. 8.2.23 – 9 U 200/22

-> Wirksamkeit der täuschungsbedingten Autorisierung wird teils verneint:

- eA: drohendes Unterlaufen der Haftungsregelung des § 675v BGB, dort Haftung des Zahlers nur bei grober Fahrlässigkeit, nicht bei einfachem Irrtum

  so OLG Dresden, Urt.v. 13.10.22 – 23 U 94/20; MüKoHGB/Linardatos Bd.6 K Rn. 66 u.a.
- aA: Gesetz sieht keine Einschränkung der Wirksamkeit der Autorisierung vor

  so zB OLG Schleswig, Bsl.v. 3.1.24 – 5 W 25/23; OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

e. Anwendung des Anscheinsbeweises bei bestrittener Autorisierung

Rspr. vor ZDRL I: Anscheinsbeweis für **Autorisierung bzw. pflichtwidrige Ermöglichung** einer Zahlung durch Zahler bei **nach außen ordnungsgemäßer Nutzung** eines Zahlungsinstruments und **praktisch nicht zu überwindendem Sicherheitssystem**

siehe BGH, Urt.v. 5.10.04 – XI ZR 210/03, BGHZ 160, 308

- **Fortgeltung dieser Grundsätze auch unter Geltung des § 675w BGB** (seit 2009)
  siehe BGH, Urt.v. 26.1.16 – XI ZR 91/14, BGHZ 208, 331
- **Anscheinsbeweis auch nach Einführung § 675w S. 4 BGB** (seit 2018) verfügbar
  = praktische Unüberwindbarkeit wird als "unterstützende Beweismittel" iSd Norm angesehen
  siehe OLG Bremen, Bsl.v. 19.5.21 – 1 W 4/21; OLG Frankfurt, Urt.v. 30.9.21 – 6 U 69/20

Grundsätze zum Anscheinsbeweis im Online Banking: (BGH Urt.v. 26.1.16, aaO.)

- Anscheinsbeweis für Autorisierung durch Zahler anwendbar, wenn Authentifizierungsverfahren allgemein als **praktisch unüberwindbar** angesehen werden kann:
  - Verfahren von Kompromittierung eingesetzter Geräte nicht berührt
  - Zugriff unberechtigter Dritte auf Übertragungsweg ausgeschlossen
  - Verwendung dynamischer TAN und Zahler kann vor Freigabe Vorgang überprüfen

-> wegen vielfältiger Angriffsmöglichkeiten **kein Anscheinsbeweis für grob fahrl. Pflichtverletzung**

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

e. Insbesondere: Anwendung und Erschütterung des Anscheinsbeweises

smsTAN-(mTAN-)Verfahren: Kein Anscheinsbeweis, da wg. zahlreicher Attacken keine praktische Unüberwindbarkeit anzunehmen, siehe BGH, Urt.v. 26.1.16 – XI ZR 91/14, BGHZ 208, 331

chipTAN-Verfahren: Anscheinsbeweis herkömmlich bejaht,
vgl. BGH aaO.; so auch OLG Dresden, Urt.v. 13.10.22 – 8 U 760/22; Urt.v. 6.4.23 – 8 U 578/22

pushTAN-Verfahren: Anscheinsbeweis teilweise verneint, da keine Nutzung getrennter Kommunikationswege (Online-Banking und TAN-App auf demselben Mobilgerät)
LG Heilbronn, Urt.v. 16.5.23 – 6 O 10/23; vgl. auch Maihold in Ellenberger/Bunte, § 33 Rn. 35
offengelassen in OLG Naumburg, Urt.v. 30.10.24 – 5 U 35/24 (Anscheinsbeweis jdf. erschüttert)

Digitale Bankkarten/ApplePay: kein Anscheinsbeweis wegen zahlreicher Phishingattacken
LG Darmstadt, Urt.v. 3.2.25 – 2 O 190/24; LG Heilbronn, Urt.v. 2.4.24 – Bm 6 O 378/23

Erschütterung des Anscheinsbeweises insbesondere durch Vortrag/Nachweis von Indizien, die für unautorisierten Zahlungsvorgang sprechen:

- zB Auslösung von Zahlungsvorgängen in räumlich/zeitlicher Entfernung vom Zahler
  OLG Brandenburg, Urt.v. 15.1.25 – 4 U 32/24; LG Heilbronn, Urt.v. 2.4.24 – Bm 6 O 378/23
- ungewöhnliche Zahlungsvorgänge (zB Auszahlungen in schneller Folge)
  LG Heilbronn, Urt.v. 27.8.24 – Bm 6 O 103/24; LG Berlin, Urt.v. 31.7.24 – 10 O 201/22
- plausibles Vorbringen des Zahlers zu Phishing/Social-Engineering-Angriff
  OLG Naumburg, aaO.; LG Halle (Saale), Urt.v. 23.6.23 – 4 O 133/22

1. Erstattungsanspruch des Zahlers bei nicht autorisierten Zahlungen aus § 675u S. 2 BGB

f. Relevanz von Überschreitungen vereinbarter Limits

Umstritten ist, ob die Überschreitung nach § 675k Abs. 1 BGB vereinbarter Limits zur Unwirksamkeit einer Autorisierung führt:

- für Schadensersatzhaftung:
  BeckOGK/Köndgen § 675k BGB Rn. 16; Grüneberg/Grüneberg, § 675k BGB Rn. 2
- für Unwirksamkeit wg. Regelung des § 675k BGB im Kontext der Autorisierung und zum umfassenden Schutz des Zahlers gegen Missbrauchsrisiken:
  OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24; Staudinger/Omlor, § 675k BGB Rn. 4

Eine etwaige Heraufsetzung des Verfügungslimits im Online-Banking durch einen unbefugten Dritten ist dem Zahler gegenüber unwirksam:

- Dritter handelt ohne Vertretungsmacht; dies gilt auch bei unbefugter Nutzung ihm überlassener Sicherheitsmerkmale, so OLG Naumburg, Urt.v. 22.5.24 – 5 U 11/24
- keine Anwendung der Grundsätze der Anscheinsvollmacht (siehe vorherige Folien)

2. Insbesondere: Anfechtbarkeit der Autorisierung durch den Zahler

(Bislang) sehr umstritten ist, ob der Nutzer eine täuschungsbedingte Autorisierung einer Zahlung anfechten kann:

Bsp.: - Man-in-the-Middle-Angriff mit manipulierter Zahlungsdateneingabe:
Nutzer erteilt Autorisierung für andere als ihm angezeigte Zahlung
- Nutzer wird telefonisch vorgetäuscht, mit Eingabe von TAN lediglich eine Rückbuchung o.ä. (statt einer Überweisung) zu autorisieren

-> bei Anfechtbarkeit uU Anspruch des Nutzers aus § 675u S. 2 BGB

Vorab: Vorliegen eines Anfechtungsgrundes?

- § 123 BGB?: Täuschung nicht durch ZDL verübt, sondern durch Dritten
  Kenntnis/Kennenmüssen des ZDL idR nicht ersichtlich (§ 123 II 1 BGB)
- § 119 I BGB (Inhaltsirrtum)?
  - zwar kein Irrtum über Erklärung einer Autorisierung als solcher
  - aber Irrtum über die Rechtsfolgen der Autorisierung, die wesentlich andere Wirkungen erzeugt als beabsichtigt (vgl. BGH, Bsl.v. 5.7.06, BGHZ 168, 210)
    -> Inhaltsirrtum daher bejaht bei OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24
    für Annahme eines (unbeachtlichen) Motivirrtums Zahrte BKR 24, 938, 941

2. Insbesondere: Anfechtbarkeit der Autorisierung durch den Zahler

Anfechtbarkeit der Erteilung einer Autorisierung?

- bisher keine Rspr des BGH hierzu; auch Gesetzesbegründung schweigt
- **e.A.: keine Anfechtbarkeit der Autorisierung**
  (siehe OLG Brandenburg, Urt.v. 31.1.18 – 13 U 5/17; LG Itzehoe, Urt.v. 1.3.24 – 9 S 25/23; BeckOGK/Köndgen § 675j Rn. 15; Grüneberg/Grüneberg § 675j Rn. 3 u.a.)
  Arg: - Anfechtbarkeit würde den Grundsatz der Unwiderruflichkeit des Zahlungsauftrags nach § 675p BGB zu unterlaufen drohen
  - teilweise Ausnahme zugelassen für Anfechtung nach § 123 BGB
  (siehe EFNB-Frey/Ahmedi § 675j Rn. 7; MüKo/Jungmann § 675p Rn. 11)

- **a.A.: Autorisierung anfechtbar nach allgemeinen Regeln der §§ 119 ff. BGB**
  (siehe OLG Köln, Bsl.v. 21.3.16 – 13 U 223/15; OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24; BeckOGK/Zahrte § 675p Rn. 111; MüKo/Armbrüster § 119 BGB Rn. 22 u.a.)
  Arg: - ZDRL II und §§ 675c-676c BGB enthalten keine abschließende Regelung zu Folgen von Willensmängeln;
  - Schutz der Interessen des ZDL durch Ersatzanspruch nach § 122 BGB

3. Ansprüche des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB aufgrund von Pflichtverletzungen des Zahlers

- Grundsätze -

Weiterer Gegenstand der Diskussion in der jüngeren Rspr:
Grds. trägt nach § 675u BGB der ZDL das Risiko einer unautorisierten Zahlung, der Zahler kann aber dem ZDL aus § 675v Abs. 3 Nr. 2 BGB haften

§ 675v BGB: Haftung des Zahlers bei missbräuchl. Nutzung eines Zahlungsinstruments
Abs. 1: Verschuldensunabhängige Haftung des Zahlers, gedeckelt auf 50 Euro.
Abs. 3: Verschuldensabhängige und unbegrenzte Haftung des Zahlers
- bei betrügerischem Handeln des Zahlers (Nr. 1)
- bei vorsätzlicher/grob fahrlässiger Pflichtverletzung (Nr. 2).
Abs. 4: Kein Schadensersatz bei Nichtanwendung der starken Kundenauthentifizierung.

Ansprüche des ZDL aus § 675v BGB können den Ansprüchen des Zahlers aus § 675u BGB durch Aufrechnung oder nach § 242 BGB entgegengehalten werden,

BGH, Urt.v. 17.11.20 – XI ZR 249/19, BGHZ 227, 343; v. 5.3.24 – XI ZR 107/22, BGHZ 240, 23

3. Ansprüche des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB aufgrund von Pflichtverletzungen des Zahlers

Konstellationen von grob fahrlässigen Pflichtverletzungen des Zahlers

- betrifft Verstöße gegen Sicherheitspflichten des Zahlers nach § 675l I BGB
- sowie Verstöße gegen vereinbarte Bedingungen nach § 675l II BGB

Nach allg. Grundsätzen trägt ZDL die **Darlegungs-/Beweislast**, möglich ist aber **sekundäre Darlegungslast des Zahlers** für Umgang mit Sicherheitsmerkmalen

LG Kiel, Urt.v. 22.6.18 – 12 O 562/17; LG Mönchengladbach, Urt.v. 23.4.25 – 3 O 35/23

Kein Anscheinsbeweis für grob fahrl. Pflichtverletzung des Zahlers im Online-Banking wegen vielfältiger Angriffsmöglichkeiten, BGH, Urt.v. 26.1.16 – XI ZR 91/14, BGHZ 208, 331 (Folie 8)

Erfolg eines Phishing-/Schadsoftware-Angriffs noch kein Indiz für Pflichtverletzung,

OLG Dresden, Urt.v. 13.10.22 – 8 U 760/22; LG Oldenburg, Urt.v. 15.1.16 – 8 O 1454/15

Antivirenprogramm: grds. Pflicht des Zahlers zu aktualisiertem Virenschutz

EFNB-Nobbe § 675v Rn. 95; Beachtung von Sicherheitshinweisen nach Ziff. 7.2 Bed. Online-Banking Sparkassen

bzgl Mobilgeräten ist diese Pflicht nicht ohne weiteres bekannt, LG Berlin, Urt. 13.12.23 – 10 O 21/23

ZDL muss (im Einzelfall schwierigen) Beweis der Kausalität fehlenden Schutzes führen

EFNB-Nobbe § 675v Rn. 105; KG, Urt.v. 12.11.24 – 4 U 122/04; OLG Dresden, aaO.

3. Ansprüche des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB aufgrund von Pflichtverletzungen des Zahlers

Telefonische Weitergabe von TANs an einen Dritten im Allgemeinen:

- pflichtwidrig wegen Eröffnung unbefugten Zugriffs auf die TAN (§ 675l I 1 BGB) grobe Fahrlässigkeit wg schweren Sorgfaltsverstoßes; Pflichtwidrigkeit der Weitergabe von TANs außerhalb Online-Banking ist jedermann einleuchtend
  OLG Karlsruhe, Urt.v. 19.11.24 – 17 U 127/22; OLG München, Bsl.v. 4.9.23 – 19 U 1508/23
  OLG Naumburg, Urt.v. 22.5.24 – 5 U 11/24
- ebenso: Eingabe von TANs im Online-Banking auf telefon. Anweisung des Dritten
  OLG Frankfurt, Urt.v. 6.12.23 – 3 U 3/23; OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24

Sonderfall bei Call-ID-Spoofing/Kenntnis des Anrufers von kontobezogenen Daten?

- besondere Überrumpelungssituation und nachvollziehbarer Glaube des Nutzers daran, tatsächlich von seiner Bank angerufen zu werden
  -> grobe Fahrlässigkeit hier vereinzelt verneint worden
  LG Köln, Urt.v. 8.1.24 – 22 O 43/23; Maume BKR 23, 766 f.; Mattil/Fohrer BKR 23, 844 f.
  -> überwiegend wird grobe Fahrlässigkeit bejaht: Masche des Call-ID-Spoofing weithin bekannt; Nutzer sollten wissen, dass jede mündliche Weitergabe sorgfaltswidrig ist.
  OLG Frankfurt, aaO.; OLG Bremen, aaO.; OLG Naumburg, aaO.

3. Ansprüche des Zahlungsdienstleisters aus § 675v Abs. 3 Nr. 2 BGB aufgrund von Pflichtverletzungen des Zahlers

Eingabe von TANs auf gefälschten Online-Banking-Seiten (zB Phishing):

- grobe Fahrlässigkeit des Zahlers jdf bei ungewöhnlichen Umständen:
  zB ungewöhnliche URL; nicht veranlasste Aktionen, insbesondere Eingabe einer Vielzahl von TANs; ungewöhnliches Layout von Phishing-Nachricht oder Website
  OLG Frankfurt, Urt.v. 6.12.23 – 3 U 3/23; OLG München, Bsl.v. 4.9.23 – 19 U 1508/23; OLG Dresden, Urt.v. 13.10.22 – 8 U 760/22; LG Heilbronn, Urt.v. 16.5.23 – 6 O 10/23; LG Lübeck, Urt.v. 3.1.24 – 3 O 38/23
- anders uU bei Quishing: Nutzer hat weniger Kontrolle über die Anwahl der jeweiligen Seite; Scannen von QR-Codes wird auch von ZDL angeboten, s. Zahrte BKR 24, 938 ff.

Fehlende Prüfung der Daten des Zahlungsvorgangs bei TAN-Eingabe:

(insbes. bei Man-in-the-Middle-Angriff oder Social Engineering)
= zugl. Verstoß gg. vereinbarte Bedingungen (Ziff. 7.3 Bed. Online-Banking Sparkassen)

- grobe Fahrlässigkeit wird überwiegend bejaht, da naheliegende Sicherheitsmaßnahme
  OLG Brandenburg, Urt.v. 15.1.25 – 4 U 32/24; OLG Dresden, v. 6.4.23 – 8 U 578/22; OLG Bremen, Bsl.v. 15.4.24 – 1 U 47/23; OLG Oldenburg, Urt.v. 21.8.18 – 8 U 163/17; LG Hamburg, Urt.v. 13.5.24 – 318 O 57/23
- anders uU bei Anzeige unklarer Texte zur Freigabe durch ZDL (zB “Portalfreischaltung”)
  KG Berlin, Urt.v. 12.11.24 – 4 U 122/24; LG Heilbronn, Urt.v. 2.4.24 – Bm 6 O 378/23; AG Stuttgart, Urt.v. 30.1.25 – 1 C 3793/24; aA: OLG Naumburg, Urt.v. 30.10.24 – 5 U 35/24; LG Wuppertal, Urt.v. 19.2.25 – 8 S 59/24

4. Insbesondere: Folgen der Nichtanwendung einer starken Kundenauthentifizierung (SCA) nach § 675v Abs. 4 BGB

a. Allgemeines

§ 675v IV 1 BGB schließt Schersatzanspruch des ZDL gegen Zahler aus bei Nichtanwendung der starken Kundenauthentifizierung (SCA, § 55 ZAG iVm RTS-VO 2018/389)
(Ausnahme: betrügerisches Handeln des Zahlers, § 675v IV 3 BGB)

Beweislast: fehlende Anwendung der SCA durch den ZDL ist nach allgemeinen Grundsätzen vom Zahler zu beweisen, da ihm günstige Tatsache

siehe OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24

b. Anwendungsfälle

Behauptete Nichtanzeige von Zahlungsbetrag/-Empfänger bei Autorisierung:

- Anwendung des § 675v IV 1 BGB bei Nachweis der Nichteinhaltung der Vorgaben aus § 55 ZAG iVm Art. 5 II lit. a RTS-VO 2018/389

  siehe LG Halle, Urt.v. 23.6.23 – 4 O 133/22; dabei entgegen dem LG keine *durchgängige* Anzeige dieser Daten erforderlich, siehe OLG Naumburg, Urt.v. 10.1.24 – 5 U 83/23

(P) - wegen Nachweislast des Zahlers dürfte bei Bestreiten des ZDL dieser Beweis in der Praxis nur schwer zu führen sein
- Sachverständigenbeweis zur Frage der Anzeige der Daten des konkreten vergangenen Zahlungsvorgangs idR ungeeignet, siehe OLG Bremen, aaO.

4. Insbesondere: Folgen der Nichtanwendung einer starken Kundenauthentifizierung (SCA) nach § 675v Abs. 4 BGB

Fälle aufsichtsrechtl. Ausnahmen von Verpflichtung zur Anwendung der SCA

- umstritten ist die Anwendbarkeit des § 675v IV BGB in Fällen, in denen aufsichtsrechtlich keine Verpflichtung zur Anwendung der SCA besteht

Bsp.: dem eigentlichen missbräuchlichen Zahlungsvorgang vorausgehende Vornahme einer **Umbuchung vom Tagesgeld- auf Girokonto des Zahlers**, hier nach Art. 15 RTS-VO 2018/389 keine SCA erforderlich

- eA: - **§ 675v IV BGB nimmt keinen Bezug auf Bestehen einer Pflicht zur Anwendung der SCA**, keine Einschränkung zu Lasten des Zahlers;
  - Nichtanwendung der SCA ist Risiko des ZDL

  siehe BeckOGK/Hofmann § 675v Rn. 94; BeckOK/Schmalenbach § 675v Rn. 17a u.a.
- aA: - **Gleichlauf der zivil- und aufsichtsrechtlichen Vorgaben**

  so OLG Bremen, Bsl.v. 15.4.24 – 1 U 47/23; OLG Frankfurt, Urt.v. 6.12.23 – 3 U 3/23 u.a.

Weiteres Argument gg Entfallen des SchErs bei Nichtanwendung der SCA bei vorangegangenen Umbuchungen: **§ 675v IV BGB ist auf den schadensbegründenden Zahlungsvorgang iSv Abs. 1 und 3** bezogen, nicht auf vorherige Umbuchung

so OLG Bremen, aaO; OLG Naumburg, Urt.v. 30.10.24 – 5 U 35/24
iE ähnlich LG Nürnberg-Fürth, Urt.v. 29.6.23 – 6 O 5996/22 (Pflichtverl. des ZDL tritt zurück)
anders dagegen Schulte am Hülse/Steinsdörfer VuR 2025, 172, 174 ff.

4. Insbesondere: Folgen der Nichtanwendung einer starken Kundenauthentifizierung (SCA) nach § 675v Abs. 4 BGB

Nichtanwendung der SCA bei Zugriff auf Online-Banking:

teils umstritten ist, ob Nichtanwendung der SCA bei bloßer Anmeldung zum Online-Banking zum Ausschluss des SchErsatzes nach § 675v IV BGB führt

so LG Berlin, Urt.v. 28.8.24 – 37 O 120/22; Schulte am Hülse/Steinsdörfer VuR 25, 172, 174 ff.

die überwiegende Rspr lehnt dies ab:

siehe u.a. OLG Naumburg, Urt.v. 22.5.24 – 5 U 11/24; Urt.v. 30.10.24 – 5 U 35/24;
OLG Brandenburg, Urt.v. 15.1.25 – 4 U 32/24; LG Nürnberg-Fürth, Urt.v. 29.6.23 – 6 O 5996/22

Aufsichtsrechtl. Vorgaben zur Anwendung der SCA bei Zugriff auf Online-Banking:
§ 55 I Nr. 1 ZAG: Verpflichtung zum Verlangen der SCA bei Online-Zugriff auf Konto
§ 55 V ZAG: Regelung der Erfordernisse der SCA im Einzelnen in RTS-VO 2018/389
Art. 10 I RTS-VO 2018/389: Ausnahme von Verpflichtung zum Verlangen der SCA bei Online-Zugriff auf Konto, wenn keine sensiblen Zahlungsdaten offengelegt werden (Kontostand und Zahlungsvorgänge der letzten 90 Tage sind keine solchen Daten)
Ausnahme nach Abs. 2: SCA bei erstmaligem Zugriff und spätestens alle 180 Tage

-> bei bloßem **Zugriff auf Online-Banking daher wohl keine SCA erforderlich**

-> **Gleichlauf von Aufsichts-/Zivilrecht**: kein Schadensersatzausschluss nach § 675v IV BGB

-> iÜ dürfte § 675v IV BGB auf Nichtanwendung der SCA bei schadensbegründendem Zahlungsvorgang bezogen sein, nicht bei vorheriger Anmeldung (siehe vorherige Folie)

5. Ansprüche des Zahlungsdienstleisters aus § 122 BGB

Weiterer Schadensersatzanspruch des ZDL außerh. der §§ 675c-676c BGB:

- bei Zulassung einer Anfechtung der Autorisierung durch Zahler (siehe Folie 12) dann auch Schadensersatzhaftung des Zahlers aus § 122 BGB:
  siehe OLG Köln, Bsl.v. 21.3.16 – 13 U 223/15; OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24; BeckOGK-Zahrte § 675p Rn. 111
- Anspruch aus § 122 BGB nicht durch Regelung des § 675v BGB ausgeschlossen, da Materie der Anfechtung wegen Willensmängeln generell nicht durch die §§ 675c-676c BGB geregelt
- Anspruch aus § 122 BGB unterliegt auch nicht gesteigerten Verschuldensanforderungen und weiteren Einschränkungen des § 675v BGB
  siehe LG Köln, Urt.v. 16.10.15 – 30 O 330/14; OLG Bremen, aaO; BeckOGK-Zahrte, aaO
  aA Franke, BKR 25, 143, 144
- Anspruch aus § 122 BGB generell auf negatives Interesse gerichtet, dies entspricht dem Schaden des ZDL in Höhe des Überweisungsbetrages
- weitere Einzelheiten noch ungeklärt – Ausübung eines Anfechtungsrechts ist gegebenenfalls auch Auslegungsfrage im Einzelfall

6. Sorgfaltspflichtverletzungen des Zahlungsdienstleisters

a. Allgemeines

Auch bei Bestehen eines SchErs-Anspruchs gg Zahler aus § 675v BGB bzw. bei Nichtbestehen eines Erstattungsanspruchs des Zahlers aus § 675u ist **vollständige oder teilweise Haftungsverlagerung bei Pflichtverletzung des ZDL** möglich

Sorgfaltspflichtverletzungen des ZDL ggü dem Zahler können hier führen zu:

- **Kürzung von Schadensersatzansprüchen des ZDL aus § 675v BGB wegen Mitverschuldens des ZDL nach § 254** (bei nicht autorisierten Zahlungsvorgängen)
- uU **eigenen Schadensersatzanspr. des Zahlers (§ 280 I BGB iVm GiroV)**
  (zB auf teilweise Erstattung des abgebuchten Zahlungsbetrags, wenn täuschungsbedingte Autorisierung durch Sorgfaltspflichtverletzung des ZDL begünstigt wurde)

Kein grundsätzlicher Wegfall der Kausalität einer Pflichtverletzung des ZDL auch bei nachfolgender Auslösung des Zahlungsvorgangs durch Pflichtverletzung des Zahlers

wie hier OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24 (ggf. Frage des Mitverschuldens)

anders dagegen OLG Frankfurt, Bsl.v. 22.9.23 – 3 U 84/23 (überholende Kausalität)

6. Sorgfaltspflichtverletzungen des Zahlungsdienstleisters

b. Fallgruppen von Pflichtverletzungen des ZDL

Ausführung eines Zahlungsvorgangs unter Verletzung eines vereinbarten Tageslimits

Betragsobergrenze nach § 675k I BGB, siehe BGH, Urt.v. 29.11.11 – XI ZR 370/10, WM 12, 164

-> Kürzung von SchErs-Anspr. des ZDL; dabei ggf. Berücksichtigung von Mitverschulden des Zahlers

siehe OLG Bremen, Bsl.v. 15.4.24 – 1 U 47/24; OLG Naumburg, Urt.v. 22.5.24 – 5 U 11/24

Sorgfaltsverstoß des ZDL wegen Nichtanwendung der SCA (soweit nicht schon § 675v IV BGB)

-> uU iRd § 254 BGB zu berücksichtigen, so OLG Bremen, Bsl.v. 15.4.24 – 1 U 47/24

Lücken im Sicherheitssystem des ZDL: Sorgfaltswidrige Verwendung eines nicht dem Stand der Technik entsprechenden Online-Banking-Systems

so EFNB-Nobbe § 675v Rn. 114; MüKo-Zetzsche § 675v Rn. 58; OLG Karlsruhe, Urt.v. 19.11.24 – 17 U 127/22

- geht über Anwendung der Vorgaben der RTS-VO 2018/389 hinaus
- Darlegungs- und Beweislast beim Nutzer:
  - Umstand eines tatsächlich erfolgten unbefugten Zugriffs begründet keinen Anscheinsbeweis für Sorgfaltspflichtsverstoß des ZDL, da unbefugter Zugriff auch bei Einhaltung aller relevanter Sicherheitsstandards nicht auszuschließen
  - kein Anscheinsbeweis auch bei Nachweis des Nutzers, dass er pers. Sicherheitsmerkmale nicht weitergegeben hat und sein PC/Mobiltelefon nicht gehackt wurden
  - Anscheinsbeweis für Sorgfaltsverstoß folgt auch nicht aus späterer Umstellung des Online-Banking-Systems des ZDL

6. Sorgfaltspflichtverletzungen des Zahlungsdienstleisters

b. Fallgruppen von Pflichtverletzungen des ZDL (Forts.)

Verletzung von Hinweis- und Warnpflichten des ZDL bei Betrug und Missbrauch

Wann ist ZDL verpflichtet, den Zahler vor Missbrauch des Online-Kontos zu warnen?

- **BGH**: - Im bargeldlosen Zahlungsverkehr muss sich Bank **grds. nicht um Valutaverhältnis kümmern**, sondern sie wird nur zu technisch einwandfreier schneller Abwicklung tätig.
  - Ausnahme nach Treu und Glauben, wenn Umstände des Einzelfalls gebieten, vor Ausführung **Rückfrage beim Kunden** zu halten, um diesen vor Schaden zu bewahren.
    BGH, Urt.v. 6.5.08 – XI ZR 56/07, BGHZ 176, 281; v. 14.5.24 – XI ZR 327/22, BGHZ 240, 312

-> **Hinweispflicht bei massiven Anhaltspunkten für drohende Schädigung des Kunden** im bargeldlosen Zahlungsverkehr durch Straftat eines Dritten, siehe BGH aaO.

-> Hinweispflicht des ZDL bei **positiver Kenntniserlangung von unbefugten Kontozugriffen**
siehe OLG Bremen, Bsl.v. 19.5.21 – 1 W 4/21; LG Saarbrücken, Urt.v. 9.12.22 – 1 O 181/20
LG Aachen, Urt.v. 6.2.24 – 10 O 53/23

- Allgemeine Verpflichtung des ZDL zur **Echtzeit-Überwachung von Zahlungsvorgängen?**
  - BGH: grds. **keine allgemeine/ohne besondere Anhaltspunkte bestehende Pflicht zur Überwachung** von Kontobewegungen, siehe BGH, aaO.
  - **Transaktionsüberwachungsmechanismen aus Art. 2 RTS-VO 2018/389:**
    -> keine individuelle Echtzeitanalyse/Vorabkontrolle zur Verhinderung der Zahlungsausführung sondern **aufsichtsrechtliche Überwachung** zur Erkennung nicht autorisierter Vorgänge
    so EBA, Single Rulebook, Question ID 2018_4090; Casper/Terlau § 1 ZAG Rn. 520;
    OLG Bremen, Bsl.v. 30.8.24 – 1 U 32/24; aA Linardatos BKR 21, 665, 675

IV. Bewertung/Ausblick

jüngere Rechtsprechung zeigt differenziertes Bild zur Haftung des Zahlers bzw. des ZDL in Betrugs-/Missbrauchsfällen im Online-Banking

signifikantes Betrugsproblem spiegelt sich in Anzahl streitiger Verfahren

These: Problemen von Betrug und Missbrauch im Online-Banking ist nicht in erster Linie durch Ausweitung der Haftung von entweder ZDL oder Zahlern zu begegnen, sondern durch (v.a. aufsichtsrechtliche) Vorgaben zur Betrugsprävention

- Vorgaben zur Stärkung der Betrugsprävention durch ZDL könnten Verfügbarkeit des Anscheinsbeweises stärken

- Einführung und Fortentwicklung neuer Zahlungsinstrumente besser vorab anhand konkretisierter aufsichtsrechtlicher Vorgaben (zB Überarbeitung der RTS-VO) zu überprüfen statt lediglich ex post im Rahmen der zivilrechtlichen Haftung

- Inhalt und Umfang der Sorgfaltspflichten des ZDL noch weiterzuentwickeln, insbesondere durch (v.a. aufsichtsrechtliche) Vorgaben, die dann auch für das Haftungsregime allgemeinverbindlich klarstellend zu beachten wären

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Ole Böger, 27.06.2025

Richter am Hanseatischen Oberlandesgericht in Bremen
Am Wall 198
28195 Bremen