

Christian Hülsenbeck

Zivil- und aufsichtsrechtliche Grundfragen des *Mobile Payments*

Wissenschaftliche Beiträge aus dem Tectum Verlag

Reihe Rechtswissenschaft

Wissenschaftliche Beiträge aus dem Tectum Verlag

Reihe Rechtswissenschaft

Band 172

Christian Hülsenbeck

Zivil- und aufsichtsrechtliche Grundfragen des Mobile Payments

Tectum Verlag

Christian Hülsenbeck
Zivil- und aufsichtsrechtliche Grundfragen des Mobile Payments

Wissenschaftliche Beiträge aus dem Tectum Verlag
Reihe: Rechtswissenschaft; Bd. 172

Zugl. Diss. Universität zu Köln 2021

© Tectum – ein Verlag in der Nomos Verlagsgesellschaft, Baden-Baden 2022
ePDF 978-3-8288-7834-1
(Dieser Titel ist zugleich als gedrucktes Werk unter der ISBN
978-3-8288-4735-4 im Tectum Verlag erschienen.)
ISSN 1861-7875

Alle Rechte vorbehalten

Besuchen Sie uns im Internet
www.tectum-verlag.de

Bibliografische Informationen der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie; detaillierte bibliografische
Angaben sind im Internet über <http://dnb.d-nb.de> abrufbar.

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Jahr 2021 von der Rechtswissenschaftlichen Fakultät der Universität zu Köln als Dissertation angenommen. Die Disputation fand am 26. August 2021 statt.

Mein besonderer Dank gilt zunächst meinem Doktorvater Herrn Professor Dr. Klaus Peter Berger, LL.M., der mir erfreulicherweise jederzeit den notwendigen wissenschaftlichen Freiraum gewährte und nützliche Anregungen zum Aufbau der Arbeit zuteilwerden ließ. Ausdrücklich zu würdigen ist ferner die äußerst zeitnahe Erstellung des Erstgutachtens. Herrn Professor Dr. Christian Rolfs danke ich gleichermaßen für die zügige Zweitkorrektur. Beiden möchte ich für das konstruktive sowie angenehme Prüfungsgespräch danken.

Weitere Anerkennung kommt dem Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. sowie den konkreten Gesprächspartnerinnen und -partnern zu, die im Rahmen eines aufschlussreichen Interviews zahlreiche wesentliche Informationen mit mir geteilt haben.

Besonders herzlich danke ich zudem meinen Freundinnen und Freunden, die mich jeweils auf unterschiedliche Weise großartig unterstützt haben. Zu diesen zählen aus dem fachlichen Bereich insbesondere David, Deborah, Hannes und Larissa, die mir immerfort als wertvolle und interessierte Gesprächspartner zu verschiedensten Themen zur Seite standen. Lina verdanke ich darüber hinaus die grundlegende Idee zum Thema dieser Arbeit, der daher nochmals besondere Anerkennung gebührt. Auf gleicher Stufe zu nennen sind vor allem Alexandra, Carolin, Eva, Jan, Julian, Julius, Lukas und Stephan, die vorwiegend die mühevollen Aufgabe des Korrekturlesens übernommen haben. Hervorheben möchte ich insofern Anna und Michael, bei denen Worte nicht ausdrücken können, was ich ihnen gegenüber an Dankbarkeit für ihre ebenso hervorragende wie umfassende Unterstützung empfinde. Speziell möchte ich auch Marcel danken, der es mir erst ermöglichte,

meine theoretischen Überlegungen wiederholt in der Praxis zu erproben.

Von ganzem Herzen danke ich schließlich meinen Eltern Klaus und Monika, meinen Großeltern Elfriede, Josef und Resi sowie meinen Großtanten Marianne und Marlies. Besonders meine Eltern ermöglichen mir die Verwirklichung meiner Ziele, indem sie mich auf meinem gesamten Lebensweg mit ihrem liebevollen Rückhalt, ihrem uneingeschränkten Vertrauen sowie ihrer außergewöhnlichen Unterstützung begleitet haben. Aus diesen und unzähligen weiteren Gründen ist ihnen diese Arbeit gewidmet.

Köln, im Januar 2022

Christian Hülsenbeck

Inhaltsverzeichnis

Abkürzungsverzeichnis	XV
Einleitung	1
A. Mobile Payment in Deutschland, Europa und der Welt	1
B. Gegenstand und Ziel der Untersuchung	5
C. Gang der Darstellung	7
1. Kapitel: Grundlagen der rechtlichen Untersuchung	11
§ 1 Geschäftsmodell samt technologischer Aspekte	11
A. Grundlegende Vorüberlegungen	11
B. Hinterlegungsprozess und Komfortstufen	14
C. Technologische Aspekte	17
§ 2 Rechtsrahmen	22
A. Unionebene	22
I. Ursprüngliche Empfehlungen 87/598/EWG, 88/590/EWG und 97/489/EG ...	23
II. Die Zahlungsdiensterichtlinien 2007/64/EG und (EU) 2015/2366	24
III. Delegierte Verordnung (EU) 2018/389	27
B. Nationale Ebene	29
I. Aufsichtsrecht	30
II. Zivilrecht	31

2. Kapitel: Aufsichtsrechtliche Grundfragen des Mobile Payments	35
§ 3 Erlaubnispflicht für das Erbringen von Zahlungsdiensten	
gemäß § 10 Abs. 1 S. 1 ZAG	36
A. Zahlungsdienste	36
I. Tatbestandsmäßiges Vorliegen eines Zahlungsdienstes	
gemäß § 1 Abs. 1 S. 2 ZAG	37
1. Zahlungsgeschäft	38
a) Zahlungskartengeschäft	41
aa) girocard mobil als Zahlungsinstrument	41
(1) Grundlagen und Erteilung des Zahlungsauftrags	42
(2) Auslösen des Zahlungsvorgangs	47
(3) Einordnung als Instrument und/oder Verfahren	48
(4) Personalisierung und Zwischenergebnis	51
bb) Einordnung als Zahlungskarte oder ähnliches	
Zahlungsinstrument	51
b) Lastschriftgeschäft	54
c) Überweisungsgeschäft	55
2. Akquisitionsgeschäft	57
a) Ausgabe von Zahlungsinstrumenten	57
b) Annahme und Abrechnung von Zahlungsvorgängen	58
3. Finanztransfergeschäft	61
4. Zahlungsauslösedienste	63
5. Sonstige Zahlungsdienste	64
II. Ausnahmetatbestände gemäß § 2 Abs. 1 ZAG	65
1. Handelsvertreter	65
2. Technische Dienstleister	66
3. Spezielle Verbundzahlungssysteme oder sehr begrenztes	
Produktspektrum	68
4. Weitere Ausnahmen	69
B. Kein Zahlungsdienstleister i. S. d. § 1 Abs. 1 S. 1 Nr. 2-5 ZAG	71
I. Kreditinstitute	71
II. Zentralbanken	73
III. Körperschaften des öffentlichen Rechts	73
IV. E-Geld-Institute	74
V. Schlussfolgerung: Zahlungsinstitut i. S. d. Nummer 1?	76
C. Sonstige Tatbestandsvoraussetzungen	79

§ 4 Starke Kundenauthentifizierung beim Mobile Payment	80
A. Grundsätzliche Pflicht zur starken Kundenauthentifizierung	80
I. Auslösen eines elektronischen (Fern-)Zahlungsvorgangs	83
1. Elektronisch	83
2. Abgrenzung zum Fernzahlungsvorgang	85
a) Grundlagen	85
b) Einschränkendes Kriterium	88
3. Zwischenergebnis	89
II. Online Zugriff auf Zahlungskonto	90
III. Sonstige riskante Handlung	92
B. Anforderungen für die Durchführung der starken Kundenauthentifizierung	92
I. Einfache Authentifizierung als Basis	93
II. Spezifische Anforderungen der starken Kundenauthentifizierung	96
1. Vertraulichkeit der Authentifizierungsdaten	96
2. Authentifizierung durch mindestens zwei unabhängige Elemente	97
a) Elemente der einzelnen Kategorien	97
aa) Kategorie Wissen	98
bb) Kategorie Besitz	100
cc) Kategorie Inhärenz	102
b) Generierung eines Authentifizierungscodes durch unabhängige Elemente	103
C. Ausnahmen von der starken Kundenauthentifizierung	106
I. Kontaktlose Zahlungen am POS	107
II. Unbeaufsichtigte Zahlungsautomaten	110
III. Kleinbetragszahlungen	111
IV. White List	113
V. Weitere Ausnahmen	115
§ 5 Zusammenfassung	116
3. Kapitel: Zivilrechtliche Grundfragen des Mobile Payments	119
§ 6 Zivilrechtliches Fundament	119
A. Anwendbare Vorschriften und Begriffsbestimmungen	119
B. Zentrale Haftungsnorm samt haftungsbegründendem Tatbestand	122
I. Nicht autorisierter Zahlungsvorgang	124
II. Pflichtverletzung des Zahlers	125
III. Verschulden	131

IV. Kein Haftungsausschluss gemäß § 675v Abs. 4 S. 1 BGB	131
1. Kein Verlangen der starken Kundenauthentifizierung	132
2. Keine Akzeptanz der starken Kundenauthentifizierung	132
3. Teleologische Reduktion des § 675v Abs. 4 S. 1 BGB?	134
§ 7 Haftungsrechtliche Besonderheiten des Mobile Payments	138
A. Schutz der girocard(s) mobil durch eine Sicherungsmaßnahme	139
I. Privilegierte girocard mobil?	142
1. Von Anfang an privilegierte girocard mobil Nr. 1.1?	142
2. Im Nachhinein privilegierte girocard mobil Nr. 1.1 ff.?	146
II. Nicht privilegierte girocard(s) mobil	151
1. Konkretisierung der Pflicht des § 675I Abs. 1 S. 1 BGB	152
2. Rechtliche Bewertung	161
a) Sicherheitsqualität einer einzelnen Schutzbarriere	162
aa) Schutzbarriere mit einer Schutzmöglichkeit	164
(1) Biometrische Merkmale	164
(2) Geheimcode	166
(3) Muster	171
bb) Schutzbarriere mit mehreren Schutzmöglichkeiten	175
b) Sicherheitsqualität der verschiedenen Sicherungsmaßnahmen	177
aa) Nicht priorisierte girocard(s) mobil	177
(1) Sicherungsmaßnahme mit einer Schutzbarriere	178
(a) Schutzbarriere 1 oder Schutzbarriere 2	179
(b) Schutzbarriere 3	181
(2) Sicherungsmaßnahme mit zwei Schutzbarrieren	182
(3) Sicherungsmaßnahme mit drei Schutzbarrieren	185
(4) Keine Sicherungsmaßnahme	185
(5) Zwischenergebnis	186
bb) Priorisierte girocard(s) mobil	187
(1) Sonstige BezahlApp(s)	188
(a) Komfortstufe 3	188
(b) Komfortstufe 2 oder Komfortstufe 1	189
(c) Sonderfall: Softwarefehler im Zusammenhang mit der Schutzbarriere 2	191
(2) Ursprüngliche Standard BezahlApp	193
(a) Komfortstufe 3	194
(b) Komfortstufe 2	194
(c) Komfortstufe 1	195

(d) Sonderfall: Softwarefehler im Zusammenhang mit der Schutzbarriere 2	197
B. Wechselseitiger Schutz der im mobilen Endgerät gespeicherten PIN(s) und girocard(s) mobil durch Komplementärmaßnahme	198
I. Konkretisierung der Pflicht des § 675I Abs. 1 S. 1 BGB	198
II. Rechtliche Bewertung	205
1. Nicht privilegierte girocard(s) mobil	207
a) Sicherheitsqualität der verschiedenen PIN-bezogenen Maßnahmen	208
aa) Bloßes Speichern der Klartext-PIN im mobilen Endgerät	209
bb) Schwerpunkt: Versteck	210
cc) Schwerpunkt: Verschlüsselung	212
(1) Geburtsdatum	213
(2) Telefonnummer	213
(3) Sonstige Verschlüsselungssysteme	215
dd) Schutz der die jeweilige PIN enthaltenden App	216
b) Sicherheitsqualität der verschiedenen Komplementärmaßnahmen	217
2. Privilegierte girocard mobil	222
a) Im Nachhinein privilegierte girocard mobil Nr. 1.1 ff.	223
b) Von Anfang an privilegierte girocard mobil Nr. 1.1	223
C. Analog notierte PIN(s) und zugehörige girocard(s) mobil	224
D. Auswirkungen der Identität einer PIN und eines als Schutzmöglichkeit verwendeten Geheimcodes	227
I. Ausgangspunkt: Geheimcode	228
II. Ausgangspunkt: Gespeicherte PIN	233
III. Gemeinsamkeiten beider Konstellationen	236
E. Zusätzliche spezifische Pflichten hinsichtlich des mobilen Endgeräts und Wechselwirkungen mit den vorstehenden Pflichten	237
I. Mitführen des mobilen Endgeräts in der Öffentlichkeit	237
II. Aufbewahrung des mobilen Endgeräts an bestimmten Orten	239
III. Aktive Weitergabe des mobilen Endgeräts und Besonderheiten in bestimmten Notsituationen	246
F. Spezifische Gefahren mobiler Endgeräte im Hinblick auf Schadsoftware	248
I. Maßnahmen zur Abwehr von Schadsoftware	251

II. Infektionsquellen des mobilen Endgeräts	253
1. Download von Apps aus nicht lizenzierten App Stores nach Rooting/Jailbreaking	254
2. Drive-by-Infektion	255
3. Aktive Verbindung mit nicht vertrauenswürdigen Quellen	256
4. Öffnen unbekannter Dateien	257
5. Angriff über aktivierte Datenverbindungen	257
III. Exkurs: Eingabe der PIN auf dem mobilen Endgerät	258
G. Angriff auf HCE-Server	259
§ 8 Zusammenfassung	260
Fazit	267
Anhang	271
Literaturverzeichnis	279
Literaturverzeichnis Internetquellen	287

Abkürzungsverzeichnis

a. A.	andere Auffassung
ABl.	Amtsblatt
Abs.	Absatz/Absätze
aE	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
aF	alte Fassung
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
Anm.	Anmerkung
App	Applikation
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BankR	Bankrecht
Begr.	Begründung
BGB	Bürgerliches Gesetzbuch
BGBL	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung des Bundesgerichtshofs in Zivilsachen
BI	Bankinformation
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
bspw.	beispielsweise
BT	Bundestag
BVR	Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa

CB	Compliance-Berater
CDCVM	Consumer Device Cardholder Verification Method
CR	Computer und Recht, Zeitschrift für die Praxis des Rechts der Informationstechnologie
CRR-Kreditinstitut	Capital-Requirements-Regulation-Kreditinstitut
DB	Der Betrieb
DK	Deutsche Kreditwirtschaft
Drucks.	Drucksache
DSGV	Deutscher Sparkassen- und Giroverband
dt.	deutsch
DuD	Datenschutz und Datensicherheit
EBA	Europäische Bankenaufsichtsbehörde
EG	Europäische Gemeinschaft
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
et al.	und andere
etc.	et cetera
EU	Europäische Union
EuCML	Journal of European Consumer and Market Law
EWG	Europäische Wirtschaftsgemeinschaft
EZB	Europäische Zentralbank
f./ff.	folgend/folgende
FCA	Financial Conduct Authority (Britische Finanzaufsichtsbehörde)
FinDAG	Gesetz über die Bundesanstalt für Finanzdienstleistungsaufsicht
Fn.	Fußnote
Frankfurt a. M.	Frankfurt am Main
ggf.	gegebenenfalls
GWR	Gesellschafts- und Wirtschaftsrecht
HCE	Host Card Emulation
HdB	Handbuch
HGB	Handelsgesetzbuch
HK	Handkommentar

Hs.	Halbsatz
i. d. R.	in der Regel
i. e. S.	im engeren Sinne
i. H. v.	in Höhe von
i. R. d.	im Rahmen des/der
i. S. d.	im Sinne des/der
i. S. e.	im Sinne eines/r
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IBAN	Internationale Bankkontonummer
inkl.	inklusive
insb.	insbesondere
jurisPR-BKR	Rechtsportal juris, PraxisReport Bankrecht
JuS	Juristische Schulung, Zeitschrift für Studium und Referendariat
K&R	Kommunikation und Recht
Kfz	Kraftfahrzeug
KPMG	KPMG AG Wirtschaftsprüfungsgesellschaft
KWG	Gesetz über das Kreditwesen
LG	Landgericht
Lit.	Literaturverzeichnis
lit.	littera (Buchstabe)
MaSI	Mindestanforderungen an die Sicherheit von Internetzahlungen
max.	maximal
min.	mindestens
MüKo	Münchener Kommentar zum Bürgerlichen Gesetzbuch
NFC	Near Field Communication (dt.: Nahfeldkommunikation)
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift, Rechtsprechungs-Report Zivilrecht
Nr.	Nummer
o. Ä.	oder Ähnliches/m

OLG	Oberlandesgericht
ÖPNV	Öffentlicher Personennahverkehr
PIN	Persönliche Identifikationsnummer
POS	Point of Sale
PSD 2	siehe ZDRL II
PWC	PricewaterhouseCoopers GmbH
RegE	Regierungsentwurf
RL	Richtlinie
Rn.	Randnummer
RTS SCA	Regulatory Technical Standards on strong customer authentication and secure communication under PSD2
S.	Seite oder Satz, je nach Zusammenhang
s. o.	siehe oben
SEPA	Single European Payments Area
sog.	sogenannte/sogenanntes/sogenannter/sogenannten
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
u. a.	unter anderem
UG	Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29. Juli 2009
vgl.	vergleiche
VuR	Verbraucher und Recht
WM	Zeitschrift für Wirtschafts- und Bankrecht, Wertpapier-Mitteilungen
z. B.	zum Beispiel
ZAG	Gesetz über die Beaufsichtigung von Zahlungsdiensten
ZBB	Zeitschrift für Bankrecht und Bankwirtschaft
ZD	Zeitschrift für Datenschutz

ZDRL I	Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG
ZDRL II	Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 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 2007/64/EG
ZDUG I	Gesetz zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zahlungsdiensterichtlinie (Zahlungsdiensteumsetzungsgesetz) vom 25. Juni 2009
ZDUG II	Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie vom 17. Juli 2017
ZfgK	Zeitschrift für das gesamte Kreditwesen
ZVglRW	Zeitschrift für Vergleichende Rechtswissenschaft

