

Inhaltsübersicht

Vorwort	VII
Inhaltsübersicht	IX
Inhaltsverzeichnis.....	XI
Literaturverzeichnis	XXIII
Materialienverzeichnis	XLVII
Abkürzungsverzeichnis.....	LI
Einleitung	1
1. Teil: Terminologie.....	7
A. Unautorisierte Zahlung	9
B. Autorisierung	11
C. Zahlungsauftrag	45
D. Weitere Begriffe	55
2. Teil: Angriffsmethoden.....	101
A. Überblick	103
B. Unterschriftenfälschung.....	105
C. Physische Entwendung des Zahlungsinstruments	107
D. Skimming (Kartendoublette)	109
E. Social Engineering.....	111
F. Hacking.....	139
G. Fazit: Vorliegen einer unautorisierten Zahlung?	169
3. Teil: Beweisrecht in Bezug auf die Autorisierung.....	173
A. Einleitung.....	175
B. Beweislast für die Autorisierung	177
C. Zulässigkeit des Anscheinsbeweises für die Autorisierung?	189
D. Fazit	231
4. Teil: Rechtsansprüche der Beteiligten	233
A. Überblick: Risikoverteilung und Prüfreihenfolge	235
B. Schicksal des Aufwendungsersatzanspruchs der Bank	237
C. Erstattungsanspruch des Kunden.....	255
5. Teil: Schadenersatzanspruch der Bank im Besonderen.....	309
A. Überblick	311
B. Beschränkte Anreizhaftung des Kunden	315
C. Unbeschränkte Verschuldenshaftung des Kunden	337
D. Verminderung und Ausschluss der Kundenhaftung.....	393

Inhaltsübersicht

6. Teil: Weitere Fragen der Bank-Kunden-Beziehung.....	405
A. Beweisrecht in Bezug auf die Kundenhaftung	407
B. Abdingbarkeit der Vorschriften durch die Vertragsparteien	423
C. Schadenersatzanspruch des Kunden.....	425
7. Teil: Prüfung der Anspruchsgrundlagen im Missbrauchsfall.....	427
8. Teil: Gesamtfazit	441
Stichwortregister	449

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
Inhaltsverzeichnis.....	XI
Literaturverzeichnis	XXIII
Materialienverzeichnis	XLVII
Abkürzungsverzeichnis.....	LI
Einleitung	1
1. Teil: Terminologie.....	7
A. Unautorisierte Zahlung	9
B. Autorisierung	11
I. Begriff und Rechtsnatur	11
II. Funktionsweise	12
III. Zugang und Widerruf	13
1. Zugang der Autorisierung	13
a) Begriff des Zugangs	14
aa) Zugangsprinzip.....	14
bb) Fiktion des Zugangs	17
b) Abgrenzung zum Zahlungseingang	17
2. Widerruf der Autorisierung.....	18
a) Grundsatz: Unwiderruflichkeit	19
b) Modifikationen bzw. Ausnahmen.....	21
c) Ausübung und Rechtsfolge des Widerrufs	25
d) Relevanz für die unautorisierte Zahlung.....	26
IV. Autorisierung bei einzelnen Zahlungsmethoden.....	28
1. Überweisung	28
2. SEPA-Lastschriftverfahren	29
3. Kartenzahlung	30
a) Debitkarte.....	32
aa) Zahlung durch das EFTPOS-System	32
bb) Geldabhebung am Bancomat	35
b) Kreditkarte	36
c) Geldkarte.....	37
4. E-Banking	40
a) Begriff und Umfang	40
b) Autorisierungsvorgang	40
c) Abgrenzungen	41
aa) Elektronische Fernzahlungsvorgänge	41

bb) Elektronische Zahlungsvorgänge.....	42
C. Zahlungsauftrag	45
I. Begriff und Rechtsnatur	45
II. Inhalt und Form.....	47
III. Wirkung	48
IV. Verhältnis zwischen Autorisierung und Zahlungsauftrag	49
1. Abstufung in der PSD2	49
2. Abgrenzung auf theoretischer Ebene	50
3. Kritik und Stellungnahme	51
D. Weitere Begriffe	55
I. Authentifizierung und starke Kundenauthentifizierung.....	55
1. Authentifizierung	55
2. Starke Kundenauthentifizierung (SCA).....	56
a) Begriff der SCA	57
b) Voraussetzungen der SCA	57
aa) Zwei Elemente aus drei Kategorien.....	57
bb) Unabhängigkeit der Elemente.....	61
cc) Schutz der Vertraulichkeit der Elemente	63
c) Anwendungsbereich der SCA.....	63
aa) Online-Zugriff auf das Konto	64
bb) Auslösung elektronischer Zahlungsvorgänge	64
cc) Handlungen im Fernzugang mit Betrugs- oder Missbrauchsrisiko	65
d) Ausnahmefälle	66
aa) Online-Zugriff für beschränkten Zweck	66
bb) Kontaktlose Zahlungen an der Verkaufsstelle	66
cc) Kleinbetragszahlungen.....	66
3. Relevanz für die unautorisierte Zahlung	67
II. Personalisiertes Sicherheitsmerkmal	67
1. Begriff und Voraussetzungen.....	67
2. Umfang.....	69
a) Passwort und PIN.....	70
b) TAN	71
aa) TAN-Listen und iTAN.....	71
bb) mTAN und appTAN	72
cc) eTAN, chipTAN, photoTAN und QR-TAN	73
dd) Fazit.....	75
c) Biometrisches Merkmal?	76
d) Unterschrift?	78
e) Elektronische Signatur?	80
f) Fazit	82
3. Relevanz für die unautorisierte Zahlung	83

III.	Zahlungsinstrument	84
1.	Begriff und Form	84
2.	Voraussetzung	85
a)	Standpunkt des EuGH	86
b)	Stellungnahme	87
c)	Beispiele	89
3.	Relevanz für die unautorisierte Zahlung	90
IV.	Verhältnisbestimmung	91
1.	Zahlungsinstrument und personalisierte Sicherheitsmerkmale	91
2.	Zahlungsinstrument und Authentifizierungsverfahren	92
3.	Authentifizierung und personalisierte Sicherheitsmerkmale	93
a)	Authentifizierung mit Einsatz der personalisierten Sicherheitsmerkmale	93
b)	Authentifizierung ohne Einsatz der personalisierten Sicherheitsmerkmale	94
4.	Authentifizierung und Autorisierung	95
5.	Fazit	97
2.	Teil: Angriffsmethoden	101
A.	Überblick	103
B.	Unterschriftenfälschung	105
C.	Physische Entwendung des Zahlungsinstruments	107
D.	Skimming (Kartendoublette)	109
E.	Social Engineering	111
I.	Überblick	111
II.	Phishing	112
1.	Allgemeines	112
2.	Phishing (URL-Spoofing)	113
3.	Vishing	115
III.	Freischaltungs-Trojaner	116
1.	Begriff und Ablauf	116
2.	Unzulässigkeit der Irrtumsanfechtung im Rahmen der PSD2	117
a)	Erklärungsirrtum	117
b)	Meinungsstreit in Deutschland	121
c)	Stellungnahme	124
d)	Fazit	129
IV.	Rücküberweisungs-Trojaner	131
1.	Begriff und Ablauf	131
2.	Unautorisierte Zahlung?	132
a)	Motivirrtum	132
b)	Anfechtung wegen absichtlicher Täuschung?	133
c)	Anfechtung aufgrund eines Grundlagenirrtums?	133

d) Fazit	134
V. CEO-Fraud	135
1. Begriff und Merkmale.....	135
2. Ablauf eines CEO-Frauds	136
3. Unautorisierte Zahlung?.....	137
VI. Fazit	138
F. Hacking.....	139
I. Überblick.....	139
1. Begriff.....	139
2. Abgrenzung zum Social Engineering	140
II. Pharming (DNS-Spoofing)	141
III. Malware-Angriffe (vor allem Trojaner-Angriffe)	142
1. Malware und ihre Unterarten	143
a) Malware	143
aa) Begriff.....	143
bb) Infektionswege.....	144
cc) Negative Auswirkungen.....	144
b) Virus und Wurm	145
c) Trojaner.....	146
d) Keylogger	148
e) Spyware.....	149
f) Bot und Botnet.....	149
2. Schema von Trojaner-Angriffen	150
3. Anwendungsbeispiele von Trojaner-Angriffen	151
a) Angriff durch den Zeus-Trojaner und seine neuen Versionen	151
b) Trojaner-Angriff mit einer zweiten SIM-Karte	153
c) Angriff durch die Mischform aus Wurm und Trojaner.....	153
IV. Man-in-the-Middle-Angriff (MITM)	154
1. Begriff und Merkmale.....	155
2. Ablauf von MITMs	157
3. Unautorisierte Zahlung?.....	158
a) Fragestellung.....	158
b) Übermittlungssirrturn?	158
c) Unautorisierte Zahlung?.....	161
d) Fazit	163
V. Weitere Angriffsformen des Hackers.....	164
1. Brute-Force-Angriff.....	164
2. Cross-Site-Scripting (XSS).....	165
3. Dumpster Diving.....	166
4. Sniffing-Angriff	166
G. Fazit: Vorliegen einer unautorisierten Zahlung?	169

3. Teil: Beweisrecht in Bezug auf die Autorisierung.....	173
A. Einleitung.....	175
B. Beweislast für die Autorisierung	177
I. Beweislastverteilung	177
II. Mindestanforderungen an den Nachweis.....	178
1. Mindestvoraussetzungen der Beweisführung	178
a) Nachweis der Authentifizierung	178
b) Nachweis der störungsfreien Aufzeichnung und Verbuchung des Zahlungsvorgangs	180
2. Bedeutung von Mindestanforderungen.....	182
a) Rechtsfolgen bei Nichterbringung der Mindest- voraussetzungen.....	182
b) Rechtsfolgen bei Erfüllung der Mindest- voraussetzungen.....	186
C. Zulässigkeit des Anscheinsbeweises für die Autorisierung?.....	189
I. Grundsatz des Anscheinsbeweises	189
1. Begriff und Rechtsnatur	189
2. Anwendungsbereich und Voraussetzungen	190
3. Erschütterung des Anscheinsbeweises.....	191
4. Relevanz für die Frage der unautorisierten Zahlungen.....	193
a) Beweisnot der Bank	193
b) Alternativität des Anscheinsbeweises im Zahlungs- verkehr	193
II. Rechtslage unter der PSD2	197
1. Grammatische Auslegung.....	197
2. Systematische Auslegung	198
3. Historische Auslegung	199
4. Teleologische Auslegung	200
5. Fazit.....	201
III. Rechtslage in den EU-Mitgliedstaaten	201
1. Deutschland.....	202
a) Zulässigkeit bis zur Umsetzung der PSD1.....	202
b) Meinungsstreit im Rahmen der PSD1 bzw. PSD2	203
c) Grundsatzurteil des BGH	206
aa) Gründe für die Zulässigkeit des Anscheinsbeweises	207
bb) Voraussetzungen des Anscheinsbeweises.....	208
cc) Erschütterung des Anscheinsbeweises.....	209
2. Österreich	209
3. Frankreich und Belgien.....	211
4. Fazit.....	212

IV. Stellungnahme	213
1. Zulässigkeit des Anscheinsbeweises mit den strengen Voraussetzungen	213
a) Praktische Unüberwindbarkeit.....	213
b) Ordnungsgemässes und fehlerfreies Funktionieren.....	214
2. Gründe für die Anwendung des Anscheinsbeweises	214
a) Gestützt von Lebenserfahrungen	215
b) Unentbehrlichkeit für Beweisführung der Bank	215
c) Spielraum innerhalb der PSD2.....	216
d) Keine Überwälzung des Missbrauchsrisikos	216
e) Angemessene Rechtsfolge bei der Anwendung des Anscheinsbeweises.....	216
3. Anwendung des Anscheinsbeweises in konkreten Authentifizierungsverfahren	219
a) Einzelfaktor-Authentifizierungsverfahren	219
b) Zwei-Faktor-Authentifizierungsverfahren.....	220
aa) Kartenzahlungsverkehr	220
bb) Zahlung via E-Banking	221
c) Fazit.....	224
4. Erschütterung des Anscheinsbeweises.....	226
a) Grundlagen.....	226
b) Unmöglichkeit der Erteilung der Autorisierung durch den Kunden	226
aa) Kartenzahlungsverkehr	227
bb) Zahlung via E-Banking	227
c) Alternativer Ablauf aufgrund eines unbefugten Zugriffs ..	228
aa) Kartenzahlungsverkehr	228
bb) Zahlung via E-Banking	229
D. Fazit	231
4. Teil: Rechtsansprüche der Beteiligten	233
A. Überblick: Risikoverteilung und Prüfrehrenfolge	235
B. Schicksal des Aufwendungsersatzanspruchs der Bank	237
I. Ausschluss des Aufwendungsersatzanspruchs.....	237
1. Überblick.....	237
2. Vertragliche Ebene: Ohne Autorisierung kein Aufwendungsersatzanspruch.....	238
3. Beweisebene: Nachweisschwierigkeit für die Autorisierung ..	240
4. Ablehnung der Rechtsscheinhaftung im Rahmen der PSD2 ..	241
a) Kein Spielraum für die Rechtsscheinhaftung in der PSD2	242
aa) Unvereinbarkeit mit dem abschliessenden Charakter des Art. 64, Art. 69 und Art. 73 Abs. 1 PSD2.....	243

bb)	Wertungswiderspruch zu Art. 72 PSD2	244
cc)	Widerspruch zum Haftungsmassstab des Art. 74 Abs. 1 UAbs. 3 PSD2.....	245
b)	Überflüssigkeit der Rechtsscheinhaftung im Rahmen der PSD2	246
aa)	Überlappung mit dem Anscheinsbeweis für die Autorisierung	246
bb)	Überlappung mit der Verschuldenshaftung des Kunden.....	247
c)	Geringe praktische Bedeutung der Rechtsscheinhaftung im Drittmissbrauchsfall.....	248
aa)	Drittmissbrauch als das «Handeln unter fremdem Namen»	248
bb)	Duldungsvollmacht	249
cc)	Anscheinsvollmacht.....	250
II.	Umfang des Ausschlusses.....	252
III.	Rechtsnatur der Ausübung des Ausschlusses.....	253
IV.	Fazit	253
C.	Erstattungsanspruch des Kunden.....	255
I.	Spezialität des Anspruchs	255
1.	Rechtsnatur und Charakter des Anspruchs	255
2.	Verhältnis zum Anspruch auf die Folgeschäden.....	257
II.	Inhalt des Anspruchs.....	257
1.	Fälligkeit des Anspruchs	258
a)	Erstattungshöchstfrist.....	258
aa)	Grundsatz	258
bb)	Ausnahme	259
cc)	Fazit	260
b)	Gewähr für die Höchstfrist	261
aa)	Unautorisierte Zahlungsvorgang aus Kundensicht...	262
bb)	Verrechnungsverbot und Ausschluss der Dolo-petit-Einrede.....	263
	(1) Dolo-petit-Einrede und Verrechnung	263
	(2) Verrechnungsverbot.....	264
	(3) Ausschluss der Dolo-petit-Einrede	268
cc)	Sekundäranspruch aus dem Leistungsverzug	269
2.	Umfang des Anspruchs	271
3.	Weise der Erfüllung	272
a)	Barauszahlung.....	273
b)	Gutschrift	273
aa)	Bedeutung	273
bb)	Rechtsnatur	274
4.	Fazit.....	276

III.	Schranke der Ausübung des Anspruchs	277
1.	Anzeigeobliegenheit.....	277
2.	Ordnungsmässigkeit der Anzeige	279
a)	Inhalt der Anzeige.....	279
b)	Form der Anzeige	280
c)	Rechtzeitigkeit der Anzeige	280
aa)	Positive Kenntnis von der Nichtautorisierung	281
bb)	Unkenntnis der Nichtautorisierung	283
3.	Rechtsfolgen.....	286
a)	Bei ordnungsgemässer Anzeige	286
b)	Bei Verletzung der Anzeigeobliegenheit.....	287
aa)	Wortlaut des Art. 71 Abs. 1 UAbs. 1 PSD2.....	287
bb)	Verwirkungsfrist und ihre Rechtsfolge	287
cc)	Erfolgloser Fristablauf als Genehmigung	264
4.	Fazit.....	289
IV.	Ausschluss des Anspruchs.....	290
1.	Ungewöhnliche und unvorhersehbare Ereignisse	291
a)	Begriff und Voraussetzungen	291
b)	Anwendungsbeispiele des Art. 93 PSD2	292
c)	Wird «eine gute Fälschung der Unterschrift» darunter eingestuft?.....	293
2.	Gesetzliche Verpflichtung.....	295
3.	Kleinbetragszahlungsinstrumente und E-Geld.....	295
a)	Kleinbetragszahlungsinstrumente	296
aa)	Begriff und Voraussetzung	296
bb)	Umfang	298
cc)	Haftungserleichterung für die Bank.....	299
b)	E-Geld.....	303
aa)	Begriff und Arten.....	303
bb)	Beziehung zwischen E-Geld und Kleinbetrags- zahlungsinstrument	304
cc)	Haftungserleichterung für die Bank.....	305
4.	Beweislast	306
V.	Fazit.....	306
5. Teil: Schadenersatzanspruch der Bank im Besonderen.....	309	
A.	Überblick	311
I.	Systematik der Schadenersatzhaftung des Kunden.....	311
II.	Anwendungsbereich der Kundenhaftung.....	312
III.	Abschliessender Charakter des Art. 74 PSD2	314
B.	Beschränkte Anreizhaftung des Kunden	315
I.	Allgemeines.....	315
1.	Ziel der Anreizhaftung	315

2. Rechtsnatur: Verschuldensabhängige Haftung	315
3. Bedeutung des Art. 74 Abs. 1 UAbs. 2 PSD2.....	320
II. Voraussetzungen	320
1. Positive Tatbestandsmerkmale.....	321
a) Schaden aus dem nicht autorisierten Zahlungsvorgang.....	321
b) Missbräuchliche Verwendung des Zahlungsinstruments ...	321
aa) Verlust und Diebstahl des Zahlungsinstruments.....	322
bb) Sonstige missbräuchliche Verwendung des	
Zahlungsinstruments	323
c) Pflichtverletzung	324
d) Kausalität	325
2. Negative Tatbestandsmerkmale	325
a) Fehlende Bemerkbarkeit	326
aa) Begriff.....	326
bb) Fehlende Bemerkbarkeit bei den Kartenzahlungen ..	327
cc) Fehlende Bemerkbarkeit bei den E-Banking-	
Zahlungen.....	328
dd) Rückausnahme	330
b) Verursachung in der Risikosphäre der Bank	330
c) Weitere Beispiele	332
III. Rechtsfolge	333
IV. Fazit	333
C. Unbeschränkte Verschuldenshaftung des Kunden	337
I. Überblick der Verschuldenshaftung.....	337
II. Handeln in betrügerischer Absicht.....	337
1. Begriff	337
2. Voraussetzung	338
3. Unautorisierte Zahlung?.....	339
4. Rechtsfolge.....	340
III. Vorsätzliche oder grob fahrlässige Pflichtverletzung.....	341
1. Schaden aus dem nicht autorisierten Zahlungsvorgang	341
2. Pflichtverletzung	342
a) Verletzung der Sorgfaltspflichten	342
aa) Verletzung der gesetzlichen Sorgfaltspflichten	343
(1) Zweck und zeitlicher Anwendungsbereich des	
Art. 69 Abs. 2 PSD2	343
(2) Schutzgegenstand des Art. 69 Abs. 2 PSD2	345
(3) Zumutbarkeit der Schutzvorkehrungen	347
bb) Verletzung der vertraglichen Sorgfaltspflichten.....	349
(1) Vertragliche Sorgfaltspflicht.....	349
(2) Inhaltskontrolle nach Art. 69 Abs. 1 lit. a	
PSD2	350
(3) Auslegung von AGB.....	352

(4) Rechtsfolge von Verstößen.....	352
cc) Systematisierung der Sorgfaltspflichten	353
(1) Aufbewahrungspflicht für das Zahlungsinstrument und die personalisierten Sicherheitsmerkmale...354	
i) Pflicht zur Getrenntaufbewahrung	354
ii) Aufbewahrungspflicht	357
iii) Geheimhaltungspflicht	360
(2) Pflicht zur Sicherung der IT-Infrastruktur	362
i) Pflicht zur Installation von Schutz- programmen.....	363
ii) Pflicht zur regelmässigen Aktualisierung....364	
iii) Pflicht zur System- und Netzwerk- sicherheit	365
(3) Pflicht zur angemessenen Reaktion auf Verdachtsmomente	366
i) Inhalt und Voraussetzung der Pflicht	366
ii) Fallkonstellationen	367
b) Verletzung der Anzeigepflicht.....	370
aa) Zur Anzeigepflicht im Allgemeinen	370
bb) Anzeigegründe bzw. Tatbestandsvarianten	371
(1) Verlust des Zahlungsinstruments.....372	
(2) Missbräuchliche Verwendung des Zahlungsinstruments	373
cc) Adressat, Form und Zeitpunkt der Anzeige	374
dd) Rechtsfolgen ordnungsgemässer Anzeigen sowie von Verletzungen der Anzeigepflicht	376
ee) Abgrenzung zur Anzeige nach Art. 71 Abs. 1 PSD2.377	
3. Verschulden	378
a) Vorsatz	379
b) Grobfahrlässigkeit.....	380
aa) Begriff und Anforderung	380
bb) Beurteilung von grober Fahrlässigkeit im Einzelfall.382	
(1) In Bezug auf die Aufbewahrungspflicht.....382	
(2) In Bezug auf die Pflicht zur angemessenen Reaktion auf Verdachtsmomente	384
(3) In Bezug auf die Anzeigepflicht	385
4. Kausalität	385
a) Allgemeines über die Kausalität	385
b) Kausalität im konkreten Drittmissbrauchsfall	387
aa) Physische Entwendung des Zahlungsinstruments	387
bb) Skimming und Pharming	388
cc) Phishing	388
dd) Malware-Angriffe	389

ee) MITM.....	389
IV. Rechtsfolge.....	390
V. Fazit	391
D. Verminderung und Ausschluss der Kundenhaftung.....	393
I. Anspruchskürzung aufgrund des Mitverschuldens der Bank.....	393
1. Voraussetzungen und Rechtsfolge	393
2. Typische Anwendungsbeispiele.....	394
a) Unterlassung der Stornobuchung.....	394
b) Unterlassung der Warnhinweise bei Auftauchen massiver Verdachtsmomente	396
c) Keine ausreichende Sicherheit für die Authentifizierung.....	396
d) Verfügungen über die vereinbarte Ausgabenobergrenze.....	398
e) Schuldhaftes Verhalten von Hilfspersonen.....	398
II. Ausschluss des Schadenersatzanspruchs der Bank.....	398
1. Ausschluss bei Nichtverlangen der SCA	399
a) Inhalt und Ziel des Art. 74 Abs. 2 PSD2	399
b) Anwendungsbereich des Art. 74 Abs. 2 PSD2	400
2. Ausschluss nach Missbrauchsanzeige.....	402
3. Weitere Ausschlussgründe	402
6. Teil: Weitere Fragen der Bank-Kunden-Beziehung.....	405
A. Beweisrecht in Bezug auf die Kundenhaftung	407
I. Allgemeine Beweislastverteilung.....	407
1. Beweislast für die Kundenhaftung sowie Haftungs- ausschlüsse	407
2. Zulässigkeit des Anscheinsbeweises für die grob fahrlässige Pflichtverletzung.....	409
II. Besonderheit beim Beweis für die Pflichtverletzung und das Verschulden	410
1. Abgrenzungsschwierigkeiten bei der Sorgfaltspflicht- verletzung	411
2. Beweisrecht bezüglich der grob fahrlässigen Pflicht- verletzung in Deutschland.....	412
a) Bei Kartenzahlungen.....	413
aa) Anscheinsbeweis für die grob fahrlässige Verletzung der Getrenntaufbewahrungspflicht	414
(1) Voraussetzungen des Anscheinsbeweises	415
(2) Erschütterung des Anscheinsbeweises.....	417
bb) Kein Anscheinsbeweis für die grob fahrlässige Verletzung der Aufbewahrungspflicht	419
b) Bei E-Banking-Zahlungen	419
aa) Kein Anscheinsbeweis für die grob fahrlässige Pflichtverletzung	420

Inhaltsverzeichnis

bb) Sekundäre Darlegungslast zulasten des Kunden.....	421
B. Abdingbarkeit der Vorschriften durch die Vertragsparteien	423
C. Schadenersatzanspruch des Kunden.....	425
7. Teil: Prüfung der Anspruchsgrundlagen im Missbrauchsfall.....	427
8. Teil: Gesamtfazit.....	441
Stichwortregister	449