Missbrauch von Zahlungskarten zwischen Aufsichtsrecht, Zivilrecht und Vertragsgestaltung*)

Bernhard Burtscher

Der Beitrag untersucht die gesetzliche Risikoverteilung zwischen Kartenaussteller und Kunde beim Missbrauch von Zahlungskarten. Besondere Bedeutung kommt der aufsichtsrechtlichen Pflicht zur starken Kundenauthentifizierung und dem zivilrechtlichen Haftungsprivileg bei fehlender starker Kundenauthentifizierung zu. Darauf aufbauend werden mögliche vertragliche Gestaltungsspielräume für Kartenaussteller beleuchtet.

Stichwörter: Zahlungskarten, starke Kundenauthentifizierung, Autorisierung, Schadenersatz, NFC-Zahlungen, Kleinbetragszahlungsinstrumente, Klauselkontrolle.
JEL-Classification: K 12, K 13, K 23, K 24, K 41.

https://doi.org/10.47782/oeba202201002001

The article examines liability for unauthorised payment transactions with payment cards under Austrian law. Special regard is paid to the rules on strong customer authentication and their implications for private law. Against this backdrop, the article further investigates potential room for contractual agreements between payment service providers and their customers.

1. Einleitung

Wird eine Zahlungskarte (Debit- oder Kreditkarte) von einem unbefugten Dritten zur Abhebung oder Zahlung verwendet, stellt sich die Frage nach der Verteilung des Missbrauchsrisikos. Da der Dritte meist nicht greifbar ist, taucht diese Frage in der Regel zunächst zwischen dem Kunden (Karteninhaber) und seinem Zahlungsdienstleister (Kartenaussteller[1]) auf.[2]

Sie wurde schon im „alten" Zahlungsverkehrsrecht, das noch weitgehend allgemeines Zivilrecht war, als „*schwieriges und umstrittenes Problem*" empfunden.[3] Das „neue" europarechtlich determinierte Zahlungsverkehrsrecht hat die Risikoverteilung im ZaDiG grundlegend neu geregelt und ein mehrstufiges[4] – aber wie sich zeigen wird, nicht minder auslegungsbedürftiges – Risikoverteilungsmodell an der Schnittstelle von Aufsichts- und Zivilrecht geschaffen.

2. Grundlagen der Risikoverteilung

2.1. „3-Stufen-Modell" (§§ 67 f ZaDiG)

Auf der ersten Stufe dieses Modells trägt der Kartenaussteller das Missbrauchsrisiko. Hat der Kunde den Zahlungsvorgang nicht „autorisiert" (dem Zahlungsvorgang also nicht gemäß § 58 ZaDiG zugestimmt), schuldet er dem Kartenaussteller keinen Aufwandersatz (§ 67 Abs 1). Das entspricht der hA zum „alten" Zahlungsverkehrsrecht, die mangels wirksamer Weisung des Kunden im Rahmen des Girovertrags sowohl einen Aufwandersatzanspruch des Kartenausstellers als auch eine Risikohaftung des Kunden nach § 1014 ABGB verneinte.[5]

Im „neuen" Zahlungsverkehrsrecht trägt der Kartenaussteller auch dann das Missbrauchsrisiko, wenn der Kunde die Zahlungskarte verloren hat oder sie ihm gestohlen worden ist, solange den Kunden daran kein Verschulden trifft (§ 68 Abs 1). Damit ist der zum alten Recht verbreiteten „Sphärentheorie", wonach der Kunde verschuldensunabhängig das Verlust- und Diebstahlsrisiko trage, weil es seiner Sphäre zuzurechnen sei,[6] der Boden entzogen.[7] Wird dem Kunden etwa eine mitgeführte Zahlungskarte gestohlen, steht er somit besser, als wenn ihm mitgeführtes Bargeld oder der Schlüssel zu seinem Bankschließfach gestohlen wird.

Das ist keineswegs selbstverständlich,[8] im Verbrauchergeschäft dennoch grundsätzlich zwingend (§ 55; S aber 4.). Während der OGH vor Inkrafttreten des ZaDiG noch AGB-Klauseln akzeptierte, die dem Karteninhaber verschuldensunabhängig das Risiko des Missbrauchs gestohlener oder verlorener Zahlungskarten zuwiesen, weil es sich in seiner Sphäre ereigne,[9] lässt das „neue" Zahlungsverkehrsrecht für solche Vereinbarungen keinen Raum mehr.[10]

Photo: Universität Liechtenstein

Dr. *Bernhard Burtscher* ist Universitätsassistent am Institut für Zivil- und Zivilverfahrensrecht der Wirtschaftsuniversität (WU) Wien; e-mail: Bernhard.Burtscher@wu.ac.at

*) Die Veröffentlichung dieses Beitrags wurde ermöglicht durch die Vergabe eines Forschungsauftrag über das Forum Bankrecht der BWG. Wir danken unseren Mitgliedern, die dieses Forum materiell unterstützen.

1) Der Kartenaussteller ist gem § 1 Abs 2 Z 5 ZaDiG ein Zahlungsdienstleister.
2) Zur Risikoverteilung zwischen Kartenaussteller und Vertragsunternehmen S etwa 4 Ob 133/14h.
3) *Koziol*, ÖBA 2001, 250 (254); stellvertretend für die Diskussion *Fellner*, Bankomatkarte 33 ff; *Vogel*, Mißbrauch von Kreditkarten 175 ff.
4) *Harrich*, ZaDiG 291.
5) 2 Ob 133/99v ÖBA 2001, 250 (*Koziol*); 4 Ob 179/02f; 3 Ob 248/06a; 10 Ob 70/07b; *Graf*, ÖBA 2007, 531 (533 f); dagegen aber *Koziol*, ÖBA 2001, 250 (254); ausf *Iro/Koziol*, ÖBA 2003, 129 (130 ff); diff *Vogel*, ÖBA 2001, 767 (773 f).
6) *Graf*, Telebanking 18; *Iro/Koziol*, ÖBA 2003, 129 (134); *Kurschel*, ecolex 1990, 79 (80).
7) *Kurz*, ecolex 2017, 836 (838).
8) Krit etwa bereits *Graf*, Telebanking 28 f.
9) 1 Ob 598/79, 3 Ob 530/91; 2 Ob 133/99v ÖBA 2001, 250 (*Koziol*); 3 Ob 248/06a; 10 Ob 70/07b; 6 Ob 233/15f.
10) Problematisch sind daher auch sogenannte „Kfz-Klauseln: 1 Ob 88/14v; dagegen aber 6 Ob 120/15p; krit zu dieser Entscheidung *Kurz*, ecolex 2017, 836 (838); S auch *Jungmann* in MüKo, BGB8 § 675l Rn 32 mwN.

Die „*Feinsteuerung*“[11] übernimmt ab der zweiten Ebene des Risikoverteilungsmodells vielmehr das Schadenersatzrecht. Der Kartenaussteller erwirbt ohne Autorisierung zwar keinen Aufwandersatzanspruch gegen den Kunden. Der Kunde haftet ihm aber schadenersatzrechtlich für den getätigten Aufwand (§ 68 Abs 1), wenn er schuldhaft eine der folgenden Pflichten verletzt: die in den Ausgabe- und Nutzungsbedingungen festgelegten Pflichten (§ 63 Abs 1); die Pflicht, den Verlust, Diebstahl oder Missbrauch der Zahlungskarte sofort dem Kartenaussteller anzuzeigen (§ 63 Abs 2) oder die Pflicht, personalisierte Sicherheitsmerkmale (und nach hA auch die Zahlungskarte selbst![12]) vor unbefugtem Zugriff zu schützen (§ 63 Abs 3).

So wird den Kunden etwa am Verlust der Karte häufig ein Verschulden treffen, was seine Haftung begründen kann.[13] Demgegenüber scheidet eine Haftung bei Diebstahl der Karte (und umso mehr bei einem Raub) im Regelfall aus. Der OGH wirft einem Kunden etwa keine Pflichtverletzung vor, wenn er eine Bankomatkarte in seine Geldbörse steckt und diese obenauf im Hauptfach eines verschlossenen Rucksacks verstaut und sie so in der U-Bahn transportiert. Der Kunde müsse auch beim Bargeldbezug am Bankomaten keine „Verrenkungen“ machen, um das „Ausspähen“ seiner PIN zu verhindern.[14]

Auch wenn der Kunde aber die Zahlungskarte leicht fahrlässig verliert, ist seine Haftung zweifach beschränkt. Erstens haftet er gar nicht, wenn der Verlust der Zahlungskarte für ihn nicht bemerkbar war (§ 68 Abs 2 Z 1).[15] Dieser eigenartige Haftungsausschluss greift nach hA nicht nur bei unabwendbaren Ereignissen (etwa Ohnmacht[16]); vielmehr soll die Bemerkbarkeit einen (weiteren) Sorgfaltsverstoß voraussetzen.[17] Der Kunde haftet demnach nur, wenn er zunächst die Zahlungskarte fahrlässig verliert und sich dann etwa trotz Verdachtsmomenten nicht vom Vorhandensein der Karte überzeugt. Selbst die Haftung dieses doppelt fahrlässigen Kunden ist aber zweitens mit € 50 begrenzt.[18]

Damit bringt das „neue“ Zahlungsverkehrsrecht einen Paradigmenwechsel: Musste der Kunde nach allgemeinem Zivilrecht den Schaden selbstverständlich schon bei leichter Fahrlässigkeit zur Gänze tragen (§ 1294 ABGB),[19] trägt er nunmehr nur den vergleichsweise geringen Selbstbehalt von € 50. Eine volle Schadenersatzpflicht des Kunden kann erst auf der dritten Stufe des Risikoverteilungsmodells bei grobem Verschulden eingreifen (§ 68 Abs 3), wobei hier immer noch eine Mäßigung durch den Richter in Betracht kommt (§ 68 Abs 4).[20]

Damit wird die – nach nationalem Recht zu ziehende (ErwG 72 zur PSD II) – Grenze zwischen leichter und grober Fahrlässigkeit zum neuralgischen Punkt des Risikoverteilungsmodells. Die damit einhergehenden heiklen Abgrenzungsfragen sollen hier nicht vertieft werden.[21] Nimmt man die Beschränkung der Kundenhaftung auf Fälle „*auffallender Sorglosigkeit*“ (§ 1324 ABGB) ernst, wird das „neue“ Zahlungsverkehrsrecht aber eine erhebliche Besserstellung des fahrlässigen Kunden gegenüber dem allgemeinen Zivilrecht bringen.[22]

2.2. „4. Stufe“: Haftungsprivileg nach § 68 Abs 5 ZaDiG

Die Zweite Zahlungsdiensterichtlinie (Payment Services Directive, PSD II) geht freilich auf der vierten Stufe des Risikoverteilungsmodells noch einen Schritt weiter. Hat der Kartenaussteller keine starke Kundenauthentifizierung verlangt oder akzeptiert der Zahlungsempfänger oder dessen Zahlungsdienstleister keine starke Kundenauthentifizierung, haftet der Kunde überhaupt nur bei betrügerischer Absicht (§ 68 Abs 5).[23] Damit befreit § 68 Abs 5 auch den grob sorglosen und selbst den vorsätzlich handelnden Kunden von der Haftung.[24]

Die „starke Kundenauthentifizierung“ ist der neue „Goldstandard“ zur „Authentifizierung“. „Authentifizierung“ ist die Überprüfung der Identität des Kunden und der personalisierten Sicherheitsmerkmale (§ 4 Z 27); sie ist Voraussetzung für den Nachweis der „Autorisierung“ des Zahlungsvorgangs (§ 66 Abs 1 Z 1).[25] Bei „starker Kundenauthentifizierung“ werden mindestens zwei Elemente der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das nur der Nutzer ist) eingesetzt (§ 4 Z 28). Beide Elemente müssen insofern voneinander unabhängig sein, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit des anderen nicht in Frage stellt.[26]

Übersetzt man diese „*monströse Begrifflichkeit*“[27] in reale Lebenssachverhalte, werden die Vorgaben plastischer. Alltagsbeispiel für die starke Kundenauthentifizierung ist die Verwendung der Zahlungskarte (Besitz) mit der dazugehörigen PIN (Wissen).[28] Moderne Zahlungsformen ermöglichen auch die Identifizierung des Kunden über sein Smartphone, das er an einen Zahlungsterminal hält (Besitz), und seinen Fingerabdruck (Inhärenz).[29]

Die Unterschrift taugt hingegen nicht zur starken Kundenauthentifizierung. Sie ist zwar nach Ansicht des EuGH ein „personalisiertes Sicherheitsmerkmal“,[30] bezieht ihren Wert als Authentifizierungsmerkmal aber erst durch einen Abgleich mit der auf der Rückseite der Zahlungskarte geleisteten Unterschrift. Sie ist somit gerade nicht unabhängig vom Besitz

11) *Mülbert*, FS Canaris 271 (278).
12) § 68 Abs 1 ist abschließend, RIS-Justiz RS0128542; ErlRV 207 BlgNR XXIV. GP, 48; *Kurz*, ecolex 2017, 836 (837 f). Nach hA kann der Kunde aber zumindest vertraglich auch dazu verpflichtet werden, die Zahlungskarte selbst (die kein personalisiertes Sicherheitsmerkmal ist, *Omlor* in Staudinger [2020] § 675l BGB Rn 3), vor unbefugtem Zugriff zu schützen, ErlRV 11 BlgNR XXVI. GP, 17; *Kodek*, ÖBA 2021, 19 (21); S auch *Hofmann* in Beck-OGK § 675l Rn 18 ff.
13) Die Beweislast für den sorglosen Verlust liegt freilich beim Kartenaussteller.
14) 3 Ob 248/06a; *Kodek*, ÖBA 2021, 19 (28 f).
15) Gleiches gilt, wenn Verlust, Diebstahl oder missbräuchliche Verwendung durch einen Angestellten des Kartenausstellers verursacht wurde (§ 68 Abs 2 Z 2).
16) S aber *Hoffmann*, VuR 2016, 243 (244 f).
17) *Kodek*, ÖBA 2021, 19 (24 f); *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 68 Rn 41 ff; *Hofmann* in Beck-OGK BGB § 675v Rn 42 f; *Zetsche* in MüKo, BGB[8] § 675v Rn 33 ff.
18) Der Kunde haftet aber trotz des missverständlichen Wortlauts auch, wenn er zwar das Abhandenkommen der Karte, aber nicht den nachfolgenden Missbrauch bemerken konnte, vgl *Hoffmann*, VuR 2016, 243 (244).
19) 4 Ob 179/02f; *Graf*, ecolex 1999, 239; *Koller*, NJW 1981, 2433 (2440).
20) *Graf*, RdW 2011, 587.
21) Ausf dazu *Kodek*, ÖBA 2021, 19.
22) *Kodek*, ÖBA 2021, 19 (30 ff). Die deutschen (Unter-)Gerichte scheinen freilich eine ausgesprochen strenge Linie vorzugeben, vgl die Nw bei *Hofmann* in BeckOGK BGB § 675l Rn 55 ff; *Linardatos* in MüKo, HGB[4] Rn G/87; *Zetsche* in MüKo, BGB[8] § 675v Rn 46 ff.
23) Gleiches gilt, nachdem der Kunde das Abhandenkommen seiner Zahlungskarte angezeigt hat (§ 68 Abs 6).
24) *Herresthal* in Langenbucher/Bliesener/Spindler, Bankrecht[3] § 675v Rn 78; *Hoffmann*, VuR 2016, 243 (248); *Kodek*, ÖBA 2021, 19 (35).
25) Ausf *Jungmann*, ZBB 2020, 1 (1 ff).
26) Ob zwei verschiedene Elemente aus derselben Kategorie verwendet werden können, ist umstritten, dafür *Hoffmann*, VuR 2016, 243 (249); dagegen *Haghofer*, VbR 2018, 173 (174).
27) *Köndgen*, JuS 2011, 481 (484).
28) *Jungmann* in Langenbucher/Bliesener/Spindler, Bankrecht[3] Kap 6 Rn 18.
29) *Haghofer*, VbR 2018, 173 (174); *Omlor* in Staudinger (2020) § 675v BGB Rn 39.
30) EuGH Rs C-287/19 *DenizBank AG/VKI* Rn 87; S dazu schon *Broucek* in Weilinger, ZaDiG § 3 Rn 53; *Casper* in Casper/Terlau, ZAG[2] § 1 Rn 442 mwN.

an der Karte und erfüllt daher nicht die Anforderungen des § 4 Z 28.[31] Weiters fehlt es an einer starken Kundenauthentifizierung insbesondere beim kontaktlosen Bezahlen ohne PIN (3.1.).

Wo den Kartenaussteller aufsichtsrechtlich eine Pflicht zur starken Kundenauthentifizierung trifft (§ 87, dazu sogleich ausf unter 3.1.), hat ein Verstoß gegen diese Pflicht verwaltungsstrafrechtliche Konsequenzen (§ 100 Abs 8 Z 2). Flankiert werden diese aufsichtsrechtlichen Vorgaben vom zivilrechtlichen Haftungsprivileg in § 68 Abs 5, das bei Verzicht auf die starke Kundenauthentifizierung selbst den vorsätzlich handelnden Kunden von der Haftung befreit. Lässt der Kunde etwa seine Kreditkarte bewusst auf einem belebten öffentlichen Platz offen liegen, trägt dennoch der Kartenaussteller das Missbrauchsrisiko, wenn ein Dritter mit der Kreditkarte auf Einkaufstour geht und dabei etwa nur die Kreditkartennummer abgefragt wird. Das muss wohl selbst dann gelten, wenn sich der Vorsatz nicht nur auf die Pflichtverletzung, sondern auch auf die Schädigung richtet, solange nicht die Grenze zur betrügerischen Absicht – also zur vorsätzlichen Täuschung über den Missbrauch[32] – überschritten ist.

Hinter diesem zivilrechtlich irritierenden Ergebnis steht eine besondere aufsichtsrechtliche *ratio*. Nach hA soll § 68 Abs 5 einen Anreiz für Zahlungsdienstleister schaffen, die Systemsicherheit durch Verwendung der starken Kundenauthentifizierung zu steigern.[33] Im eben skizzierten Beispiel könnte der Missbrauch der Kreditkarte ja verhindert werden, wenn dem Dieb etwa die Eingabe einer PIN oder der Nachweis eines biometrischen Merkmals abverlangt würde.

2.3. Reichweite des § 68 Abs 5?

Diese seltsame Verquickung von Aufsichts- und Zivilrecht wirft aber die Frage nach der Reichweite des § 68 Abs 5 auf. Greift das zivilrechtliche Haftungsprivileg nur, wenn der Kartenaussteller gegen seine aufsichtsrechtliche Pflicht verstößt, die starke Kundenauthentifizierung zu verlangen? Oder selbst dann, wenn der Kartenaussteller aufsichtsrechtlich gar nicht zur starken Kundenauthentifizierung verpflichtet ist?

Was wie eine technische Detailfrage wirkt, erweist sich als Kristallisationspunkt des Risikoverteilungsmodells. Wäre § 68 Abs 5 von der aufsichtsrechtlichen Pflicht zur starken Kundenauthentifizierung entkoppelt, würde sich nämlich das oben skizzierte Gesamtgefüge noch einmal markant verschieben. Die Grundregel wäre dann nicht mehr eine betraglich unbegrenzte Kundenhaftung ab grobem Verschulden, sondern erst ab betrügerischer Absicht.[34] Das ZaDiG würde sich damit vom allgemeinen Zivilrecht noch ein gutes Stück weiter entfernen. Es verwundert daher nicht, dass die Frage in der Literatur zunehmend kontrovers diskutiert wird und zuletzt sogar – wenngleich wohl unbemerkt – den EuGH beschäftigt hat.

3. Gesetzliche Risikoverteilung zwischen Aufsichts- und Zivilrecht

3.1. Starke Kundenauthentifizierung: aufsichtsrechtliche Pflicht?

Um die Frage nach der Reichweite des § 68 Abs 5 beantworten zu können, muss man zunächst wissen, wann das Aufsichtsrecht die starke Kundenauthentifizierung verlangt. *Sedes materiae* ist § 87 Abs 1: Demnach muss der Kartenaussteller eine starke Kundenauthentifizierung verlangen, wenn der Kunde online auf sein Zahlungskonto zugreift (Z 1), einen elektronischen Zahlungsvorgang auslöst (Z 2) oder über einen Fernzugang eine Handlung vornimmt, die ein Betrugs- oder Missbrauchsrisiko birgt (Z 3). Da der bloße Zugriff auf das Zahlungskonto (Z 1) keinen finanziellen Nachteil verursacht, interessieren hier Z 2 und Z 3.

Dabei hat sich die Literatur mit Blick auf ErwG 95 auf ein „weites" Verständnis „elektronischer Zahlungsvorgänge" (Z 2) geeinigt. Einer starken Kundenauthentifizierung bedarf es daher nicht nur bei Kartenzahlungen im Internet,[35] sondern regelmäßig auch beim Bargeldbezug am Bankomaten[36] und auch bei Zahlungen über einen POS-Terminal (etwa an der Ladenkassa).[37]

Nicht erforderlich ist eine starke Kundenauthentifizierung nach Auffassung der European Banking Authority (EBA) hingegen insbesondere bei „klassischen" Kreditkartenzahlungen im Präsenzgeschäft unter Verwendung eines „Imprinters". Diese seien *„paper-based"*,[38] weil die aufgeprägten Kreditkartendaten mithilfe des „Imprinters" auf den Leistungsbeleg durchgedrückt werden, wo der Kunde unterschreibt.[39] Die EBA verlangt auch bei Bestellungen per Post oder über das Telefon („Telephone Order"-Verfahren) keine starke Kundenauthentifizierung; hier soll somit auch kein missbrauchsträchtiger Fernzugriff (Z 3) vorliegen.[40] Auch ErwG 95 zur PSD II meint lapidar, es „*dürfte nicht notwendig sein, für […] papiergestützte Zahlungsvorgänge oder Bestellungen per Post oder Telefon, dasselbe Schutzniveau zu gewährleisten*."

Damit macht das Aufsichtsrecht die Sicherheit des Zahlungsvorgangs auch von den Risikopräferenzen des Kartenausstellers abhängig. Der Kartenaussteller darf papiergestützte Kartenzahlungen mit Unterschrift weiterhin honorieren, solange die am Zahlungsbeleg geleistete und die auf der Karte hinterlegte Unterschrift übereinstimmen.[41] Es besteht also keine Pflicht des Kartenausstellers, nur besonders „sichere" Zahlungsverfahren zu verwenden. Besonders „sichere" Zahlungsverfahren müssen nur bei elektronischer Abwicklung implementiert werden.

Dieser Regelungsansatz wirkt etwas merkwürdig, dürfte seinen Grund aber darin finden, dass nur bei „elektronischen Zahlungsvorgängen" (über das Internet) eine Verbindung zum Kartenaussteller hergestellt wird, sodass er nur hier eine starke Kundenauthentifizierung vornehmen kann. In offline durchgeführte Zahlungen ist der Kartenaussteller nicht eingebunden.[42]

So kann die starke Kundenauthentifizierung nach hA auch unterbleiben, wenn auf einem Chip oder einem Magnet-

31) *Hofmann*, BKR 2014, 105 (108 f); *Jungmann* in Langenbucher/Bliesener/Spindler, Bankrecht³ Kap 6 Rn 19; *Omlor* in Staudinger (2020) § 675l Rn 5.
32) Dazu *Kodek*, ÖBA 2019, 19 (26).
33) *Jungmann*, ZBB 2020, 1 (8); *Koch*, ÖBA 2019, 106 (111 f); *Linardatos* in MüKo, HGB VI⁴ Rn G/147; *Omlor*, BKR 2019, 105 (112 f); *Tuder*, Grundsatzfragen 83; *Zahrte*, NJW 2018, 337 (340).
34) So *Hoffmann*, VuR 2016, 243 (253); *Hofmann*, BKR 2018, 62.
35) Dazu bereits EBA/GL/2014/12_Rev1, Leitlinie zur Sicherheit von Internetzahlungen (19.12.2014); *Baumbach/Hefermehl/Casper*, Wechselgesetz, Scheckgesetz, Recht des Zahlungsverkehrs²⁴ Rn E/391.
36) *Zahrte*, BKR 2019, 484 (488 f).
37) *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 87 Rn 20; *Terlau*, ZBB 2016, 122 (132); BT-Drs. 18/11495, 140.
38) EBA/RTS/2017/02 „Final Report – Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)", 23.2.2017, S 143 zu Comment [272], Z 2; S auch ErwG 95: „*papiergestützte Zahlungsvorgänge*".
39) *Jungmann*, ZBB 2020, 1 (3 f); *Terlau*, ZBB 2016, 122 (132); *Zahrte* in Casper/Terlau, ZAG² § 55 Rn 42.
40) EBA/RTS/2017/02, S 73 zu Comment [46], S 94 zu Comment [90]; S auch ErwG 95 zur PSD II; aA *Nasarek* in Casper/Terlau, ZAG² Anh zu § 55 Rn 85.
41) *Taupitz*, NJW 1996, 217 (221 mwN); Vogel, Mißbrauch 26 f mwN.
42) *Zahrte* in Casper/Terlau, ZAG² § 55 Rn 42.

Verlag Österreich

streifen gespeicherte Kreditkartendaten in einem offline betriebenen Zahlungsterminal eingelesen werden und der Kunde dann auf dem Leistungsbeleg unterschreibt.[43] Das ist konsequent: die Authentifizierung des Kunden kann hier nur der Zahlungsempfänger vornehmen, mangels Verbindung zum Kartenaussteller aber nicht dieser selbst.

Dieser Regelungsansatz trägt auch den Interessen des Kunden Rechnung: Wo elektronische Zahlungen wegen des Fehlens einer stabilen Internetverbindung nicht durchführbar sind (etwa in entlegenen Gegenden), verbietet das Aufsichtsrecht die Kartenzahlung nicht schlechthin. Vielmehr darf auf ein weniger sicheres Authentifizierungsverfahren zurückgegriffen werden. Dem Kunden wird es schließlich allemal lieber sein, papiergestützt oder magnetstreifenunterstützt zu bezahlen, als gar keine Zahlung vornehmen zu können.

Offline durchgeführte Kreditkartenzahlungen sind heute dennoch ein Auslaufmodell. Die starke Kundenauthentifizierung stellt den praktischen Regelfall dar,[44] was der Frage nach der Reichweite des § 68 Abs 5 im Kreditkartengeschäft etwas von ihrer praktischen Schärfe nimmt.

Im Wirtschaftsleben allgegenwärtige Ausnahmen von der starken Kundenauthentifizierung normieren aber die kleinteiligen „Regulatory Technical Standards" (RTS), die die Europäische Kommission in der auf Art 98 PSD II gegründeten DelVO 2018/389 erlassen hat. Von großer praktischer Bedeutung ist etwa die Ausnahme für „*kontaktlose Kleinbetragszahlungen*"[45] in Art 11 DelVO 2018/389, wonach Zahlungen bis maximal € 50 ohne starke Kundenauthentifizierung durchgeführt werden können (lit a). Das gilt nach der bisher wohl überwiegenden Ansicht im Schrifttum bis zu einem über maximal fünf Zahlungsvorgänge (lit c) akkumulierten Gesamtbetrag von € 150 (lit b).[46] Mit der Zahlungskarte können daher kontaktlos am Händlerterminal jedenfalls 3 x € 50 oder 5 x € 30 ohne PIN bezahlt werden.

Im Einzelnen bleibt hier freilich vieles unklar. Art 11 lit b DelVO kann man nämlich seinem Wortlaut nach auch so verstehen, dass in die Höchstgrenze von € 150 der aktuelle Zahlungsvorgang (iHv maximal € 50, lit a) nicht einzurechnen ist (arg „die früheren kontaktlosen elektronischen Zahlungsvorgänge"). Bei dieser Lesart könnten insgesamt bis zu € 200 ohne PIN bezahlt werden.[47] Diese Auslegung hätte indes die eigenartige Konsequenz, dass nach Art 11 lit b DelVO zwar 4 x € 50, aber nicht 5 x € 40 ohne PIN bezahlt werden könnten.[48]

Weiters ist unklar, ob es sich bei den € 150 bzw € 200 um eine absolute Höchstgrenze handelt oder ob nach Art 11 lit c DelVO (arg „oder") alternativ maximal fünf Zahlungsvorgänge à € 50 ohne PIN erlaubt sind. Der Normtext lässt dieses Verständnis zu, damit würde aber die Höchstgrenze in Art 11 lit b DelVO ausgehebelt. Außerdem wären die Konsequenzen eigenartig: Während 5 x € 50 ohne PIN bezahlt werden könnten, wären etwa 6 Zahlungen à € 40 nicht ohne PIN möglich.

Die Verwirrung ist somit groß. Dass es nicht gelungen ist, eine einfache Höchstgrenze zweifelsfrei festzulegen (deren Nichteinhaltung durch den Kartenaussteller verwaltungsstrafrechtlich sanktioniert ist!), spricht nicht für die legistische Qualität der DelVO 2018/389. Welche Auslegung sich letztlich durchsetzen wird, ist kaum absehbar. Die vom bislang überwiegenden Schrifttum vertretene Ansicht, wonach alle Zahlungsvorgänge zusammenzurechnen sind und die dabei erzielte Summe die Höchstgrenze von € 150 und die Maximalanzahl von fünf nicht überschreiten darf, ist aber die einfachste und wohl auch die sachgerechteste Lösung. Mit der Zahlungskarte können daher 5 x € 30 oder 3 x € 50 ohne PIN bezahlt werden.

Folgt man dem, kann bei „elektronischen Fernzahlungsvorgängen"[49] die starke Kundenauthentifizierung jedenfalls bis € 30 (einzeln) und € 100 (gesamt) unterbleiben (Art 16 DelVO). Führt der Zahlungsdienstleister eine „Transaktionsrisikoanalyse" durch und ermittelt anhand vorgegebener Schwellenwerte, dass ein elektronischer Fernzahlungsvorgang „mit einem niedrigen Risiko verbunden" ist, sind je nach Risikoklasse sogar Einzelzahlungen von € 100/250/500 ohne starke Kundenauthentifizierung möglich (Art 18 iVm Anhang DelVO).

Während die Erwägungsgründe die eben skizzierten „Kleinbetragsausnahmen" mit dem geringen Risiko für den Kunden begründen[50] (und damit offenbar davon ausgehen, dass den Kunden auch ohne starke Kundenauthentifizierung das Missbrauchsrisiko treffen kann, dazu noch 3.3.3.), sehen die RTS auch für „größere" Beträge einzelne Ausnahmen von der starken Kundenauthentifizierung vor,[51] etwa bei der Zahlung von Verkehrsnutzungsentgelten und Parkgebühren an unbeaufsichtigten Terminals (Art 12 DelVO). Das liegt daran, dass hier eine starke Kundenauthentifizierung aus operativen Gründen oft nicht durchführbar ist und durch einfache und benutzerfreundliche Zahlungsmethoden etwa in Parkgaragen oder an Mautstellen lange Wartezeiten und Verkehrschaos sowie Unfälle vermieden werden sollen.[52]

Diese hier nur kursorisch dargestellten Ausnahmen von der starken Kundenauthentifizierung akzentuieren die Frage nach der Reichweite des § 68 Abs 5. Haftet der Kunde selbst dann nicht, wenn aufsichtsrechtlich gar keine Pflicht zur starken Kundenauthentifizierung besteht: wenn etwa ein unbefugter Dritter mit der bewusst im Kaffeehaus liegengelassenen Zahlungskarte kontaktlos 3 x € 50 am Händlerterminal bezahlt? Oder haftet der Kunde „schon" bei grober Fahrlässigkeit und Vorsatz?

Auch wenn es hier um Kleinbeträge geht, ist die praktische Bedeutung dieser Frage nicht zu unterschätzen. Zum einen summieren sich Kleinbeträge bei aggregierter Betrachtung; zum anderen ist die Vergewisserung über die gesetzliche Risikoverteilung Voraussetzung für die inhaltlich zulässige und transparente AGB-Gestaltung im Massengeschäft (dazu 4.2.), die auch mit Blick auf mögliche Verbandsklagen besondere Beachtung verdient.

3.2. 9 Ob 31/15x: keine Haftung ohne Authentifizierung?

Im Rahmen einer Verbandsklage hat denn auch der OGH die hier interessierende Frage bereits gestreift. Der Anlassfall betraf freilich noch das ZaDiG 2009

43) *Jungmann*, ZBB 2020, 1 (4); *Linardatos* in MüKo, HGB[4] Rn G/29; vgl dazu die Feststellungen in 4 Ob 133/14h.
44) *Hoffmann*, VuR 2016, 243 (251); *Zahrte* in Casper/Terlau, ZAG² § 55 Rn 42.
45) *Jungmann*, WM 2021, 557 (561).
46) *Hofmann* in BeckOGK BGB § 675v Rn 113.1; diesem folgend *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 87 Rn 33; offene Formulierung bei *Omlor* in Staudinger § 675v Rn 40.
47) Dagegen *Hofmann* in BeckOGK BGB § 675v Rn 113.1.
48) Nach Art 11 lit c könnten dann zwar 5 x € 40 bezahlt werden, aber etwa nicht 6 x € 30.
49) Von diesem Begriff erfasst ist jedenfalls das Distanzgeschäft über das Internet, *Omlor* in Staudinger (2020) § 675v BGB Rn 42. Zu den weiteren (erheblichen) Auslegungsschwierigkeiten *Hoffmann*, VuR 2016, 243 (251).
50) ErwG 11 DelVO 2018/389; *Hofmann* in BeckOGK BGB § 675v Rn 112. S auch Art 13 hinsichtlich der „Liste der vertrauenswürdigen Empfänger", wo das Erfordernis der starken Kundenauthentifizierung überhaupt entfällt.
51) *Jungmann*, ZBB 2020, 1 (5); für eine einschränkende Auslegung *Hofmann* in BeckOGK BGB § 675v Rn 114 f.
52) ErwG 11 DelVO 2018/389; näher *Omlor* in Staudinger (2020) § 675v BGB Rn 40.

Verlag Österreich

und das „Telephone-Order-Verfahren" im Kreditkartengeschäft: Hier hafte der Kunde nur bei betrügerischer Absicht, wenn bei einem Kreditkartenmissbrauch lediglich auf der Kreditkarte aufgeprägte Merkmale wie Kartennummer, Verfallsdatum und Prüfzahl abgefragt würden.

Das ist erstaunlich, weil das ZaDiG 2009 weder die starke Kundenauthentifizierung noch ein dem § 68 Abs 5 ZaDiG 2018 vergleichbares Haftungsprivileg kannte. PIN-Zahlungen waren zum Inkrafttreten des ZaDiG 2009 im Kreditkartengeschäft noch eher unüblich. Die Begründung des OGH setzt aber schon einen Schritt früher an: eine Zahlungskarte sei gar kein Zahlungsinstrument, wenn sie nicht mit personalisierten Sicherheitsmerkmalen (§ 4 Z 14) verwendet werde, wozu die auf der Karte aufgeprägten Merkmale gerade nicht zählten, weil diese nicht geheim gehalten werden könnten. Da eine Haftung des Kunden aber den „Missbrauch eines Zahlungsinstruments" voraussetze, hafte der Kunde schon aus diesem Grund nicht.[53)]

Diese Auffassung ist spätestens seit zwei Judikaten des EuGH überholt. Abgesehen davon, dass es nicht besonders intuitiv ist, einer Zahlungskarte die Qualifikation als Zahlungsinstrument abzusprechen, differenziert etwa § 64 Abs 2 S 1 (Art 70 Abs 2 PSD II) zwischen „Zahlungsinstrumenten" und „personalisierten Sicherheitsmerkmalen". Beide Begriffe sind somit voneinander unabhängig; personalisierte Sicherheitsmerkmale sind kein konstitutives Element eines Zahlungsinstruments.[54)]

Das beweist auch § 57 Abs 1 Z 2 (Art 63 Abs 1 lit b PSD II), wo von „anonym" genutzten „Kleinbetragszahlungsinstrumenten" die Rede ist. Dass bei anonymer Nutzung gerade keine personalisierten Sicherheitsmerkmale eingesetzt werden, schadet der Qualifikation als „Zahlungsinstrument" ganz offensichtlich nicht. Daraus hat der EuGH in den Rechtssachen *T-Mobile Austria* und *DenizBank* den zwingenden Schluss gezogen, dass ein „Zahlungsinstrument" auch einen „nicht personalisierten Verfahrensablauf" erfassen kann.[55)]

Das ist auch mit speziellem Blick auf das Risikoverteilungsmodell in §§ 67 f überzeugend. Nach § 57 Abs 2 Z 2 kann nämlich bei anonym genutzten Kleinbetragszahlungsinstrumenten die Haftung des Kunden nach § 68 vertraglich ausgestaltet werden (dazu 4.2.). Diese Regelung ergibt nur Sinn, wenn nach dispositivem Recht eine Haftung des Kunden überhaupt bestehen kann. Da bei anonymer Nutzung aber von vornherein keine Identifizierung anhand personalisierter Sicherheitsmerkmale erfolgt,[56)] kann die Haftung nach § 68 nicht von der Verwendung personalisierter Sicherheitsmerkmale abhängen. Vielmehr ist die Zahlungskarte stets „Zahlungsinstrument". Eine Haftung des Kunden nach § 68 bei missbräuchlicher Verwendung der Zahlungskarte kommt daher grundsätzlich auch ohne Authentifizierung in Betracht.

3.3. Starke Kundenauthentifizierung: zivilrechtliche Obliegenheit?

Damit ist aber noch nicht beantwortet, ob nur die Absätze 1 bis 4 oder auch der Absatz 5 des § 68 anwendbar sind. Der Wortlaut des § 68 Abs 5 (wie des zugrundeliegenden Art 74 Abs 2 PSD II) lässt dies offen. Nach dieser Bestimmung genießt der Kunde das besondere Haftungsprivileg, wenn „der Zahlungsdienstleister des Zahlers keine starke Kundenauthentifizierung verlangt".

Daraus leitet *Haghofer* eine „*haftungsrechtliche Obliegenheit*" des Kartenausstellers zur Verwendung der starken Kundenauthentifizierung ab, deren Verletzung unabhängig von der Verletzung einer aufsichtsrechtlichen Pflicht dem Kartenaussteller (bis zur betrügerischen Absicht) alle Schadenersatzansprüche nehme.[57)] Diese Ansicht vertritt mit Blick auf den gleichlautenden § 675v Abs 4 BGB auch eine im Vordringen begriffene Strömung in der deutschen Literatur.[58)] Im Ergebnis wird damit – auf anderem Begründungsweg – an 9 Ob 31/15x angeknüpft.

Dahinter steht offenbar der Gedanke, dass die zivilrechtliche Obliegenheit zur Sorgfalt in eigenen Angelegenheiten über die verwaltungsrechtlichen Pflichten des Geschädigten hinausgehen kann. So besteht grundsätzlich etwa keine Pflicht zum Tragen eines Fahrradhelms; verzichtet der Geschädigte auf den Helm, kann ihn aber ein Mitverschulden treffen (§ 1304 ABGB).[59)] § 68 Abs 5 soll nun offenbar ein entsprechendes Ergebnis gesetzlich festschreiben, dabei aber statt der Schadensteilung eine Kulpakompensation vorsehen.[60)]

Diese Auffassung erscheint erheblich begründungsbedürftig, wird die Kulpakompensation doch schon im Allgemeinen als „*archaisch*"[61)] und wenig sachgerecht empfunden. Trotzdem soll dieser allgemeinen Systemwidrigkeit noch eine weitere Systemwidrigkeit beigefügt werden: Während § 878 S 3 ABGB für die Kulpakompensation nämlich voraussetzt, dass beide Vertragspartner der gleiche Verschuldensgrad trifft,[62)] soll § 68 Abs 5 schematisch und undifferenziert auch den vorsätzlichen Kunden von jeder Haftung freistellen, obwohl der Kartenaussteller alle aufsichtsrechtlichen Vorgaben einhält.

3.3.1. Historische Interpretation

Für diese schon *prima facie* verblüffende Auffassung könnte die Genese der Richtlinie sprechen. Während nämlich Art 66 Abs 1 des Kommissionsvorschlags zur PSD II das besondere Haftungsprivileg noch auf Fälle beschränkte, in denen der Zahlungsdienstleister bei „*Zahlungen mittels eines Fernkommunikationsmittels*" auf die starke Kundenauthentifizierung verzichtete,[63)] ist diese Beschränkung im Richtlinientext entfallen. Daraus könnte man ableiten, dass das Haftungsprivileg von den aufsichtsrechtlichen Vorgaben, wonach die starke Kundenauthentifizierung nur in bestimmten Fällen verpflichtend ist, entkoppelt werden sollte.

Zwingend ist dieser Schluss aber nicht, weil im Kommissionsvorschlag (Art 87) auch die aufsichtsrechtliche Pflicht zur Verwendung einer starken Kundenauthentifizierung noch auf Fälle beschränkt war, in denen „*der Zahler einen elektronischen Zahlungsvorgang auslöst*". Das Europäische Parlament hat den Anwendungsbereich der starken Kundenauthentifizierung dann graduell

53) 9 Ob 31/15x ÖBA 2017, 115 (*Koch*) = jusIT 2016, 147 (*Janisch*); so auch *Casper/Pfeifle*, WM 2009, 2343 (2344); *Hofmann* in BeckOGK BGB § 675v BGB Rn 127 f.

54) *Linardatos*, Haftungssystem 179 f; *ders* in MüKo, HGB[4] Rn G/36; *Jungmann* in Langenbucher/Bliesener/Spindler, Bankrecht[3] Kap 6 Rn 14; *Oechsler*, WM 2010, 1381 (1381 f); *Omlor*, BKR 2019, 105 (107); *ders* in Staudinger (2020) § 675c BGB Rn 22.

55) EuGH Rs C-616/11, *T-Mobile Austria/VKI* Rn 34 f; EuGH Rs C-287/19 *DenizBank/VKI* Rn 71.

56) EuGH Rs C-287/19 *DenizBank/VKI* Rn 87; krit *Habersack*, EuZW 2020, 767 (769).

57) *Haghofer*, VbR 2018, 173 (175 ff); aA *Koch*, ÖBA 2019, 106 (112 f).

58) *Hoffmann*, VuR 2016, 243 (248, 250); *Hofmann*, BKR 2018, 62; *Jungmann*, ZBB 2020, 1 (8); *Zahrte*, BKR 2019, 126 (130); so wohl auch *Habersack*, EuZW 2020, 767 (768); *Schmid* in Emmenegger, Zahlungsverkehr 67 (82); aA *Omlor*, WM 2018, 57 (63); *Zetsche* in MüKo, BGB[8] § 675v Rn 63.

59) 2 Ob 99/14v ZVR 2014/218 (*Karner*); *Karner* in KBB[6] § 1304 Rn 8 mwN; ausf *Schweighofer*, Schutzbekleidung 56 ff, 63 ff.

60) Zur Einordnung des § 68 Abs 2 als Kulpakompensation bereits *Kodek*, ÖBA 2021, 19 (25).

61) *Koziol*, ZEuP 1998, 593.

62) 4 Ob 95/77; 4 Ob 127/97y; *Bollenberger/P. Bydlinski* in KBB[6] § 878 Rn 7.

63) COM (2013) 547 final, 76 f; *Linardatos*, WM 2014, 300 (303).

erweitert (Art 97 Abs 1 PSD II). Folglich entfiel auch in der Haftungsregel (Art 74 Abs 2 PSD II) die Begrenzung auf „Zahlungen mittels eines Fernkommunikationsmittels", ohne dass damit eine Entkoppelung des Zivilrechts vom Aufsichtsrecht gewollt sein musste.[64]

Bis heute ist nämlich das Verhältnis der Tatbestände „elektronischer Zahlungsvorgang" (Art 97 Abs 1 lit b PSD II), „elektronischer Fernzahlungsvorgang" (Art 97 Abs 2 PSD II) und „Fernzahlungsvorgang" (Art 4 Z 6 PSD II) zueinander ausgesucht unklar. Aus der insoweit missglückten Textierung[65] der Richtlinie lassen sich daher keine weitreichenden Schlüsse ziehen.

Auch dass das zivilrechtliche Haftungsprivileg in Art 74 Abs 2 PSD II bereits zum 13.1.2018 umzusetzen war (Art 115 Abs 1 PSD II), während die in Artt 97 f PSD II und den dazugehörigen RTS normierte aufsichtsrechtliche Pflicht zur starken Kundenauthentifizierung erst zum 14.9.2019 in Kraft trat (Art 115 Abs 4 PSD II iVm Art 38 Abs 2 DelVO 2018/389), spricht nicht zwingend für ein Auseinanderfallen von aufsichtsrechtlicher Pflicht und zivilrechtlicher Obliegenheit.[66] Dass hinter dem zeitlich versetzten Inkrafttreten eine bewusste Entscheidung des Europäischen Gesetzgebers steht, ist nämlich nicht erwiesen.

3.3.2. Systematische Interpretation

Da eine historische Auslegung somit zu keinem eindeutigen Ergebnis führt, bemüht *Haghofer* systematische Erwägungen: Das Haftungsprivileg des § 68 Abs 5 sei eine Ausnahme zum Risikoverteilungsmodell in § 68 Abs 1 und 3. Da aber die Absätze 1 und 3 von den aufsichtsrechtlichen Vorgaben zur starken Kundenauthentifizierung in § 87 unabhängig seien, könne auch Abs 5 nicht auf diese aufsichtsrechtlichen Vorgaben in § 87 abgestimmt sein.[67]

Dass die Ausnahmebestimmung (§ 68 Abs 5) keinen engeren Anwendungsbereich haben dürfe als die Regelbestimmung (§ 68 Abs 1 und 3), ist indessen ein *non sequitur*. Dass § 68 Abs 5 *lex specialis* zu § 68 Abs 1 und 3 ist, sagt nichts über den Anwendungsbereich dieser speziellen Regel aus. Es ist im Gegenteil denkbar, dass die spezielle Regel einen speziellen, auf § 87 abgestimmten, Anwendungsbereich hat. Dass Ausnahmevorschriften im Zweifel weit auszulegen wären, hat noch niemand vertreten.

3.3.3. Teleologische Interpretation

Entscheidend müssen daher teleologische Überlegungen sein. Dabei spricht schon der aufsichtsrechtliche Regelungszweck des § 68 Abs 5 entscheidend gegen ein Auseinanderfallen von aufsichtsrechtlicher Pflicht und zivilrechtlicher Obliegenheit. § 68 Abs 5 will einen Anreiz für Kartenaussteller schaffen, die starke Kundenauthentifizierung zu verwenden (s 2.2.). Dieser Anreiz kann aber nur so weit reichen wie das Gesetz die starke Kundenauthentifizierung verlangt. Wo der Gesetzgeber aufsichtsrechtlich auf die starke Kundenauthentifizierung verzichtet hat, hat er dies nämlich bewusst getan und dabei die Interessen der Kunden bereits mitberücksichtigt und gegen die Interessen der Kartenaussteller abgewogen.[68]

Diese aufsichtsrechtliche Determinante würde durch ein von den aufsichtsrechtlichen Pflichten entkoppeltes zivilrechtliches Haftungsprivileg unterlaufen.[69] So sehen die RTS Ausnahmen von der starken Kundenauthentifizierung insbesondere bei kontaktlosen Kleinbetragszahlungen vor (Art 11 DelVO 2018/389). Trüge der Kartenaussteller bei fehlender Kundenauthentifizierung ohnehin stets das Missbrauchsrisiko, hätte man das bequeme und gerade in Pandemiezeiten hochgeschätzte kontaktlose Zahlen hingegen für weitaus höhere Beträge zulassen können.

Weitere Ausnahmen sehen die RTS für Fälle vor, in denen die starke Kundenauthentifizierung technisch nur schwer durchführbar oder für den Kunden besonders unpraktisch wäre (etwa an einer Mautstelle). Dieser Zweck würde konterkariert, wenn man den Kartenaussteller auch gegenüber dem vorsätzlich handelnden Kunden mit dem Missbrauchsrisiko belastete, weil dann der Anreiz verloren ginge, benutzerfreundliche Zahlungsmethoden zu ermöglichen.

Nicht überzeugend ist daher das Argument, die Haftung des Kunden dürfe „*nicht von den Risikopräferenzen des Zahlungsdienstleisters abhängig gemacht*" werden.[70] Erstens übergeht dieses Argument, dass der Kunde ohnehin nur bei grobem Verschulden betraglich unbegrenzt haftet. Zweitens kann man dem Kartenaussteller seine „*Risikopräferenz*" dann nicht zum Vorwurf machen, wenn er sie auf die detaillierten aufsichtsrechtlichen Vorgaben abgestimmt hat.

Das zeigt auch die Ausnahme von der starken Kundenauthentifizierung für papiergestützte Kreditkartenzahlungen mittels Unterschrift. Zwar ist der Kunde in der Tat nicht weniger schutzwürdig, wenn ein unbefugter Dritter seine Kreditkarte papiergestützt anstatt online verwendet. Dass der Kunde bei papiergestützten Zahlungen dennoch schlechter steht (weil er nicht in den Genuss des besonderen Haftungsprivilegs nach § 68 Abs 5 kommen kann), ist aber Folge des aufsichtsrechtlichen Regelungsansatzes, der hier eben keine starke Kundenauthentifizierung verlangt, weil der Kartenaussteller in den Zahlungsvorgang nicht eingebunden ist (s 3.1.).[71] Das Aufsichtsrecht erlaubt missbrauchsanfällige papiergestützte Kreditkartenzahlungen mittels Unterschrift weiterhin. Honoriert der Kartenaussteller solche Zahlungen, kann man ihm – wenn die Unterschriften auf Leistungsbeleg und Kreditkarte übereinstimmen[72] – seine „Risikopräferenz" daher nicht vorwerfen. Wenn das Haftungsprivileg in § 68 Abs 5 eine „*zivilrechtliche Sanktion*"[73] für den Kartenaussteller sein soll, gibt es ohne entsprechendes Verhaltensunrecht keinen Bedarf und keine Rechtfertigung für eine solche Sanktion.

Dagegen kann auch nicht eingewendet werden, es „*verbiete sich*" schon allein deshalb, dem Kunden das Missbrauchsrisiko aufzubürden, weil ein unbefugter Dritter die Karte verwende.[74] In §§ 67 f geht es immer um die Verteilung des Drittmissbrauchsrisikos. Müsste der Kunde dieses Risiko nie tragen, wäre § 68 überflüssig.

Irreführend ist auch das Argument, dass sich die „*Abweichung vom Standard der starken Kundenauthentifizierung für den Kunden nicht nachteilig*" auswirken dürfe.[75] Erstens geht es gerade um Fälle, in denen die starke Kundenauthentifizierung nicht der „Standard" ist. Zweitens kann vom Verzicht auf die starke Kundenauthentifizierung im Allgemeinen auch der Kunde profitieren, weil er seine Kreditkarte auch offline einsetzen kann (3.1.). Drittens ist der einzige „Nachteil"

64) *Koch*, ÖBA 2019, 106 (112). 65) Ausf *Hoffmann*, VuR 2016, 243 (251).
66) *Omlor*, BKR 2019, 105 (113); aA *Haghofer*, VbR 2018, 173 (174).
67) *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 68 Rn 64; S auch *Hoffmann*, VuR 2016, 243 (250).
68) Vgl *Linardatos* in MüKo, HGB VI[4] Rn K/157.
69) *Linardatos* in MüKo, HGB VI[4] Rn G/147; *Omlor*, BKR 2019, 105 (113); *Terlau*, ZBB 2016, 122 (133); S auch *Werner*, WM 2018, 449 (454).
70) *Schmalenbach* in BeckOK-BGB[57] § 675v Rn 13b; *Hoffmann/Rastegar*, WM 2021, 957 (962).
71) *Zahrte*, NJW 2018, 337 (340).
72) Vogel, Mißbrauch 26 f; *Taupitz*, NJW 1996, 217 (221 mwN).
73) *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 68 Rn 54.
74) *Haghofer*, VbR 2018, 173 (176).
75) So aber *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 87 Rn 11; *Jungmann*, ZBB 2020, 1 (8).

für den Kunden die Anwendbarkeit des gegenüber den allgemeinen zivilrechtlichen Regeln für ihn ohnehin großzügigen Risikoverteilungsmodells in § 68 Abs 1–3.

Eine Haftung des Kunden kommt nach diesen Regeln nur bei Verschulden, eine betraglich unbeschränkte Haftung überhaupt nur bei grobem Verschulden in Betracht. Wollte man bei fehlender starker Kundenauthentifizierung auch den grob sorglosen Kunden von jeder Haftung freistellen, würde man dem Verbraucherschutz einen „*Bärendienst*“[76] erweisen. Der Kartenaussteller müsste die Kosten für Missbrauchsschäden dann nämlich über höhere Entgelte auf die Gesamtheit seiner Kunden überwälzen.[77] Wirtschaftlich drohte eine Quersubventionierung grob sorgloser (und sogar vorsätzlich handelnder!) Kunden zu Lasten sorgfältiger Kunden, weil es ja eine Illusion wäre zu glauben, der Kartenaussteller trage den Schaden endgültig.[78]

Im aufsichtsrechtlichen Glasperlenspiel gerät allzu leicht in Vergessenheit, wie weit man sich hier bereits von allen anerkannten zivilrechtlichen Grundsätzen entfernt hat. So war es immerhin für *Canaris* „*unter Gerechtigkeitsgesichtspunkten schlechterdings [schon] nicht einzusehen*“,[79] warum die Bank jene Risiken tragen solle, die sich in der Sphäre des Kunden verwirklichen. Völlig selbstverständlich erschien der zivilrechtlichen Lehre, dass der leicht fahrlässige Kunde das Missbrauchsrisiko zur Gänze selbst tragen müsse.[80] Für ein Haftungsprivileg zugunsten des grob fahrlässigen und sogar des vorsätzlich handelnden Kunden gibt es dann aber endgültig keine Rechtfertigung mehr. Eine schematische Kulpakompensation ohne *culpa* des Kartenausstellers erschiene aus zivilrechtlicher Sicht sachwidrig und aus ökonomischer Sicht mit Blick auf die Risikoabsorption durch sorgfältige Kunden unzweckmäßig.

Diese Auffassung entspricht im Übrigen nicht nur dem englischen Umsetzungsgesetz, wo Art 77 Abs 4 lit c Payment Services Regulation (PSR) dem Kunden den Genuss des besonderen Haftungsprivilegs nur gewährt, wenn Art 100 PSR die starke Kundenauthentifizierung aufsichtsrechtlich verlangt.[81] Es wird sich zeigen, dass auch der EuGH in der Rs *DenizBank* implizit diese Auffassung bestätigt. Dies erschließt sich freilich erst indirekt aus dem vertraglichen Gestaltungsspielraum, sodass darauf in diesem Zusammenhang näher einzugehen ist (4.5.).

4. Vertragliche Risikoverteilung bei Kleinbetragszahlungen

4.1. EuGH C-287/19 *DenizBank*

Die *DenizBank*-Entscheidung hat im Schrifttum bislang vor allem mit Blick auf Erklärungsfiktionsklauseln Beachtung gefunden.[82] Sie hat aber auch im hier interessierenden Zusammenhang große Bedeutung, weil der EuGH bei kontaktlosen Zahlungen mit einer Zahlungskarte auch im Verbrauchergeschäft Raum für vertragliche Vereinbarungen sieht.

Für vertragliche Vereinbarungen scheint § 55 zwar keinen Spielraum zu lassen, weil §§ 67 f im Verbrauchergeschäft grundsätzlich zwingend sind (2.1.). Anderes gilt aber für „Kleinbetragszahlungsinstrumente“, die Einzelzahlungsvorgänge bis max € 30 (im Inland € 60) betreffen oder die entweder eine Ausgabenobergrenze von max € 150 (im Inland € 300) haben oder Geldbeträge iHv max € 150 (im Inland € 400) speichern (§ 57 Abs 1 und 2). Bei anonymer Nutzung solcher „Kleinbetragszahlungsinstrumente“ ist das gesetzliche Risikoverteilungsmodell der §§ 67 f auch im Verbrauchergeschäft dispositiv (§ 57 Abs 1 Z 2).

Der EuGH qualifiziert nun die zum kontaktlosen Bezahlen verwendete NFC-Funktion („Near Field Communication“) einer Zahlungskarte als eigenes „Kleinbetragszahlungsinstrument“. Eine „*multifunktionale*“[83] Zahlungskarte sei daher Träger zweier Zahlungsinstrumente: einerseits der „regulären“ Zahlungskartenfunktion zur Zahlung „regulärer“ Beträge und andererseits der NFC-Funktion zur Zahlung von „Kleinbeträgen“ iSd Art 63 PSD II (§ 57 ZaDiG).[84]

Verständlich wird diese Einordnung durch den Zusammenhang mit der starken Kundenauthentifizierung. Nach Art 11 DelVO 2018/389 ist bei kontaktlosen Zahlungen mit der NFC-Funktion jedenfalls bis zu einem Gesamtbetrag von € 150 keine starke Kundenauthentifizierung erforderlich (dazu ausf 3.1.). Daher lässt sich vertreten, dass die NFC-Funktion eine „Ausgabenobergrenze“ von € 150 aufweist.[85] Innerhalb dieser Ausgabenobergrenze wird die NFC-Funktion „anonym“ genutzt iSd § 57 Abs 1 Z 2, weil keine PIN abgefragt wird.[86]

Das Schrifttum ist von der EuGH-Entscheidung dennoch überrascht worden.[87] Bislang subsumierte man unter den Begriff „Kleinbetragszahlungsinstrument“ nämlich insbesondere „*Prepaidinstrumente*“[88] wie die deutsche „Geldkarte“[89] oder die „Quick-Funktion“[90] österreichischer Bankomatkarten. Hier autorisiert der Kunde (meist durch Eingabe der PIN am Bankomaten) im Voraus das „Aufladen“ der Karte mit einem begrenzten Betrag, der dann ohne Eingabe der PIN abgebucht werden kann. Die aufgeladene Karte hat damit Bargeldersatzfunktion und ist einer gefüllten Brieftasche vergleichbar, die ohne PIN verwendet werden kann.[91]

Bei der NFC-Funktion einer Zahlungskarte ist die Interessenlage ähnlich, aber nicht identisch. Zwar unterbleibt auch hier eine Identifizierung des Kartenverwenders über die PIN und ist auch hier das Risiko für den Kunden betraglich begrenzt. Allerdings setzt sich der Kunde nicht durch „Aufladen“ einer Zahlungskarte bewusst dem Risiko aus, ein „bargeldersetzendes“ Instrument mitzuführen. Vielmehr sind moderne Zahlungskarten automatisch mit einer NFC-Funktion ausgestattet. Der Kunde entscheidet sich im Regelfall zwar bewusst für die Zah-

76) *van Gelder*, FS Nobbe 55 (64).
77) *Koziol*, ÖBA 2001, 250 (255); *van Gelder*, FS Nobbe 55 (64).
78) AA *Schmalenbach* in BeckOK-BGB[57] § 675v Rn 13b; S auch *Jungmann*, WM 2021, 557 (569).
79) *Canaris*, Bankvertragsrecht I[3] Rn 527o.
80) Vgl nur 4 Ob 179/02f; *Graf*, ecolex 1999, 239; *Koller*, NJW 1981, 2433 (2440).
81) Vgl auch 5 Ob 15/20x: „*Gemäß § 87 Abs 1 Z 2 ZaDiG 2018 ist der Zahlungsdienstleister zwar verpflichtet, bei elektronischen Zahlungsvorgängen eine starke Kundenauthentifizierung zu verlangen. Führt der Zahlungsdienstleister nicht ausreichend gesicherte Zahlungen* ***trotzdem*** *durch, haftet er […] für allfällige Missbräuche, sofern sich der Zahler nicht betrügerisch verhalten hat*“. Mit dieser „Haftung“ ist gemeint, dass der Zahlungsdienstleister keinen Aufwandersatzanspruch hat und trotzdem abgebuchte Beträge „erstatten“ muss (§ 67).
82) *Faber*, ÖBA 2021, 305; *Foglar-Deinhardstein*, VbR 2021, 9; *Kellner*, ÖBA 2020, 539; *Prankl*, ecolex 2021, 713; *Th. Rabl*, „Böse“ und „gute“ Zustimmungsfiktionen, ecolex 2021, 693.
83) *Jungmann*, WM 2021, 557.
84) EuGH Rs C-287/19 *DenizBank/VKI* Rn 77 ÖBA 2021, 123 (*Koch*).
85) Vgl *Foerster* in BeckOGK BGB § 675i Rn 13.
86) EuGH Rs C-287/19 *DenizBank/VKI* Rn 80 ff.
87) *Habersack*, EuZW 2020, 767 (769); *Jungmann*, WM 2021, 557 (562, 567 f).
88) *Casper* in MüKo, BGB[8] § 675i Rn 1.
89) *Casper* in MüKo, BGB[8] § 675i Rn 8; *Habersack*, EuZW 2020, 767 (768 f); *Jungmann*, WM 2021, 557 (567 f).
90) ErläutRV 207 BlgNR 24. GP 39; *Weilinger/Gratzl* in Weilinger, ZaDiG § 33 Rn 7.
91) BT-Drs. 16/11643, 105; *Casper* in MüKo, BGB[8] § 675i Rn 14; *Foerster* in BeckOGK BGB § 675i Rn 2; *Herresthal* in Langenbucher/Bliesener/Spindler, Bankrecht[3] 2. Kap. § 675i Rn 1.

Verlag Österreich

lungskarte, hat aber keine Wahl, auf die insoweit „gefährlichere“ NFC-Funktion zu verzichten.[92]

Darauf geht der EuGH aber nicht näher ein: Entscheide sich der Kunde für die Möglichkeit einer „anonymen“ Nutzung der NFC-Funktion iSd Art 63 PSD II, werde er „*damit einverstanden [sein], gegebenenfalls den Auswirkungen der nach dieser Bestimmung zulässigen vertraglichen Beschränkung der Haftung des Zahlungsdienstleisters ausgesetzt zu sein*.“[93]

Nutzt der Kartenaussteller diesen vertraglichen Gestaltungsspielraum, sind somit für den Missbrauch ein und derselben Zahlungskarte zwei unterschiedliche Regelungsregime anwendbar, je nachdem ob der unbefugte Dritte mit der Zahlungskarte „reguläre“ Zahlungen oder Kleinbetragszahlungen mit der NFC-Funktion tätigt. Das rückt die vertraglichen Gestaltungsspielräume und -grenzen des Kartenausstellers in den Mittelpunkt.

4.2. Gestaltungsspielräume und -grenzen

In dem der Rs *DenizBank* zugrundeliegenden Ausgangsverfahren ging es – etwas vergröbert – um eine Reihe von AGB-Klauseln, die den Kartenaussteller von jedem Missbrauchsrisiko befreien sollten (im Detail dazu sogleich).[94] Das wirft die Frage auf, ob § 57 Abs 1 Z 2 Vereinbarungen, die dem Kunden das Missbrauchsrisiko zuweisen, uneingeschränkt erlaubt. Schließlich nennt § 57 Abs 1 Z 2 sowohl § 67 als auch § 68 ausdrücklich als dispositive Bestimmungen.

Der EuGH, der über die streitgegenständlichen Klauseln inhaltlich nicht entscheiden musste, hat dazu freilich ausgesprochen, dass die Klausel-Richtlinie im Verbrauchergeschäft neben der PSD II anwendbar bleibe.[95] Auch das Schrifttum bekennt sich dazu, dass AGB-Klauseln für Kleinbetragszahlungsinstrumente an § 879 Abs 3 ABGB und § 6 KSchG zu messen sind.[96] Häufig wird freilich gleichzeitig betont, dass das Missbrauchsrisiko vertraglich zur Gänze dem Kunden zugewiesen werden könne, weil die Öffnungsklausel in § 57 Abs 1 Z 2 gerade Abweichungen von §§ 67 f erlaube.[97]

Damit greift man indes der Klauselkontrolle vor. Richtig dürfte zwar sein, dass §§ 67 f kein Leitbildcharakter für Kleinbetragszahlungsinstrumente zukommt,[98] weil §§ 67 f den Kunden gegenüber dem allgemeinen Zivilrecht stark begünstigen (2.1.). Daher haben Kartenaussteller erheblichen Gestaltungsspielraum, weil Klauseln, die zulasten des Kunden von §§ 67 f abweichen, so lange sachlich gerechtfertigt sind, als sie dem allgemeinen Zivilrecht entsprechen. Zu prüfen bleibt aber, inwieweit Unterschreitungen dieses zivilrechtlichen Standards zulässig sind.

Auch der OGH nimmt im Anschluss an die *DenizBank*-Entscheidung eine Klauselkontrolle vor, äußert sich dabei aber etwas missverständlich. Einerseits sei eine Klausel zulässig, wonach der Kartenaussteller den Betrag eines nicht autorisierten Zahlungsvorgangs nicht erstatten müsse (Klausel 16 S 1). Anderseits sei eine Klausel unzulässig, wonach der Kunde das Risiko des Kartenmissbrauchs trage (Klausel 17). Einerseits sei nämlich der Erstattungsanspruch gem § 67 dispositiv (§ 57 Abs 1 Z 2); andererseits verstoße es aber gegen § 879 Abs 3 ABGB, eine „Haftung“ des Kartenausstellers gänzlich auszuschließen.[99]

Beide Aussagen passen nicht zusammen. Dass der OGH Klausel 17 kassiert, weil sie den Kunden auch mit dem Risiko eines vom Kartenaussteller verschuldeten Missbrauchs belastet, ist nicht zu beanstanden. Wenn es aber solche Fälle gibt, in denen zwingend der Kartenaussteller das Missbrauchsrisiko trägt, muss es in diesen Fällen auch einen Erstattungsanspruch geben.

Zwar erlaubt § 57 Abs 1 Z 2, den Erstattungsanspruch nach § 67 abzubedingen. Der Kartenaussteller könnte daher etwa vorsehen, dass er den Betrag des nicht autorisierten Zahlungsvorgangs nicht „unverzüglich“ erstatten und wertstellen muss. Er darf aber nicht beliebig in die Verteilung des Missbrauchsrisikos eingreifen, weil Kartenaussteller das Risiko eines selbst verschuldeten Kartenmissbrauchs nicht auf ihre Kunden überwälzen dürfen. Daher ist auch Klausel 16 S 1 unzulässig, weil diese Einschränkung in der Klausel nicht zum Ausdruck kommt.

Praktisch relevanter als die schadenersatzrechtliche Einstandspflicht des Kartenausstellers sind freilich Fälle, in denen diesen am Kartenmissbrauch kein Verschulden trifft. Es geht um Fälle, in denen entweder ein Verschulden des Kunden vorliegt oder in denen sich ein Zufallsrisiko verwirklicht. Wie mit diesen Fällen umzugehen ist, konnte der OGH offenlassen. Es bietet sich aber an, anhand seiner Judikatur vor Inkrafttreten des ZaDiG zu differenzieren.

Zunächst spricht nichts dagegen, den Kunden auch für leichte Fahrlässigkeit haften zu lassen. Die Haftung für leichte Fahrlässigkeit entspricht nicht nur dem zivilrechtlichen Standard (§ 1294 ABGB); sie ist bei Kleinbetragszahlungsinstrumenten auch betraglich beschränkt. Hinzu kommt ein ökonomisches Argument: haften sorglose Kunden, reduziert sich die Gefahr, dass Missbrauchsrisiken über höhere Entgelte auf sorgfältige Kunden überwälzt werden.[100]

Der OGH hat vor Inkrafttreten des ZaDiG auch AGB-Klauseln akzeptiert, nach denen der Karteninhaber verschuldensunabhängig das Risiko des Missbrauchs gestohlener oder verlorener Zahlungskarten tragen musste, weil es sich in seiner Sphäre ereigne.[101] Teile der Lehre vertraten dieses Ergebnis auch ohne entsprechende vertragliche Vereinbarung, weil der Kunde das Risiko des Verlusts oder Diebstahls besser beherrschen könne und er im Ergebnis so gestellt werden solle wie er beim Verlust oder Diebstahl von Bargeld stünde (2.1.).[102]

Umso mehr müssen solche Klauseln für die Verteilung des Missbrauchsrisikos bei NFC-Zahlungen zulässig sein, weil das Risiko hier von vornherein betraglich beschränkt ist. § 57 Abs 1 erlaubt vertragliche Abweichungen von §§ 67 f gerade wegen der Nähe von Kleinbetragszahlungsinstrumenten zu Bargeld.[103] Dann muss es grundsätzlich auch möglich sein, für Kleinbetragszahlungsinstrumente die Risikoverteilung bei Bargeld vertraglich nachzubilden. Ein schon zum allgemeinen Zivilrecht umstrittener Grenzfall ist freilich der Raub der Zahlungskarte.[104]

92) *Hoffmann/Rastegar*, WM 2021, 957 (962).
93) EuGH Rs C-287/19 *DenizBank/VKI* Rn 91.
94) EuGH Rs C-287/19 *DenizBank/VKI* Rn 33.
95) EuGH Rs C-287/19 *DenizBank/VKI* Rn 60 ff; ErwG 55 PSD II: getätigt hat der EuGH diese Aussage freilich im Zusammenhang mit Erklärungsfiktionsklauseln.
96) *Casper* in MüKo, BGB[8] § 675i Rn 12; *Foerster* in BeckOGK BGB § 675i Rn 18.
97) *Foerster* in BeckOGK BGB § 675i Rn 23; vgl auch *Kodek*, ÖBA 2021, 19 (38).
98) *Casper* in MüKo, BGB[8] § 675i Rn 12; *Foerster* in BeckOGK BGB § 675i Rn 18.
99) 8 Ob 105/20d.
100) Vgl 10 Ob 102/15w; 7 Ob 137/14v; *Graf* in Kletečka/Schauer, ABGB-ON[1.05] § 879 Rn 279/2.
101) 1 Ob 598/79, 3 Ob 530/91; 2 Ob 133/99v ÖBA 2001, 250 (*Koziol*); 3 Ob 248/06a; 10 Ob 70/07b; 6 Ob 233/15f.
102) *Canaris*, Bankvertragsrecht I[3] Rn 527o, 710; *Graf*, Telebanking 25 ff.
103) BT-Drs. 16/11643, 105; *Casper* in MüKo, BGB[8] § 675i Rn 14; *Foerster* in BeckOGK BGB § 675i Rn 2; *Herresthal* in Langenbucher/Bliesener/Spindler, Bankrecht[3] 2. Kap. § 675i Rn 1.
104) Vgl schon *Graf*, Telebanking 18, 27 ff; krit *Freudenthaler*, Giroüberweisung 124.

Keine Entsprechung findet bei Bargeld hingegen das Risiko eines technischen Missbrauchs. Angesprochen sind damit zum einen Angriffe auf die Abwicklungssysteme des Kartenausstellers, die etwa zu Fehlbuchungen führen könnten. Zum anderen ist es offenbar technisch möglich, die per NFC-Funktion übertragenen Daten abzufangen, um sie für missbräuchliche Zahlungen zu verwenden („*eavesdropping*“).[105)]

In diesem Zusammenhang hat der OGH noch vor Inkrafttreten des ZaDiG ausgesprochen, dass eine Klausel, wonach der Kunde auch das Risiko eines technischen Missbrauchs trage, gegen § 879 Abs 3 ABGB verstoße.[106)] Das gilt auch im neuen Zahlungsverkehrsrecht unstrittig dann, wenn Angreifer – was technisch offenbar möglich ist[107)] – die abgefangenen Daten für Zahlungen verwenden, die die Kleinbetragsgrenze des § 57 überschreiten, weil hier von vornherein kein vertraglicher Gestaltungsspielraum besteht.

Die besseren Gründe sprechen dafür, diese Judikatur auch auf Kleinbetragszahlungsinstrumente zu übertragen. Zwar ist hier das Risiko für den Kunden betraglich beschränkt. Gleichwohl hat der Kunde keine Möglichkeit, technischen Missbrauch zu verhindern, während der Kartenaussteller durch technische Vorkehrungen am ehesten die Kompromittierung seiner Abwicklungssysteme und Zahlungskarten verhindern kann. Sodann kann der Kartenaussteller die Kosten des technischen Missbrauchs auf die Gesamtheit seiner Kunden verteilen.[108)] Schließlich fällt ins Gewicht, dass moderne Zahlungskarten standardmäßig über die NFC-Funktion verfügen und der Kunde im Regelfall diese Funktion nicht „abbestellen“ kann.[109)] Jedenfalls solange ihm keine echte „Wahlmöglichkeit“ angeboten wird,[110)] wäre eine Belastung des Kunden mit dem Risiko des technischen Missbrauchs daher gröblich benachteiligend.

Ein Anhaltspunkt dafür findet sich auch in der Richtlinie. Nach ErwG 71 der PSD II soll die Richtlinie „*die Verantwortung der Zahlungsdienstleister für die technische Sicherheit ihrer eigenen Produkte nicht berühren*“.[111)] Der EuGH hat in der *DenizBank*-Entscheidung diesen Grundsatz auch für Kleinbetragszahlungsinstrumente hervorgehoben.[112)] Auch der OGH hält es für unzulässig, dem Kunden das Risiko einer Verwendung technisch minderwertiger Kartensysteme aufzuerlegen.[113)] Zwar treffen beide Gerichte diese Aussage im Zusammenhang mit der Sperre der Zahlungskarte, sie lässt sich aber auch auf den technischen Missbrauch übertragen.

Der Kartenaussteller müsste daher zwischen dem Abhandenkommen der Karte durch Verlust oder Diebstahl und dem technischen Missbrauch transparent unterscheiden, weil im Verbrauchergeschäft auch eine geltungserhaltende Reduktion einer zu weitreichenden Klausel ausscheidet.[114)] Die oben zitierte Klausel 17, die den Kartenaussteller von jedem Missbrauchsrisiko befreit, wäre daher auch aus diesem Grund unzulässig.

Weist eine Klausel das Verlust- und Diebstahlsrisiko dem Kunden, das Risiko eines technischen Missbrauchs hingegen dem Kartenaussteller zu, stellt sich die Frage nach der Beweislast. Bucht der Kartenaussteller den strittigen Betrag ab und beruft sich der Kunde auf die fehlende Autorisierung des Zahlungsvorgangs, hilft dem Kunden zwar unstrittig nicht der Nachweis, dass ein Dritter die Karte verwendet habe, weil er gerade das Verlust- und Diebstahlsrisiko trägt. Offen ist aber, wen die Beweislast dafür trifft, dass (k)ein technischer Missbrauch erfolgt ist.

Leider scheint die gesetzliche Regelung für dieses Problem wenig durchdacht zu sein. Grundsätzlich muss der Kartenaussteller die Voraussetzungen eines Aufwandersatzanspruchs beweisen. Nach § 66 Abs 1 muss er dafür nachweisen, dass der Zahlungsvorgang authentifiziert (Z 1), ordnungsgemäß aufgezeichnet und verbucht (Z 2), und nicht durch einen technischen Fehler oder eine andere Störung des Zahlungsdienstes beeinträchtigt wurde (Z 3). Das entspricht der Judikatur, wonach erst die Verwendung der PIN (Z 1: Authentifizierung) einen Anscheinsbeweis dafür erbringt, dass der Kunde die Karte selbst verwendet hat.[115)]

Diese Regelung, die für „reguläre“ Zahlungen mit PIN gedacht ist, ist für kontaktlose Zahlungen freilich unpassend. Da hier gerade keine PIN verwendet wird, ist der Nachweis der Authentifizierung (Z 1) von vornherein unmöglich.[116)] Dennoch ist § 66 offenbar auch bei anonymer Nutzung von Kleinbetragszahlungsinstrumenten anwendbar, wie sich daraus ergibt, dass diese Bestimmung nach § 57 Abs 1 Z 2 abbedungen werden kann. Es empfiehlt sich daher für Kartenaussteller, von dieser Möglichkeit Gebrauch zu machen. Eine Klausel, wonach der Kartenaussteller die Authentifizierung nicht nachweisen muss (§ 66 Abs 1 Z 1), ist zulässig, weil die Öffnungsklausel in § 57 Abs 1 Z 2 sonst von vornherein sinnlos wäre.

Der OGH hatte nun aber im Gefolge der *DenizBank*-Entscheidung über eine Klausel zu entscheiden, die den Kartenaussteller auch von der Pflicht befreite, den Nachweis einer ordnungsgemäßen Aufzeichnung und Verbuchung (§ 66 Abs 1 Z 2) und den Nachweis der Störungsfreiheit des Zahlungsvorgangs (§ 66 Abs 1 Z 3) zu erbringen. Der OGH hielt diese „Klausel 15“ für zulässig, weil § 57 Abs 1 Z 2 eben ausdrücklich erlaube, § 66 abzubedingen.[117)]

Dieses Ergebnis erscheint aber gerade im Verbandsprozess bedenklich. Bei kundenfeindlichster Auslegung kann Klausel 15 nämlich so verstanden werden, dass der Kartenaussteller seine internen Aufzeichnungen nicht herausgeben muss, dass der Kunde also auf wesentliche Beweismittel in einem etwaigen Zivilprozess vorab verzichtet. Solche „Beweisverträge“ wären nach verbreiteter Auffassung schon wegen einer Verletzung der zivilprozessualen Wahrheits- und Vollständigkeitspflicht unzulässig.[118)] An solchen Grundfesten des Zivilprozessrechts sollte auch § 57 Abs 1 Z 2 nicht rütteln können. Aber auch wenn man Klausel 15 als „vertragliche Beweislastregel“ versteht, gegen die keine grundsätzlichen öffentlichrechtlichen Bedenken bestehen,[119)] ist die privatrechtliche Rechtfertigung für eine solche Klausel zweifelhaft. Immerhin verbietet § 6 Abs 1 Z 11 KSchG Beweislastregeln im Verbrauchergeschäft selbst

105) *Jungmann*, WM 2021, 557 (571 f); *Hoffmann/Rastegar*, WM 2021, 957 (958).
106) RIS-Justiz RS0113753.
107) Vgl Focus, Wissenschaftler hacken NFC-Bezahlfunktion bei Visa-Karten, https://www.focus.de/finanzen/boerse/sicherheitsluecke-bei-visa-wissenschaftler-hacken-nfc-bezahlfunktion-bei-visa-karten_id_12377908.html (abgerufen am 29.5.2021); *Hoffmann/Rastegar*, WM 2021, 957 (958 mwN).
108) S dazu *Koziol*, ÖBA 2001, 250 (255); *Kurschel*, ecolex 1990, 79 (80 f).
109) Vgl 8 Ob 105/20d.
110) Vgl dazu *Graf* in Kletečka/Schauer, ABGB-ON[1.05] § 879 Rn 285 ff mwN.
111) Vgl auch ErwG 91 der PSD II.
112) EuGH Rs C-287/19 *DenizBank/VKI* Rn 103.
113) 8 Ob 105/20d.
114) EuGH Rs C-618/10 *Banco Español* JBl 2012, 434 (*Lukas*) = ÖBA 2013, 69 (*Geroldinger*); 2 Ob 22/12t; 3 Ob 237/16y; *P. Bydlinski/Bollenberger* in KBB[6] § 879 Rn 30.
115) 2 Ob 133/99v ÖBA 2001,250 (*Koziol*); BGH WM 2012, 164; ausf *Zetsche* in MüKo, BGB[8] § 675w Rn 29 ff.
116) EuGH Rs C-287/19 *DenizBank/VKI* Rn 87; krit *Habersack*, EuZW 2020, 767 (769).
117) 8 Ob 105/20d.
118) *Fasching*, Lehrbuch ² Rn 823; großzügiger aber *Trenker*, Parteidispositionen 252 ff mwN.
119) *Fasching*, Lehrbuch² Rn 889 ff; *Trenker*, Parteidispositionen 260 ff.

Verlag Österreich

in Individualvereinbarungen. Es fehlt eine sachliche Rechtfertigung dafür, warum gerade im Zahlungsverkehrsrecht solche Beweislastregeln ohne Einschränkung in AGB zulässig sein sollten.

Dabei erweist sich gerade die vom OGH beurteilte Klausel 15 als problematisch. Zumindest im Verbandsprozess müsste die Klausel wohl so ausgelegt werden, dass für die erfolgreiche Geltendmachung eines Aufwandersatzanspruchs durch den Kartenaussteller dessen bloße Behauptung ausreiche, die Zahlungskarte sei eingesetzt worden.[120] Es läge dann am Kunden zu beweisen, dass die Abbuchung auf einen technischen Missbrauch der Karte oder gar auf einen Fehler im System des Kartenausstellers zurückgeht. Dabei handelt es sich freilich um Umstände aus der Sphäre des Kartenausstellers, sodass der Kunde diesen Beweis ohne Vorlage bankinterner Unterlagen kaum je erbringen könnte. Wie sollte der Kunde etwa nachweisen, dass beim Kartenaussteller Buchungsfehler passiert sind? Eine solche Klausel, die im Zahlungsverkehr dem Kunden die Beweislast für Umstände aus der Verantwortungssphäre der Bank zuweist, hat der BGH zuletzt sogar im B2B-Geschäft für unzulässig gehalten.[121] Das gilt im Verbrauchergeschäft umso mehr, zumal § 66 die Wertung zu entnehmen ist, dass keine schutzwürdigen Geheimhaltungsinteressen der Bank entgegenstehen.

Daher ist § 57 Abs 1 Z 2 einschränkend auszulegen. Die Bestimmung erlaubt keine willkürlichen Abweichungen von § 66 Abs 1, sondern nur sachgerechte Modifikationen der Beweislast. Es ist zwar nicht ausgeschlossen, für den Fall des *non liquet* eine Vermutung zu vereinbaren, dass kein technischer Missbrauch vorliegt.[122] Diese Vermutung muss aber eine sachliche Grundlage haben. Nach allgemeinen Grundsätzen muss der Kartenaussteller daher die Aufzeichnung des Zahlungsvorgangs und die technische Störungsfreiheit nachweisen.[123]

Kann der Kartenaussteller auf diese Weise darlegen, dass seine Sphäre mangelfrei ist, spricht in der Tat viel dafür, dass entweder der Kunde selbst oder eine andere berechtigte Person oder ein Dieb (für den der Kunde ja bei entsprechender vertraglicher Vereinbarung ebenfalls haften würde) den Zahlungsvorgang getätigt hat.[124] Der technische Missbrauch erscheint dann als unwahrscheinliches Szenario,[125] auch wenn keine PIN abgefragt wurde. Man könnte daher von der Vereinbarung einer widerleglichen Vermutung sprechen, dass bei nachgewiesener ordnungsgemäßer Aufzeichnung und nachgewiesener Störungsfreiheit die Ursache für einen Missbrauch aus der Sphäre des Kunden stammt. Solche Vereinbarungen werden für Kleinbetragszahlungsinstrumente zulässig sein, weil sonst die Öffnungsklausel in § 57 Abs 1 Z 2 sinnlos wäre. Dem Kunden muss es aber offenstehen, den wahrscheinlichen Geschehensablauf zu entkräften.[126] Damit hat im Ergebnis jeder Vertragspartner die seiner Sphäre entstammenden Nachweise zu erbringen, was die sachliche Rechtfertigung einer solchen Beweislastregel unterstreicht.[127]

Es wird freilich eine Herausforderung für Kartenaussteller werden, diese Beweislastverteilung transparent in ihren AGB abzubilden. Das Transparenzgebot (§ 6 Abs 3 KSchG) verlangt im Übrigen auch, dass beim Kunden nicht der Eindruck entsteht, die vertragliche Risikoverteilung gelte auch für „reguläre" Zahlungsvorgänge mit der Zahlungskarte, weil hier das gesetzliche Risikoverteilungsmodell der §§ 67 f zwingend ist. Es muss für den Kunden nachvollziehbar sein, welches Risikoverteilungsregime für welchen Fall zur Anwendung kommt.

4.3. Verhältnis zur starken Kundenauthentifizierung

Sodann stellt sich die Frage, bis zu welchem Betrag der eben skizzierte Gestaltungsspielraum bei „Kleinbetragszahlungsinstrumenten" reicht. Hier ist der Zusammenhang von Kleinbetragszahlungsinstrumenten und starker Kundenauthentifizierung zu beachten, denn die Kleinbetragsausnahmen in Art 11 DelVO 2018/389 ähneln zwar der Definition des Kleinbetragszahlungsinstruments in § 57 Abs 1; beide Bereiche decken sich aber nicht völlig.

So ist das Regime für Kleinbetragszahlungsinstrumente für innerstaatliche Zahlungen bis € 60 (einzeln) oder € 300 (gesamt), für grenzüberschreitende Zahlungen bis € 30 (einzeln) oder € 150 (gesamt) anwendbar (§ 57 Abs 1 und 2). Nach Art 11 DelVO 2018/389 kann auf die starke Kundenauthentifizierung hingegen jedenfalls bis € 50 (einzeln) und € 150 (gesamt) verzichtet werden (zu den Auslegungsschwierigkeiten in diesem Zusammenhang s schon 3.1.). Es gibt also zumindest drei verschiedene „Kleinbetragsregime".

Diese Überlappung ist legistisch missglückt, weil sie die Frage aufwirft, bis zu welchem Betrag das Missbrauchsrisiko bei NFC-Zahlungen privatautonom geregelt werden kann: für innerstaatliche Zahlungsvorgänge etwa bis € 150 (Art 11 DelVO 2018/389) oder bis € 300 (§ 57 Abs 2)? Darf der Kartenaussteller Zahlungen ohne PIN bis € 300 zulassen und das Missbrauchsrisiko vertraglich bis zu diesem Betrag auf den Kunden überwälzen, obwohl aufsichtsrechtlich ab € 150 eine starke Kundenauthentifizierung vorgeschrieben ist?

Bei näherem Hinsehen löst sich dieser Widerspruch freilich auf, weil ein vertraglicher Gestaltungsspielraum nach § 57 Abs 1 Z 2 nur bei anonymer Nutzung des Kleinbetragszahlungsinstruments besteht. Besteht aber aufsichtsrechtlich eine Pflicht zur starken Kundenauthentifizierung, darf der Kartenaussteller eine anonyme Nutzung gar nicht zulassen. Dann bleibt es grundsätzlich bei der zwingenden Anwendung der §§ 67 f, wenn nicht einer der Ausnahmetatbestände der DelVO 2018/389 die Zahlung größerer Beträge erlaubt.[128]

Das Problem kann sich also im Regelfall nur stellen, wenn der Kartenaussteller entgegen seiner aufsichtsrechtlichen Pflicht keine starke Kundenauthentifizierung verlangt. Gerade für diesen Fall befreit § 68 Abs 5 den Kunden aber ohnehin bis zur Grenze der betrügerischen Absicht von jeder Haftung (dazu oben 2.2.). Es stellt sich daher abschließend die Frage, ob § 68 Abs 5 vertraglich abbedungen werden kann.

4.4. Vertraglicher Ausschluss des § 68 Abs 5?

§ 57 Abs 1 Z 2 scheint dies auf den ersten Blick nahezulegen, weil nach dieser Bestimmung „§§ 66 und 67 sowie § 68 Abs. 1, 2, 4 **und 5**" bei anonymer Nutzung von Kleinbetragszahlungsinstrumenten dispositiv sind. Auf den zweiten Blick erweist sich § 57 Abs 1 Z 2 freilich als richtlinienwidrig. Art 63 Abs 1 lit b PSD II erlaubt nämlich nur vertragliche Abweichungen von Art 74 Abs 1 und 3 (= § 68 Abs 1–4). Art 74 Abs 2 (= § 68 Abs 5) ist hingegen nicht genannt und kann daher *e contrario* gerade nicht abbedungen werden.

120) *Hoffmann/Rastegar*, WM 2021, 957 (963).
121) BGH XI ZR 294/19 NJW 2021, 1458; dazu im Allgemeinen *Graf* in Kletečka/Schauer, ABGB-ON[1.05] § 879 Rn 311; vgl 5 Ob 556/90 ÖBA 1990, 1009 (*Schauer*).
122) Zur Zulässigkeit solcher „Vermutungsvereinbarungen" *Trenker*, Parteidispositionen 270 f.
123) Vgl *Graf*, ecolex 1999, 239 (240 f).
124) Vgl *Graf*, Telebanking 39 f; *Koziol*, ÖBA 2001, 250 (255).
125) Vgl *Jungmann*, WM 2021, 557 (572); S schon *Koziol*, ÖBA 2001, 250 (255).
126) 2 Ob 133/99v ÖBA 2001, 250 (*Koziol*); *Trenker*, Parteidispositionen 271.
127) Vgl *Schauer*, ÖBA 1990, 1009 (1013).
128) S Art 12 ff, Art 18 DelVO 2018/389: hier bleibt die Kleinbetragsgrenze des § 57 maßgeblich.

Man steht also vor der Frage, ob § 57 Abs 1 Z 2 trotz des entgegenstehenden Wortlauts richtlinienkonform interpretiert werden kann.[129] Dabei besteht Einigkeit, dass das europarechtliche Gebot zur richtlinienkonformen Interpretation auch die wortlautübersteigende richtlinienkonforme Rechtsfortbildung umfasst,[130] eine richtlinienkonforme Auslegung oder Rechtsfortbildung aber nicht *contra legem* erfolgen darf.[131] Die anerkannte Grenze bildet die Übereinstimmung von Gesetzeswortlaut und Wille des Gesetzgebers („*lex lata*-Grenze").[132]

Im Übrigen sind Grund und Grenzen der richtlinienkonformen Interpretation zunehmend heftig umstritten.[133] Die Diskussion entzündet sich insbesondere an der Frage, ob und wie der Wille des nationalen Gesetzgebers zur korrekten Umsetzung der Richtlinie (Generalumsetzungswille) zu berücksichtigen ist.[134] Während manche dem Generalumsetzungswillen in der Regel Vorrang gegenüber der nationalen Norm einräumen wollen,[135] schieben andere den Generalumsetzungswillen beiseite: der Plan des Gesetzgebers sei ausschließlich jenem „*[innerstaatlichen] Normenmaterial zu entnehmen, das unmittelbar anzuwenden ist*".[136]

Eine sachgerechte Lösung dürfte in der Mitte liegen: Der Generalumsetzungswille genießt keinen absoluten Vorrang vor dem „innerstaatlichen Regelungsplan", er kann bei der Auslegung des gesetzgeberischen Willens aber auch nicht einfach ignoriert werden.[137]

Das zeigt sich im hier interessierenden Fall deutlich, wo die Textierung des § 57 Abs 1 Z 2 schlicht ein Redaktionsversehen ist. In den Erläuterungen zu § 57 heißt es nämlich lapidar, dass mit dieser Bestimmung Art 63 PSD II umgesetzt werde.[138] Der Gesetzgeber hatte somit keinen über die korrekte Umsetzung der Richtlinie hinausgehenden Plan, sondern hat sich beim Versuch einer wörtlichen Übernahme des Richtlinientexts schlicht „verschrieben".

Das kann bei der Auslegung des § 57 Abs 1 Z 2 nicht außer Acht gelassen werden. Nachweisliche „Erklärungsirrtümer" des Gesetzgebers werden als Redaktionsversehen im Wege der Auslegung entsprechend der wirklichen Absicht des Gesetzgebers berichtigt.[139] Daran kann sich nichts ändern, wenn die Absicht des Gesetzgebers in der korrekten Umsetzung einer Richtlinie liegt. Es gibt keinen Widerspruch zwischen Generalumsetzungswille und innerstaatlichem Regelungsplan. Man könnte in diesem Zusammenhang auch von einer bloß „*richtlinienorientierten*"[140] Rechtsfindung als Erscheinungsform der historischen Interpretation sprechen.

Dass § 57 Abs 1 Z 2 auf ein Redaktionsversehen zurückgeht, zeigt sich deutlich, wenn man auch § 57 Abs 1 Z 1 in den Blick nimmt, wo ein weiteres Redaktionsversehen schlummert. Dort heißt es nämlich, dass „§ 68 Abs. 4 und 5" vertraglich abbedungen werden können, wenn das Kleinbetragszahlungsinstrument nicht gesperrt werden kann. Damit lehnt sich § 57 Abs 1 Z 1 an den zugrundeliegenden Art 63 Abs 1 lit a PSD II an, wo es in der deutschen Urfassung heißt, dass „Artikel 74 Absatz 2" (= § 68 Abs 5) abbedungen werden kann.

Dabei handelt es sich nun aber seinerseits um ein Redaktionsversehen des Europäischen Gesetzgebers. In allen anderen Sprachfassungen wird nämlich auf „Artikel 74 Absatz 3" (= § 68 Abs 6) Bezug genommen, was auch der einzig sinnvolle Regelungsgehalt ist. Nach Art 74 Abs 3 PSD II muss der Zahlungsdienstleister nämlich das Missbrauchsrisiko bis zur Grenze der betrügerischen Absicht tragen, sobald der Kunde den Verlust, den Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments angezeigt hat. Davon kann aber nach Art 63 Abs 1 lit a PSD II bei Kleinbetragszahlungsinstrumenten vertraglich abgewichen werden, wenn eine Sperre des Kleinbetragszahlungsinstruments technisch nicht möglich ist.[141] Das ist evident sinnvoll: kann ein Zahlungsinstrument nicht gesperrt werden, nützt dem Kartenaussteller auch die Anzeige des Abhandenkommens nichts; daher wäre ein besonderes Haftungsprivileg des Kunden nach der Anzeige sachwidrig. Keinen Sinn würde es hingegen ergeben, wenn gerade bei nicht sperrbaren Zahlungsinstrumenten das Haftungsprivileg bei fehlender starker Kundenauthentifizierung (Art 74 Abs 2 PSD II) dispositiv wäre.

In allen anderen Sprachfassungen bezieht sich Art 63 Abs 1 lit a PSD II daher auf Art 74 Abs 3 PSD II. Der Europäische Gesetzgeber hat den Fehler in der deutschen Sprachfassung mittlerweile auch berichtigt und Art 63 Abs 1 lit a auf Art 74 Abs 3 bezogen.[142] Dem österreichischen Gesetzgeber ist nicht nur diese Berichtigung entgangen; ihm ist im Anschluss an § 57 Abs 1 Z 1 vielmehr in Z 2 auch ein weiteres Redaktionsversehen unterlaufen.

Diese Fehler sollte der österreichische Gesetzgeber entsprechend korrigieren. Bis dahin lässt der Blick auf das Europarecht aber keinen Zweifel daran, dass sich der Gesetzgeber im unübersichtlichen Dickicht von Normverweisen planwidrig verirrt hat. § 57 Abs 1 ist daher einer berichtigenden Auslegung zugänglich. Z 1 muss sich auf § 68 Abs 6, und Z 2 muss sich auf § 68 Abs 1 – 4 sowie Abs 6 beziehen. § 68 Abs 5 ist hingegen bei richtigem Verständnis auch für Kleinbetragszahlungsinstrumente zwingend.[143]

Daher kann der Kunde – nach der von der bislang hA im Schrifttum vertretenen Auslegung des Art 11 DelVO 2018/389 (dazu oben 3.1.) – grundsätzlich nur bis maximal € 150 zur Risikotragung verpflichtet werden, es sei denn einer der Ausnahmetatbestände in der DelVO 2018/389 erlaubt die Zahlung größerer Beträge ohne starke Kundenauthentifizierung (etwa an der Mautstelle).[144] Diese Auslegung ist auch deshalb vorzugswürdig, weil dem Kunden so der vom Aufsichtsrecht bezweckte Schutz erhalten bleibt.

4.5. Zusammenschau: Bestätigung durch EuGH C-287/19 *DenizBank*

Die eben angestellten Überlegungen bestätigen schließlich die unter 3.3. vertretene Ansicht zur Reichweite des Haftungsprivilegs bei fehlender starker

129) Zweifelnd *Koch*, ÖBA 2021, 123 (133 f).
130) Statt aller *Perner*, EU-Richtlinien 77 mwN.
131) EuGH Rs C-268/06 *Impact*; EuGH C-212/04 Rs *Adeneler*; *Perner*, EU-Richtlinien 94 ff. 132) *Schauer* in Kletečka/Schauer, ABGB-ON[1.02] § 6 Rn 31; *Schürnbrand*, JZ 2007, 910 (916 f).
133) *P. Bydlinski*, JBl 2015, 2 (5); *ders*, RZ 2019, 30.
134) S zur Rs *Lexitor* etwa *Beham*, ZFR 2021, 116; *P. Bydlinski*, ZFR 2021, 212; zur Rs *Endress/Allianz* S *Schauer*, VR 2017/1-2, 33 (45); *Perner/Spitzer*, Rücktritt 26 ff
135) Vgl *Roth/Jopen* in Riesenhuber, Methodenlehre[4] Rn 64 mwN; für „Auswahlregel" *Perner*, EU-Richtlinien 92 ff.
136) *Schauer*, VR 2017/1-2, 33 (45).
137) Dazu in unterschiedlichen Schattierungen *P. Bydlinski*, JBl 2015, 2 (5); *Canaris*, FS F. Bydlinski (2002) 47 (96 ff, 100); *Perner*, EU-Richtlinien 87 ff; *Perner/Spitzer*, Rücktritt 30.
138) ErlRV 11 BlgNR XXVI. GP, 17.
139) *F. Bydlinski*, Methodenlehre[2] 393; *Kodek* in Rummel/Lukas, ABGB[4] § 6 ABGB Rn 104; *Schauer* in Kletečka/Schauer, ABGB-ON[1.02] § 6 Rn 16.
140) *Perner*, EU-Richtlinien 87 mwN.
141) EuGH Rs C-287/19 *DenizBank/VKI* Rn 94 ff.
142) Berichtigung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25.11.2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/46/EG, ABl L 169 vom 28.6.2016.
143) So auch *Jungmann*, WM 2021, 557 (569 ff), der freilich im Übrigen anderer Ansicht ist.
144) S Art 12 ff, Art 18: hier bleibt die Kleinbetragsgrenze des § 57 maßgeblich.

Kundenauthentifizierung (§ 68 Abs 5). Einerseits hat sich gezeigt, dass dieses Haftungsprivileg auch bei anonymen NFC-Zahlungen zwingend ist. Andererseits hat der EuGH in der *DenizBank*-Entscheidung ausgesprochen, dass der Kartenaussteller bei anonymen NFC-Zahlungen vertraglich grundsätzlich auch vom Missbrauchsrisiko befreit werden kann.

Bei anonymen NFC-Zahlungen erfolgt aber gerade keine starke Kundenauthentifizierung. Dann kann man den zwingenden § 68 Abs 5 nicht so auslegen, dass das besondere Haftungsprivileg bei fehlender starker Kundenauthentifizierung auch zur Anwendung kommt, wenn der Kartenaussteller aufsichtsrechtlich gar nicht zur starken Kundenauthentifizierung verpflichtet ist (etwa bei NFC-Zahlungen innerhalb der von Art 11 DelVO 2018/389 gezogenen Kleinbetragsgrenzen). Sonst würde man Kartenausstellern nämlich den vom EuGH mit einer Hand gegebenen vertraglichen Gestaltungsspielraum mit der anderen Hand wieder nehmen.[145)]

5. Zusammenfassung

Zusammenfassend lässt sich sagen, dass der Missbrauch von Zahlungskarten auch im „neuen" Zahlungsverkehrsrecht ein schwieriges Problem bleibt. Das Zusammenspiel von Zivil- und Aufsichtsrecht, von Europarecht und nationalem Recht verläuft nicht immer friktionsfrei. Ineinander verschachtelte Rechtsakte, ihre unklare teleologische Fundierung und ihre schwere Lesbarkeit sowie Redaktionsfehler des europäischen wie des nationalen Gesetzgebers erschweren die Auslegung. Im Wesentlichen lassen sich aber folgende Schlussfolgerungen ziehen:

1. Neuralgischer Punkt des „neuen" Zahlungsverkehrsrechts ist die Grenze zwischen leichter und grober Fahrlässigkeit. Nimmt man diese Grenze ernst, bewirkt dies eine erhebliche Privilegierung des leicht fahrlässigen Kunden gegenüber dem allgemeinen Zivilrecht.
2. Erfolgt keine starke Kundenauthentifizierung, haftet auch der grob sorglose und selbst der vorsätzlich handelnde Kunde nicht (§ 68 Abs 5). Das gilt aber nur, wenn der Kartenaussteller aufsichtsrechtlich zur starken Kundenauthentifizierung verpflichtet ist. Unterbleibt die starke Kundenauthentifizierung hingegen im Einklang mit den aufsichtsrechtlichen Vorgaben (etwa bei kontaktlosen Kleinbetragszahlungen), haftet der Kunde „schon" bei grober Fahrlässigkeit.
3. Für kontaktlose Kleinbetragszahlungen mit der NFC-Funktion (Near Field Communication) eröffnet die *DenizBank*-Entscheidung des EuGH Kartenausstellern vertragliche Gestaltungspielräume. Für den Missbrauch ein und derselben Zahlungskarte können daher zwei unterschiedliche Regelungsregime Anwendung finden.
4. Dabei kann das Risiko eines Verlusts oder Diebstahls der Zahlungskarte grundsätzlich auch auf den Kunden verlagert werden (§ 57), sodass der Kunde nicht erst ab grober Fahrlässigkeit haftet. Nicht überwälzt werden kann hingegen das Risiko eines technischen Missbrauchs der Zahlungskarte (§ 879 Abs 3 ABGB).
5. Nicht abbedungen werden kann auch das Haftungsprivileg des Kunden bei fehlender, aber aufsichtsrechtlich verpflichtender starker Kundenauthentifizierung. Daher reicht der vertragliche Gestaltungsspielraum nur bis zu den in der DelVO 2018/389 normierten Betragsgrenzen. Folgt man der bislang hA zur Bestimmung dieser Betragsgrenzen, kann der Kunde somit vertraglich nur bis maximal € 150 zur Risikotragung verpflichtet werden, es sei denn einer der Ausnahmetatbestände in der DelVO 2018/389 erlaubt die Zahlung größerer Beträge ohne starke Kundenauthentifizierung.
6. Wollen Kartenaussteller ihre vertraglichen Gestaltungsspielräume ausnützen, stehen sie vor der schwierigen Herausforderung, diese Rechtslage in AGB transparent abzubilden (§ 6 Abs 3 KSchG). Dieser Aufgabe kommt mit Blick auf mögliche Verbandsklagen (§§ 28 f KSchG) freilich besondere Bedeutung zu. ◆

145) Vgl *Habersack*, EuZW 2020, 767 (768).

Literaturverzeichnis

Baumbach / Hefermehl / Casper, Wechselgesetz, Scheckgesetz, Recht des Zahlungsverkehrs[24] Rn E/391.

Beham, Richtlinienkonforme Auslegung und nationaler Auslegungsprotektionismus, ZFR 2021, 116.

Bydlinski P., Die Auslegung des § 16 Abs 1 aF VKrG im Lichte der EuGH-Entscheidung Lexitor, ZFR 2021, 212.

Bydlinski P., Richtlinienkonforme „gesetzesübersteigende" Rechtsfindung und ihre Grenzen – eine methodische Vergewisserung anlässlich 20 Jahre EU-Mitgliedschaft, JBl 2015, 2.

Bydlinski P., Richtlinienkonforme Rechtsfindung: Der OGH (4 Ob 62/16w), die Lex-lata-Grenze und die Kernfunktion von Gesetzesrecht, RZ 2019, 30.

Canaris, Bankvertragsrecht I[3] (1988).

Canaris, Die richtlinienkonforme Auslegung und Rechtsfortbildung im System der juristischen Methodenlehre, FS F. Bydlinski (2002) 47.

Casper / Pfeifle, Missbrauch der Kreditkarte im Präsenz- und Mail-Order-Verfahren nach neuem Recht, WM 2009, 2343.

Casper / Terlau (Hrsg), ZAG[2] (2020).

Drescher / Fleischer / K. Schmidt, Münchener Kommentar zum HGB VI[4] (2019).

F. Bydlinski, Juristische Methodenlehre und Rechtsbegriff[2] (Nachdruck 2011).

Faber, Vertragsänderungen durch Zustimmungsfiktion bei Verbraucherverträgen über Zahlungsdienste in rechtsvergleichender Betrachtung, ÖBA 2021, 305.

Fasching, Lehrbuch des österreichischen Zivilprozeßrechts[2] (1990).

Fellner, Die Bankomatkarte (2003).

Foglar-Deinhardstein, Zustimmungsfiktion reloaded: Der EuGH hat gesprochen! VbR 2021, 9.

Graf, Missbrauch von Zahlungsinstrumenten: Schadensteilung bei Verschulden des Kunden? RdW 2011, 587.

Graf, Rechtsfragen des Telebanking (1997).

Graf, Wer haftet beim Bankomatkartenmißbrauch? ÖBA 2007, 531.

Graf, Wer haftet beim Telebanking? ecolex 1999, 239.

Gsell / Krüger / Lorenz / Reymann, Beck-OGK (2021).

Habersack, Die PSD 2 im Visier des EuGH, EuZW 2020, 767.

Haghofer, Starke Kundenauthentifizierung nach dem ZaDiG, VbR 2018, 173.

Harrich, ZaDiG: Zivilrechtliche Aspekte des Zahlungsdienstegesetzes (2011).

Hau / Poseck, Beck'scher Onlinekommentar BGB.

Hoffmann, Kundenhaftung unter der Neufassung der Zahlungsdiensterichtlinie, VuR 2016, 243.

Hoffmann / Rastegar, Kontaktlose Zahlungen im Privatrecht, WM 2021, 957.

Hofmann, Das neue Haftungsrecht im Zahlungsverkehr, BKR 2018, 62.

Hofmann, Haftung im Zahlungsverkehr, BKR 2014, 105.

Iro / Koziol, Risikotragung bei gefälschten Aufträgen an die Bank, ÖBA 2003, 129.

Jungmann, Das System von Haftung beim missbräuchlichen Kreditkarteneinsatz ohne starke Kundenauthentifizierung, ZBB 2020, 1.

Jungmann, Das zahlungsdiensterechtliche Regelungsregime für „Proximity Payments“, WM 2021, 557.

Kellner, Zustimmungsfiktionsklauseln: Das nächste Kapitel, ÖBA 2020, 539.

Kletečka / Schauer (Hrsg), ABGB-ON.

Koch, Anm zu EuGH 11.11.2020, C-287/19, ÖBA 2021, 123.

Koch, Prüfung und Bearbeitung eines Überweisungsauftrags durch den beauftragten Zahlungsdienstleister nach ZaDiG 2018/PSD II, ÖBA 2019, 106.

Kodek, Haftung für nicht autorisierte Zahlungsvorgänge (§§ 67, 68 ZaDiG 2018), ÖBA 2021, 19.

Koller, Die Verteilung des Scheckfälschungsrisikos zwischen Kunde und Bank, NJW 1981, 2433.

Köndgen, Das neue Recht des Zahlungsverkehrs, JuS 2011, 481.

Koziol, Anm zu 2 Ob 133/99y, ÖBA 2001, 250.

Koziol, Rechtsfolgen der Verletzung einer Schadensminderungspflicht – Rückkehr der archaischen Kulpakompensation? ZEuP 1998, 593.

Koziol/P. Bydlinski / Bollenberger, ABGB Kurzkommentar[6] (2020).

Kurschel, Wer trägt den Schaden? „Verdoppelte“ und verlorene Bankomatkarten, ecolex 1990, 79.

Kurz, Inhaltskontrolle von Bankkartenbedingungen und Missbrauchshaftung nach dem ZaDiG, ecolex 2017, 836.

Langenbucher / Bliesener / Spindler, Bankrechts-Kommentar[3] (2020).

Linardatos, Das Haftungssystem im bargeldlosen Zahlungsverkehr (2013).

Linardatos, Der Kommissionsvorschlag für eine Zahlungsdiensterichtlinie II – Ein Überblick zu den haftungsrechtlichen Reformvorhaben, WM 2014, 300.

Mülbert, Was Kreditinstitute für erforderlich halten dürfen – Risikoverteilung zwischen Kreditinstitut und Kunde bei Zahlungen an betrügerische Dritte, FS Canaris (2007) 271.

Oechsler, Die Haftung nach § 675v im kreditkartengestützten Mailorderverfahren, WM 2010, 1381.

Omlor, Online-Banking unter Geltung der Zweiten Zahlungsdiensterichtlinie (PSD II), BKR 2019, 105.

Omlor, Zahlungsdiensteaufsichtsrecht im zivilrechtlichen Pflichtengefüge, WM 2018, 57.

Perner, EU-Richtlinien und Privatrecht (2012).

Perner / Spitzer, Rücktritt von der Lebensversicherung (2020).

Prankl, Zustimmungsfiktionsklauseln in Zahlungsdienste-Rahmenverträgen unterliegen Inhalts- und Transparenzkontrolle, ecolex 2021, 713.

Rabl Th., „Böse“ und „gute“ Zustimmungsfiktionen, ecolex 2021, 693.

Roth / Jopen, Die richtlinienkonforme Auslegung, in Riesenhuber (Hrsg), Europäische Methodenlehre[4] (2021) 377.

Rummel / Lukas, Kommentar zum ABGB[4] (2015).

Säcker / Rixecker / Oetker / Limperg, Münchener Kommentar zum BGB VI[8] (2020).

Schauer, Anm zu 5 Ob 556/90, Spätrücktritt in der Lebensversicherung – die Entscheidung EuGH Endress/Allianz und ihre Konsequenzen für das österreichische Recht, VR 2017/1-2, 33.

Schauer, ÖBA 1990, 1009 (1013).

Schmid, (Starke) Kundenauthentifizierung: Aufsichtsrecht und Zivilrecht, in *Emmenegger*, Zahlungsverkehr (2018) 67.

Schürnbrand, Die Grenzen richtlinienkonformer Rechtsfortbildung im Privatrecht, JZ 2007, 910.

Schweighofer, Schutzbekleidung und Mitverschulden im Sport (2019).

Taupitz, Kreditkartenmißbrauch: Thesen zur zulässigen Verteilung des Haftungsrisikos in AGB, NJW 1996, 217.

Terlau, Die zweite Zahlungsdiensterichtlinie – zwischen technischer Innovation und Ausdehnung des Aufsichtsrechts, ZBB 2016, 122.

Trenker, Einvernehmliche Parteidispositionen im Zivilprozess (2020).

Tuder, Grundsatzfragen des ZaDiG (2018).

van Gelder, Phisher, Pharmer & Co, FS Nobbe (2009) 55 (64).

Vogel, Mißbrauch von Kreditkarten (2000).

Vogel, Risikoverteilung bei Diebstahl oder Verlust der Kreditkarte, ÖBA 2001, 767.

Weilinger / Knauder / Miernicki (Hrsg), ZaDiG 2018 (2020).

Werner, Wesentliche Änderungen des Rechts der Zahlungsdienste durch Umsetzung der Zweiten EU-Zahlungsdiensterichtlinie in deutsches Recht, WM 2018, 449.

Zahrte, Neuerungen im Zahlungsdiensterecht, NJW 2018, 337.