
Chancen, Risiken, Probleme von Zahlungsinstrumenten. Perspektive des Verbraucherschutzes.

13.10.2026 | 5. Verbraucher:innentalk | AKNÖ

Petra Leupold



AGENDA

1. Digitalisierung des Zahlungsverkehrs
2. Aktuelle Problemfelder aus der Praxis
3. Bargeld: Annahmepflicht / Aufschlag
4. Phishing-Betrugsfälle
5. Unzulässige Gebühren – Zugang zum Recht
6. Ausblick: Agentic Commerce/Payments

● Digitalisierung des Zahlungsverkehrs

1.0 Bargeld

2.0 Online Banking / Kartenzahlung

3.0 Wallets / Digitaler Euro

4.0 Agentic Payments

● ● Bargeld vs bargeldloser Zahlungsverkehr

- **EZB-Study on the payment attitudes of consumers in the euro area (SPACE), 12/2024**
 - → 38% in Ö bevorzugen Bargeld als Zahlungsmethode (höchster Wert EU-weit)
 - → 39% in Ö bevorzugen Kartenzahlung / Cashless-Payment
- Vorteile von Bargeld aus Verbrauchersicht
 - inklusiv wirkendes Zahlungsmittel, das ohne technische Systeme unmittelbar bilateral abgewickelt werden kann und auch Personengruppen einschließt, die nicht über digitale Zahlungsmittel verfügen → vgl EG 14 EU-Bargeld-VO-E: sozialpolitische Funktion zur finanziellen Inklusion für vulnerable Gruppen
 - „Recht auf Anonymität“ vs Nachverfolgbarkeit von Konsumverhalten und Zahlungsflüssen durch Drittanbieter
 - funktioniert auch in Blackout-Szenarien und bei Systemabstürzen von Bezahlssystemen
 - ermöglicht es vielen Menschen, ihre Ausgaben besser zu überblicken und zu kontrollieren

Annahmepflicht von Bargeld vs cashless only

- Privatrechtliche Annahmepflicht de lege lata?
 - Bsp 1: „Cards only“ bei Mpreis-Markt in Innsbruck 2023
 - Bsp 2: „Cashless only“-Testphase in Billa Filiale am WU-Campus 2024
- Zahlungsmittelhierarchie von staatlichen und nichtstaatlichen Zahlungsmitteln: Annahmepflicht von Bargeld als dispositive Norm (§ 907a Abs 1 S 1 ABGB)
- Wahlrecht des Verbrauchers zwischen Barzahlung und Banküberweisung (§ 6a Abs 1 S 1 KSchG); vgl auch § 15 Abs 3 MRG zugunsten des Mieters
- hA: Unzulässigkeit des Ausschlusses von Bargeld in AGB jedenfalls im Präsenzgeschäft (§ 879 Abs 3 ABGB, § 864a ABGB) → arg Aushöhlung des Status des Euro als gesetzliches Zahlungsmittel



Annahmepflicht von Bargeld vs cashless only II

- vgl die stRsp, wonach ein Ausschluss von Bargeldzahlungen und Überweisungen und die Vereinbarung des Lastschriftverfahrens als einzig zulässiger Zahlungsart unzulässig ist
- OGH 4 Ob 50/00g (Mobilfunktarif), 7 Ob 263/07p (Lebensversicherung), 1 Ob 124/18v (Paylife-Kreditkarten), 9 Ob 38/19g (Pay-TV-Anbieter); 7 Ob 151/07t
- Art 4 Abs 3 EU-Bargeld-VO-E: währungsrechtliche Annahmepflicht von Euro-Banknoten und -Münzen als gesetzliche Zahlungsmittel zum vollen Nennwert (vgl EuGH Rs Hessischer Rundfunk, C-422/19)
 - Reichweite der Ausnahmen von der Annahmepflicht strittig (Privatautonomie)
 - → Art 5 Abs 1 lit b: „Vereinbarung“ eines anderen Zahlungsmittels – AGB-Ausschluss zulässig?

● ● Zulässigkeit von Bargeldaufschlägen?

- Bsp: ÖBB-Aktion „Karte zücken – Preis drücken“
- keine ausdrückliche gesetzliche Regelung zur (Un-)Zulässigkeit von Aufschlägen
- Verbot von Entgelten für die Nutzung bestimmter Zahlungsinstrumente (Surcharging-Verbot (§ 56 Abs 3 ZaDiG 2018 = § 27 Abs 6 ZaDiG aF); Ermäßigungen bei Nutzung bestimmter Zahlungsinstrumente sind zulässig (Normzweck: Preistransparenz, Schutz der Nachfrage-Entscheidung)
- → § 56 Abs 3 ZaDiG ist nicht auf Bargeldzahlung anzuwenden (§ 3 Abs 3 Z 1 leg cit)
- Art 4 Abs 3 Bargeld-VO-E: Entgeltverbot zum Schutz von Bargeld in seiner Funktion als gesetzliches Zahlungsmittel

Betrug im bargeldlosen Zahlungsverkehr

- Phishing-Betrug ist ein Massenphänomen geworden, die Beschwerdefälle nehmen kontinuierlich zu (vgl. EBA Consumer Trends Report 2024/25, EBA/EZB Report on Payment Fraud 2025).
- Schadenssumme von 115,4 Mio EUR im Jahr 2025 = Anstieg um 17,6% zum Vorjahr; bei betrügerischen Überweisungen Anstieg der Schäden um 74% gegenüber 2022 (OeNB).
- Die Methoden der Täter werden zunehmend professioneller und sind von echter Bankkommunikation kaum noch zu unterscheiden.
- Betrugsfälle gehen vermehrt auf Social Engineering und KI-Angriffe zurück.
- Opfer von Phishing-Angriffen sind nicht nur weniger digitalaffine oder ältere Risikogruppen, Durchschnittsalter 48 Jahre (BMASGPK-Bericht).
- Die Schadenssummen steigen, der Durchschnittsschaden beträgt 4.333 EUR (BM: 8.500 EUR bei Überweisungen, höhere Schäden bei Instant Payments).
- Rd 2 Drittel der Fälle betreffen Kartenzahlungen, rd 1 Drittel Überweisungen.
- In 77 % der Fälle saß mindestens ein Empfänger im Ausland.

● ● Fallbeispiel 1 – nicht autorisierte Zahlung

Registrierung eines Betrügergeräts

- Das Opfer erhält eine SMS – oft im echten Nachrichtenverlauf der Bank – mit der Aufforderung, Zugangsdaten zu bestätigen und der Drohung einer Sperre am nächsten Tag. Der Link führt auf eine perfekt nachgebaute Bankseite. Mit den eingegebenen Zugangsdaten stellen die Betrüger eine Login-Anfrage, die das Opfer freigibt, im Glauben, sich selbst einzuloggen. Danach beantragen sie die Registrierung ihres eigenen Geräts. Das Opfer bestätigt per mTAN oder Push, ohne zu merken, dass es das Gerät der Täter freischaltet. Die Täter haben dann uneingeschränkten Zugriff, erhöhen Limits und zahlen innerhalb weniger Minuten. Eine sofortige Sperre durch das Opfer kommt meist zu spät.
- **Rechtliche Einordnung → nicht autorisierte Zahlung:** Die Bank trägt den Schaden.
- Erstattungsanspruch des Kunden nach § 67 ZaDiG → die Bank muss bis Ende des folgenden Bankarbeitstags den Kontostand berichtigen (Ausnahme: begründeter Betrugsverdacht und unverzügliche schriftliche Meldung an FMA)



Fallbeispiel 1 – nicht autorisierte Zahlung II

- **Problem:** Banken erstatten Schäden oft zunächst nicht und berufen sich dabei auf ein angeblich grobes Verschulden der Kundinnen.
- → keine Aufrechnungsmöglichkeit der Bank mit Schadenersatzansprüchen gegen den grob fahrlässigen Kunden (hL, Rsp)
 - OGH 8 Ob 106/20a VbR 2021/78
 - Schlussanträge des GA in der Rs C-70/25, Tukowiecka, VbR 2026/30, wonach es dem ZDL nach Art 73 f PSD II 2015/2366 verwehrt ist, die unverzügliche Erstattung unter Berufung darauf abzulehnen, dass der Zahler seinen Pflichten grob fahrlässig nicht nachgekommen ist; der ZDL muss seinen Schadenersatzanspruch gem Art 74 PSD II (§ 68 Abs 3 ZaDiG) nach der erfolgten Erstattung vielmehr klageweise durchsetzen, falls der Zahler diesen nicht anerkennt.
- Musterprozesse und Sammelklagen des VKI → Ergebnis: in allen Fällen wurden die Ansprüche der Betroffenen nach Einbringung der Klage und vor Ergehen eines Urteils erfüllt
- Anhängige Verbandsverfahren gegen die Geschäftspraktik von Banken, in Fällen nicht autorisierter Zahlungsvorgänge eine Berichtigung des Kundenkontos unter Berufung auf Schadenersatzansprüche abzulehnen

● ● Fallbeispiel 2 – autorisierte Zahlung

Vom Betrüger angelegte, vom Zahler selbst freigegebene Überweisungen

- Ein erster Phishing-Angriff gibt den Betrügern Zugang zum Konto; sie erstellen Umbuchungen vom Sparkonto, Limiterhöhungen und Überweisungsaufträge. Im zweiten Schritt ruft ein angeblicher Bankmitarbeiter an und behauptet, verdächtige Zugriffe bemerkt zu haben. Das Opfer soll die Aufträge per Push-Bestätigung „stornieren“ und gibt diese in Wahrheit frei.
- **Rechtliche Einordnung:** autorisierte oder nicht autorisierte Zahlung? (str)
 - → entscheidend für die Risikoverteilung zwischen Bank und Kunden
 - bei autorisierter Zahlung: kein Erstattungsanspruch des Kunden nach § 67 ZaDiG, Aufwandsersatzanspruch der Bank (§ 1014 ABGB) → Schaden liegt beim Verbraucher
 - für autorisierte Zahlung: OGH 7 Ob 95/24g EvBl 2025/111 (krit Burtscher) = ZFR 2025/8 (zust Fletzberger/Falke); OLG Linz 1 R 45/25f VbR 2026/64; Fletzberger/Falke, ZFR 2024/160; aA Kriegner, RdW 2025/560; Burtscher, Zahlungsverkehr und Zivilrecht (2026) 170 ff, arg Normzweck der §§ 67 f ZaDiG, technische Kompromittierung, „cheapest insurer“



Transaktionsmonitoring

- Die Bank muss nach Art 2 DelVO (EU) 2018/389 ein ausreichend wirksames FTM-System implementieren, das (autorisierte und nicht autorisierte) betrügerische Zahlungen erkennt; bei Verdacht muss die Zahlung blockiert und beim Kunden rückgefragt werden.
- OLG Linz 1 R 45/25f VbR 2026/64: Die Bank haftet dem Zahler bei Implementierung eines unzureichenden Transaktionsüberwachungssystems wegen schuldhafter Verletzung vertraglicher Schutz- und Sorgfaltspflichten / Schutzgesetzverletzung (§ 1311 ABGB).
- Beim automatisierten Abgleich der Höhe des Zahlungsbetrags mit der bisherigen Umsatzstruktur des Zahlers ist nicht isoliert auf jede einzelne Überweisung abzustellen, bei mehreren Transaktionen in kurzer Zeit ist vielmehr die Gesamtheit der Zahlungen maßgeblich. Es ist daher nicht nur zu prüfen, ob der kumulierte Betrag sämtlicher Überweisungen vom bisherigen Zahlungsverhalten abweicht, sondern auch, ob es Auffälligkeiten in Bezug auf die Anzahl der Überweisungen gibt (hier: 41 Überweisungen iHv rd EUR 200.000 von 2 Konten in einem Zeitraum von 1,5 Std).
- Mitverschulden (§ 1304 ABGB), wenn auch dem Zahler iZm der Bekanntgabe seiner Verfügernummer und der Freigabe von von unbekannten Dritten angelegten Überweisungen ein grob sorgfaltswidriges Verhalten vorzuwerfen ist.
- Anhängige Verbandsverfahren zur Unterbindung von Verstößen gegen die Pflicht zum Transaktionsmonitoring.



Ausblick: PSR/PSD III

- Stand: vorläufige Einigung im Trilog 11/2025, Bestätigung im ECON-Ausschuss des EP 05/2026, Veröffentlichung im EU-Amtsblatt voraussichtlich Ende 2026/2027
- Ziele: verbesserter Schutz der Nutzer vor Betrug und Datenmissbrauch
- Verschärfung des Haftungsregimes der Bank bei missbräuchlichen Zahlungen
 - Ausweitung des Begriffs der nicht autorisierten Zahlung
 - Geben sich Betrüger als Mitarbeiter des Zahlungsdienstleisters aus, gelten vom Kunden ausgelöste Transaktionen als „nicht autorisiert“, sofern das Opfer Anzeige erstattet, die Bank unverzüglich informiert und nicht grob fahrlässig gehandelt hat (Art 59) → Auslegung des Begriffs der groben Fahrlässigkeit wird zentral (bislang nur Konkretisierung durch die nationale Rsp)
- Allgemeine Pflicht zur Überprüfung der Übereinstimmung von IBAN und Kontoinhaber vor Ausführung von Überweisungen („verification of payee“, seit 10/2025 bei Echtzeitüberweisungen nach der SEPA-VO)
- Freischaltung von Endgeräten und Erhöhung von Zahlungslimits
 - Verwendung einer starken Kundenauthentifizierung
 - 4-stündige Delay / Cooling-off-Periods nach Limiterhöhung (Art 51)

Fazit

- Phishing-Betrug ist aus Verbrauchersicht aktuell das größte Problemfeld im digitalen Zahlungsverkehr.
- Besonders problematisch: erhebliche Professionalisierung, rasche Weiterentwicklung und Skalierung der Angriffsmethoden durch verstärkten Einsatz von Social Engineering und KI-Unterstützung, Maximierung des Schadenspotentials für Verbraucher:innen.
- Das geltende Recht sieht eine grundsätzlich kundenfreundliche Risikoverteilung zwischen Bank und Kunden vor, allerdings gibt es in der Praxis Probleme bei Rechtsdurchsetzung und Rechtssicherheit.
- Erforderlich ist ein Bündel an Maßnahmen zur Bekämpfung von Phishing:
 - Betrugsprävention durch Informationskampagnen und Sensibilisierung der Bürger:innen → Warnsignale einordnen, Zahlungsentscheidungen kritisch hinterfragen, nicht unter Druck setzen lassen
 - Institutioneller Schulterschluss und effektiver Informationsaustausch von Aufsichtsbehörden, Strafverfolgungsbehörden, Beratungsstellen und Verbraucherorganisationen → Start „Aktion 10 Tage gegen Phishing“
 - Verbesserte Durchsetzung von Verbraucheransprüchen (effective redress) und gezielte Verfahren zur Klärung offener Rechtsfragen (strategic litigation, Rechtssicherheit)
 - Verbesserung der Transaktionsmonitoringsysteme zur Erkennung und Verhinderung von Betrug



Unzulässige Gebührenklauseln

- **Bsp 1: Bearbeitungsentgelt** von 1,65% des autorisierten Betrags bei Fremdwährungs- und grenzüberschreitenden Transaktionen in Kreditkarten-AGB → Verstoß gegen § 6 Abs 3 KSchG, weil dem Verbraucher eine Überprüfung der Überschneidung mit anderen vereinbarten Entgelten (hier: Währungsumrechnungsentgelte) nicht möglich ist (OGH 5 Ob 191/24k VbR 2026/39)
- **Bsp 2: „Information** über die Nichtdurchführung von Zahlungstransaktionen, zB Daueraufträge, SEPA Lastschriften, ... EUR 8,30“ → Verstoß gegen § 6 Abs 3 KSchG: Nur eine zulässige Ablehnung eines Zahlungsauftrags bietet eine Basis für die Verrechnung des Entgelts (§ 73 Abs 1, § 56 Abs 1 ZaDiG); die Klausel ermöglicht die Einbeziehung beliebiger anderer Transaktionen in ihren Anwendungsbereich (OLG Wien 4 R 89/22w VbR 2023/101)
- **Bsp 3: „Kartensperre EUR 40“** → Entgeltpflicht verstößt gegen § 56 Abs 1 ZaDiG, § 6 Abs 3 KSchG
- **Bsp 4: „Nachbestellung** auf Kundenwunsch (zB Namensänderung) EUR 15,00“ → Verstoß gegen § 6 Abs 3 KSchG, weil nicht jede Ausstellung einer Ersatzkarte „auf Kundenwunsch“ zu einer Entgeltpflicht führen darf (OGH 10 Ob 60/17x VbR 2018/51)

Unzulässige Gebührenklauseln II

- **Rechtsfolgen unzulässiger Gebührenklauseln**
 - Anwendbarkeit der stRsp des EuGH / OGH
 - Ersatzloser Entfall der unzulässigen Klausel, Unzulässigkeit geltungserhaltender Reduktion/ergänzender Vertragsauslegung, keine Anwendbarkeit dispositiven Rechts
 - → **Rückzahlungsansprüche der Kunden** hinsichtlich der auf Basis der unwirksamen Klauseln bezahlten Entgelte
 - keine kenntnisunabhängige Verjährung (Effektivitätsgrundsatz) → Rückzahlungsansprüche verjähren (frühestens) in 30 Jahren ab Zahlung
 - **Problem:** keine Kenntnis der Verbraucher:innen von Unzulässigkeit der Gebühren / Rückzahlungsansprüchen → keine Geltendmachung, keine Kompensation
 - de lege lata keine Informationspflichten der Bank
 - bei Geltendmachung und Verweigerung der Rückzahlung → kein ausreichender Zugang zum Recht insbesondere bei Bagatell- und Streuschäden

● ● Ausblick: Agentic Commerce / Payments

- Verbraucher:innen lassen sich bei Konsumententscheidungen zunehmend von KI-Chatbots unterstützen (Produkt- und Preisvergleich)
- Händler:innen nutzen KI bei Bonitätsprüfungen („Buy Now Pay Later“, siehe VKrG 2026) und der Auswahl von Zahlungsarten (zur Vereinbarkeit mit Art 22 DSGVO siehe die anhängige Rs VKI/Universal Versand, EuGH C-568/25)
- Agentic Commerce/Payments: KI-Agenten wickeln den vollständigen Bestell- und Bezahlvorgang autonom ab (AI-ready tokens) – Agenten als neue Intermediäre auf Nachfragerseite
 - aktuell (noch) keine Praxisrelevanz in Ö, aber erste Verbandsverfahren zu Produkten von US-Anbietern anhängig
 - wirft komplexe verbraucher- und gesellschaftspolitische sowie rechtliche Fragen auf
 - → vgl GA SVRV „Verbraucherschutz im Agentic Commerce“ 10/2026, ELI-Model-Rules on Digital Assistants for Consumer Contracts

● ● Ausblick: Agentic Commerce / Payments II

- **Chancen:**
 - Senkung von Transaktionskosten (Suche und Suchradius, Information, Anbahnung, Kontrolle)
 - Optimierung von Konsumentscheidungen, Schutz vor Kostenfallen und Betrug
 - Reduktion von Impulskäufen („Friction by Design“, Verzögerung im Kaufprozess)
 - Abbau von Informationsasymmetrien zwischen Händler und Verbraucher
 - Potential für sustainable consumption by design (Agenten als „choice engines“)
 - Bündelung von Nachfrage → kollektive Verhandlungsmacht

● ● Ausblick: Agentic Commerce / Payments III

- **Risiken:**
 - Autonomierisiko: Haftung für unvorhersehbare Handlungen von Agenten
 - Manipulationsrisiken: Manipulation durch und von Agenten (agentenspezifische Dark Patterns)
 - Autonomieverlust, Kontrollverlust über Kaufentscheidungen (Delegation)
 - Informationsasymmetrien im Verhältnis Verbraucher – Anbieter von KI-Agenten
 - Intransparenz algorithmischer Systeme / Black-Box-Effekte
 - Wettbewerb: Konkurrenz um Auswahl durch Agenten → neue Gatekeeper-Strukturen („Foreclosure by Agents“), Marktkonzentration durch Netzwerk- und Lock-in-Effekte (siehe Plattformökonomie)
 - Langfristig: negative Auswirkungen auf individuelle Entscheidungs- und Kaufkompetenzen



Fazit

-
- Agentic Commerce bietet sowohl Chancen als auch Schadenspotential für Verbraucher:innen und hat potentiell erhebliche Auswirkungen auf Markt, Wettbewerb und Gesellschaft.
 - Die rasant voranschreitende technologische Entwicklung wirft normative Grundsatzfragen für Verbraucher-, Wirtschafts- und Gesellschaftspolitik auf, die einer breiten intra- und interdisziplinären Diskussion unter Einbindung von Sozial-, Rechts- und Wirtschaftswissenschaften sowie der Zivilgesellschaft bedürfen (Vorsorgeprinzip, Bewahrung rechtspolitischer Handlungsspielräume).
 - Der geltende Verbraucherrechtsrahmen ist auf seine „agent-readiness“ dahingehend zu prüfen, ob ausreichender Schutz vor Risiken und Schäden durch KI-Agenten gewährleistet ist (Produkthaftungsregime, DSA und DMA, Verbrauchervertrags- und Haftungsrecht, Zahlungsdiensterecht, Lauterkeitsrecht).



Vielen herzlichen Dank für Ihre Aufmerksamkeit

Dr. PETRA LEUPOLD, LL.M. (UCLA)
Leitung Intervention

petra.leupold@vki.at
+ 43 676 852270 329

Verein für Konsumenteninformation
Linke Wienzeile 18
1060 Wien | Vienna | Austria

www.vki.at | www.konsument.at |
www.verbraucherrecht.at

ZVR-Zahl 389759993