Bundeskartellamt

4. Beschlussabteilung

B 4 – 71/10

VERWALTUNGSVERFAHREN
BESCHLUSS
GEM. § 32 GWB

–für die Veröffentlichung bestimmte Fassung –

Beschluss

In dem Verwaltungsverfahren

1. Die Deutsche Kreditwirtschaft
   Bundesverband deutscher Banken e.V.
   Burgstraße 28
   10178 Berlin

   – Beteiligte zu 1. –

2. Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.
   Schellingstraße 4
   10785 Berlin

   – Beteiligter zu 2. –

3. Deutscher Sparkassen- und Giroverband e.V.
   Charlottenstraße 47
   10117 Berlin

   – Beteiligter zu 3. –

Verfahrensbevollmächtigte der Beteiligten zu 1.-3.:
Oppenländer Rechtsanwälte
Börsenplatz 1
70174 Stuttgart
Telefax: 0711 / 601 87 – 222

4. Bundesverband deutscher Banken e.V.
   Burgstraße 28
   10178 Berlin

– Beteiligter zu 4.. –

Verfahrensbevollmächtigte des Beteiligten zu 4.:
Dentons Europe LLP
Markgrafenstrasse 33
10117 Berlin
Telefax: 030 / 264 73-133

5. Sofort GmbH
   Fußbergstraße 1
   82131 Gauting

– Beigeladene zu 5. –

Verfahrensbevollmächtigte der Beigeladenen zu 5.:
Kapellmann und Partner Rechtsanwälte
Viersener Straße 16
41061 Mönchengladbach
Telefax: 02161 / 811-777

6. giropay GmbH
   An der Welle 4
   60322 Frankfurt a.M.

– Beigeladene zu 6. –

Verfahrensbevollmächtigte der Beigeladenen zu 6.:
Osborne Clarke
Innere Kanalstraße 15

50823 Köln
Telefax: 0221 / 5108 - 4111

zur Prüfung eines Verstoßes gegen Art. 101 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union[1] (AEUV) und § 1 des Gesetzes gegen Wettbewerbsbeschränkungen[2] (GWB) sowie gegen § 19 Abs. 3 Satz 1 i.V.m. § 19 Abs. 1, Abs. 2 Nr. 1 GWB hat die 4. Beschlussabteilung des Bundeskartellamtes am 29.06.2016 beschlossen:

1. Es wird festgestellt, dass der dem Amt mit Schreiben vom 05.08.2009 mitgeteilte Beschluss der Beteiligten zu 1. über die Annahme der Sonderbedinungen für das Online-Banking in Bezug auf Ziff. 7.2 Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich, Ziff. 10.2.1 Abs. 5, vierter Spiegelstrich rechtswidrig ist.

2. Es wird festgestellt, dass die Beschlussfassung der Beteiligten zu 2. mit dem Inhalt, die auf Ebene der Beteiligten zu 1. erstellten Sonderbedingungen für das Online-Banking anzunehmen, sowie deren Bekanntmachung und Empfehlung durch Schreiben vom 07.07.2009 an die Regionalverbände und durch Verbandsrundschreiben vom 05.08.2009 in Bezug auf Ziff. 7.2. Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich, Ziff. 10.2.1. Abs. 5, vierter Spiegelstrich der von der Beteiligten zu 1. beschlossenen Sonderbedinungen für das Online-Banking rechtswidrig sind.

3. Es wird festgestellt, dass die Beschlussfassung der Beteiligten zu 3. mit dem Inhalt, die auf Ebene der Beteiligten zu 1. erstellten Sonderbedingungen für das Online-Banking anzunehmen, sowie deren Bekanntmachung und Empfehlung durch Rundschreiben an die Institute der Sparkassengruppe vom 13.08.2009 in Bezug auf Ziff. 7.2. Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich, Ziff. 10.2.1. Abs. 5, vierter Spiegelstrich der von der Beteiligten zu 1. beschlossenen Sonderbedinungen für das Online-Banking rechtswidrig sind.

4. Es wird festgestellt, dass die Beschlussfassung der Beteiligten zu 4. mit dem Inhalt, die auf Ebene der Beteiligten zu 1. erstellten Sonderbedingungen für das Online-

---

[1] Vertrag über die Arbeitsweise der Europäischen Union in der Fassung der Bekanntmachung vom 09.05.2008 (Amtsblatt der EU 2008/C 115/01).

[2] Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26.06.2013 (BGBl. I S. 1750) zuletzt geändert durch Art. 258 V v.31.08.2015 (BGBl. I 1474).

Banking anzunehmen, sowie deren Bekanntmachung und Empfehlung durch Rundschreiben an die Mitglieder vom 22.07.2009 in Bezug auf Ziff. 7.2. Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich, Ziff. 10.2.1. Abs. 5, vierter Spiegelstrich der von der Beteiligten zu 1. beschlossenen Sonderbedinungen für das Online-Banking rechtswidrig sind.

5. Die Vollziehung dieser Verfügung wird ausgesetzt.

Gründe

A. Einleitende Zusammenfassung

1. Die Sonderbedingungen für das Online-Banking (im Folgenden „OBB“ oder „Online-Banking-Bedingungen“) sind Teil der Allgemeinen Geschäftsbedingungen von Banken. Sie wurden von der Deutschen Kreditwirtschaft (im Folgenden: DK)[3] und den in ihr vertretenen Spitzenverbänden der deutschen Kreditwirtschaft gemeinsam erarbeitet und werden von den jeweiligen Mitgliedsinstituten im Verhältnis zu ihren Kunden flächendeckend angewendet. Sie regeln u.a. Sorgfaltspflichten der Online-Banking-Kunden im Umgang mit den Personalisierten Sicherheitsmerkmalen PIN (Persönliche Identifikationsnummer) und TAN (Transaktionsnummer). So dürfen nach den Bestimmungen der Online-Banking-Bedingungen PIN und TAN nicht außerhalb gesondert vereinbarter Internetseiten, z.B. nicht auf Online-Händlerseiten, eingegeben werden.

2. Ziffer 7.2. Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich der OBB[4] lauten:

„Der Teilnehmer hat seine Personalisierten Sicherheitsmerkmale (vgl. Nummer 2.1) geheim zu halten und nur im Rahmen einer Auftragserteilung über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie sein Authentifizierungsinstrument (vgl. Nummer 2.2) vor dem Zugriff anderer Personen sicher

---

[3] Bis zum August 2011 bezeichnete sich die DK als Zentraler Kreditausschuss („ZKA“). Im Folgenden wird auch im Zusammenhang mit Sachverhalten, die vor August 2011 liegen, einheitlich die Bezeichnung DK verwendet, soweit es sich nicht um Zitate oder Bezeichnungen von Gremien wie z.B. Arbeitsgruppen handelt.

[4] Die Gliederungsebenen in den OBB der Sparkassen und privaten Banken weichen zum Teil von dem Beschluss der DK ab, der Text der Sorgfaltspflichten ist bei den verschiedenen Bankengruppen identisch.

zu verwahren. Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen. Insbesondere ist zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten: […] Das Personalisierte Sicehrheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z.B. nicht auf Online-Händlerseiten).“

Die mit der Sorgfaltspflicht korrespondierende Haftungsregelung unter Ziffer 10 .2.1 Abs. 5, vierter Spiegelstrich lautet:

„*Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er […] das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (vgl. Nummer 7.2 Absatz 2, 3. Spiegelstrich, […].*“

3. Die zur Vereinbarung und Umsetzung dieser Regelung getroffenen Beschlüsse der DK und der in ihr vertretenen Spitzenverbände der deutschen Kreditwirtschaft verstoßen gegen Artikel 101 AEUV und § 1 GWB, da sie eine Wettbewerbsbeschränkung bezwecken, zumindest aber bewirken. Die beanstandeten Klauseln zielen bereits ihrem Wortlaut nach ausschließlich auf ein Verbot der Tätigkeit von Zahlungsauslösediensten wie z. B. der Sofort GmbH, die mit Hilfe dieser Personalisierten Sicherheitsmerkmale Bezahlverfahren den im Internet tätigen Online-Händlern und Kunden anbietet. Die beanstandeten Online-Banking-Bestimmungen sind zudem objektiv geeignet, die Nutzung von Zahlungsauslösediensten durch Online-Händler und Bankkunden zu erschweren oder sogar ganz auszuschließen.

4. Die beanstandeten Online-Banking-Bedingungen adressieren nur scheinbar Sicherheitsprobleme. Wie die Entstehungsgeschichte dieser Online-Banking-Bedingungen zeigt, ist die Behinderung von Zahlungsauslösediensten der tatsächliche mit der Einführung der beanstandeten Online-Banking-Bestimmungen verfolgte Zweck. Die Regelungen lassen sich nicht als notwendiger Teil eines konsistenten Sicherheitskonzepts der Banken einstufen; sie sind vielmehr dazu bestimmt und geeignet, die eigenen Ertragsinteressen der in den Mitgliedsverbänden der DK zusammengeschlossenen Kreditinstitute zu wahren.

5. Durch die beanstandeten Bestimmungen werden innovative Zahlungsdiensteanbieter behindert, die ein Dienstleistungsangebot entwickelt haben, das von Online-Händlern nachgefragt wird, weil es sowohl deren Bedürfnis nach einer preiswerten und schnellen Zahlungsoption, als auch ein identisches Interesse der Online-Kunden deckt. Solche innovativen Verfahren erlangen mit ihrer stetig steigenden Marktdurchdringung und Nutzung durch Kunden eine wachsende Bedeutung auf dem Markt für Internetbezahlverfahren und fördern den Wettbewerb auf diesem Markt, worauf etablierte Anbieter von Bezahlverfahren reagieren müssen.

6. Die beschlossenen Sonderbedingungen für das Online-Banking ermöglichen es Kreditinstituten, durch Errichtung einer rechtlichen Marktzutrittsschranke Wettbewerber vom Markt auszuschließen bzw. deren Marktauftritt erheblich zu erschweren, weil Kunden, die sich für die Nutzung eines Zahlungsauslösedienstes entscheiden, gegen die geltenden Allgemeinen Geschäftsbedingungen ihrer kontoführenden Bank verstoßen und haftungsrechtliche Konsequenzen in Kauf nehmen müssen. Im Zusammenhang mit der von der DK betriebenen Medienpolitik, die auf eine „Ächtung“ von bankenunabhängigen Zahlungsdiensteanbeitern zielt, haben die Online-Banking-Bedingungen und die Haftungsfolgen die Marktentwicklung von Zahlungsdiensteanbietern erheblich erschwert.

7. Dass es in Folge der beanstandeten Klauseln bisher nicht zu einer vollständigen Eliminierung des Wettbewerbs durch Zahlungsauslösedienste gekommen ist, resultiert im Wesentlichen daraus, dass einige wenige Anbieter, wie die Sofort GmbH, trotz aller durch die Kreditwirtschaft im Zusammenhang mit den Sorgfaltspflichten initiierten oder unterstützten Maßnahmen nicht von der Vermarktung ihres Angebots Abstand genommen haben. Die DK hat Unternehmen, die Dienstleistungen im Zusammenhang mit dem Online-Banking-Zugang angeboten haben, unter Hinweis auf die von ihr beschlossenen AGB-Regelungen zur Einstellung ihrer Tätigkeit aufgefordert. Zum überwiegenden Teil war sie mit dieser Strategie erfolgreich. Darüber hinaus hat die DK mit dem sog. „Intermediärskonzept“ einen Handlungsrahmen erarbeitet, der vorgibt, wie sich die Kreditwirtschaft gegen die Tätigkeit von Zahlungsauslösediensten positionieren kann: Angedachte Maßnahmen, wie an die Kunden gerichtete Warnungen vor der Nutzung solcher Dienstleister, wurden auf Internetseiten der Kreditinstitute veröffentlicht und gegenüber Händlern thematisiert. Auch gegenüber der Presse wurde auf vermeintliche Risiken und Probleme bei der Nutzung des Angebots von Zahlungsauslösediensten hingewiesen. Schließlich muss sich die Sofort GmbH auch in mehreren derzeit noch anhängigen zivilrechtlichen Verfahren wegen ihres Geschäftsmodells mit den Regelungen der OBB auseinandersetzen. In diesen Zivilverfahren ist zum Teil nur deshalb bisher noch kein Urteil ergangen, weil die kartellrechtliche Zulässigkeit der beanstandeten

Bestimmungen im vorliegenden kartellrechltichen Verfahren parallel geprüft wurde und die Gerichte die bei ihnen anhängigen Verfahren bis zu einer Entscheidung des Bundeskartellamtes ausgesetzt haben. Die Bestimmungen stellen keine vom Kartellverbot nicht erfasste reine Nebenbestimmung dar; sie sind auch nicht gemäß Artikel 101 Abs. 3 AEUV und § 2 GWB freistellungsfähig. Selbst wenn die Regelung zu Effizienzen führen sollte – was nicht vorgetragen und erst recht nicht nachgewiesen worden ist – sind sie jedenfalls nicht unerlässlich zur Verwirklichung des Ziels.

8. Die Vereinbarung einheitlicher Sorgfaltspflichten und deren Empfehlung an die angeschlossenen Kreditinstitute stellen kartellrechtswidrige Beschlüsse von Unternehmensvereinbarungen dar. Diese dienen im Zusammenwirken mit weiteren Maßnahmen der DK und der Spitzenverbände der Kreditwirtschaft der Behinderung des Wettbewerbs durch neu im Markt auftretende Zahlungsauslösedienste. Insgesamt ist das Handeln der DK und der Spitzenverbände der Kreditwirtschaft angesichts seiner erklärten Zielsetzung, seiner Historie und der vielfältigen Vorgehensweisen gegen Zahlungsauslösedienste als ein kollektives Vorgehen der Kreditwirtschaft im Rahmen eines Gesamtplans zur Ausschaltung des Wettbewerbs durch Zahlungsauslösedienste zu sehen. Die zugrundeliegenden Beschlüsse und deren Empfehlung verstoßen sowohl auf der Ebene der DK als auch auf der Ebene der Spitzenverbände unter dem Aspekt der Koordinierung gegen Art. 101 AEUV sowie gegen § 1 GWB. Die Umsetzung dieses Gesamtplans, zu dem auch die Abstimmung der Beteiligten zu 1. bis 4. über die Online-Banking-Bedingungen in Bezug auf die Sorgfaltspflichten im Umgang mit den Personalisierten Sicherheitsmerkmalen zählt, stellt zudem – selbst im Falle einer unterstellten Zulässigkeit der Koordinierung – eine unbillige Behinderung von anderen Unternehmen und damit ein missbräuchliches Verhalten im Sinne von § 19 Abs 3 Satz 1 i.V.m. Abs. 1, Abs. 2 Nr. 1 GWB dar.

9. Der Verstoß gegen Art. 101 Abs. 1 AEUV und § 1 GWB, § 19 Abs. 3 Satz 1 i.V.m. Abs. 1, Abs. 2 Nr. 1 GWB dauert an. Die Empfehlungen wirken fort, sie sind Grundlage für die Allgemeinen Geschäftsbedingungen der einzelnen Kreditinstitute, die sie praktisch flächendeckend umsetzen.

10. Der europäische Gesetzgeber verlangt in der überarbeiteten Zahlungsdiensterichtlinie 2 (im Folgenden PSD2)[5], dass in der Zeit bis zu deren Umsetzung in nationales Recht die

---

[5] 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 2013/26/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, Abl. der Europäischen Union vom23.12.2015. In der Praxis ist auch im deutschen

Kontinuität des Wettbewerbs sicherzustellen ist und bestehende Dienstleister unabhängig von deren Geschäftsmodell ihre Dienstleistungen anbieten dürfen. Dabei soll eine ungerechtfertigte Diskriminierung vorhandener Marktteilnehmer vermieden werden. Diese Verpflichtung richtet sich an alle staatlichen Stellen und damit auch an das Bundeskartellamt. Aus diesem Grund ist der Erlass dieses Beschlusses geboten.

B. Sachverhalt

I. Die Beteiligten

1. Die Deutsche Kreditwirtschaft

11. Beteiligte des Kartellverwaltungsverfahrens sind die Deutsche Kreditwirtschaft sowie die in ihr zusammenwirkenden Spitzenverbände der deutschen Kreditwirtschaft. Hierzu zählen u.a. der Bundesverband deutscher Banken e.V. (im Folgenden: BdB), der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (im Folgenden: BVR) sowie der Deutsche Sparkassen- und Giroverband e.V. (im Folgenden: DSGV). Die Federführung in der DK wechselt jährlich zwischen BdB, BVR und DSGV. Aktuell ist der BdB Federführer der DK.

12. Die DK verfügt nicht über eine eigene Infrastruktur, sondern greift auf die Ressourcen ihrer Mitglieder und insbesondere des jeweiligen Federführers zurück. Die DK tritt zwar in der Öffentlichkeit und insbesondere gegenüber Organen der Gesetzgebung und Verwaltungsbehörden in den sie betreffenden Fragen einheitlich auf, hat aber im Gegensatz zu ihren Mitgliedern nicht den Status eines eingetragenen Vereins.

2. Bundesverband der Deutschen Volksbanken und Raiffeisenbanken

13. Der BVR ist der Spitzenverband der genossenschaftlichen Kreditwirtschaft in Deutschland. Mitglieder sind alle Genossenschaftsbanken. Der BVR vertritt bundesweit und international die Interessen der genossenschaftlichen Finanzgruppe. Hierbei koordiniert und entwickelt der BVR innerhalb der Gruppe eine gemeinsame strategische Ausrichtung. Gleichzeitig berät und unterstützt der Verband seine Mitglieder in rechtlichen, steuerlichen und betriebswirtschaftlichen Fragen.[6] Satzungsmäßiger Zweck des Verbandes sind die Förderung, Betreuung und Vertretung der fachlichen und der

---

Sprachraum die Verwendung der Abkürzung der englischen Bezeichnung Payment Service Directive 2 = PSD2 allgemein üblich.

6 Vgl. https://www.bvr.de/Wer_wir_sind/Unsere_Aufgaben, Stand 07.06.2016.

besonderen wirtschaftspolitischen und wirtschaftlichen Interessen der Mitglieder und der diesen angeschlossenen Einrichtungen innerhalb des Bereiches der genossenschaftlichen Kreditwirtschaft.[7]

3. Deutscher Sparkassen- und Giroverband

14. Der DSGV ist der Dachverband der Sparkassen-Finanzgruppe. Seine Mitglieder sind die Regionalverbände der Sparkassengruppe, 409 Sparkassen (Stand Januar 2016), sieben Landesbanken-Konzerne, die DekaBank, neun Landesbausparkassen, elf Erstversicherergruppen der Sparkassen und zahlreiche weitere Finanzdienstleistungsunternehmen.

15. Der DSGV vertritt die Interessen der Sparkassen-Finanzgruppe und organisiert die Willensbildung innerhalb der Gruppe. Darüber hinaus legt er die strategische Ausrichtung der Sparkassen-Finanzgruppe fest. Hierzu erarbeiten seine Mitglieder und Verbundunternehmen mit dem DSGV Konzepte für eine erfolgreiche Marktbearbeitung. Das betrifft die markt- und betriebstrategischen Themen, angefangen von der Produktentwicklung und -abwicklung, dem Risikomanagement und der Gesamtbanksteuerung, dem Karten- und Zahlungsverkehr bis hin zu ganzheitlichen Beratungsansätzen für alle Kundensegmente.[8]

4. Bundesverband deutscher Banken

16. Der BdB ist der Spitzenverband der privaten Banken. Ihm gehören rund 200 Banken und 11 Mitgliedsverbände an. Der BdB unterstützt seine Mitgliedsinstitute bei der Umsetzung gesetzlicher Vorgaben und bietet bei bankrechtlichen, bankpraktischen und bankpolitischen Fragen Hilfestellung. Der BdB liefert über sein Tochterunternehmen Bank-Verlag Fachpublikationen und Formulare für das Alltagsgeschäft. In enger Zusammenarbeit zwischen Verbandszentrale und Mitgliedern erfolgt zudem die Tätigkeit in diversen Gremien wie Ausschüssen, Arbeitskreisen, Arbeitsgruppen oder Kommunikationsforen.[9]

---

[7] Vgl. § 3 Abs. 1 Satzung Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V, https://www.bvr.de/p.nsf/0/E9CB768B7DE38656C1257CE1004F68F6/$file/BVR-Satzung2015.pdf, Stand 07.06.2016.

[8] Vgl. http://www.dsgv.de/de/ueber-uns/aufgaben_und_ziele.html, Stand 07.06.2016.

[9] Vgl. https://bankenverband.de/ueber-uns/unser-selbstverstaendnis/, Stand 07.06.2016.

II. Nicht (mehr) am Verfahren beteiligte Mitglieder der DK

1. Bundesverband Öffentlicher Banken Deutschlands e.V.

17. Der Bundesverband Öffentlicher Banken Deutschlands e.V. (im Folgenden: VÖB) ist ebenfalls ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt mehr als 60 Mitgliedsinstitute, darunter die Landesbanken sowie die bundes- und ländereigenen Förderbanken. Der VÖB ist Teil der DK und war an den Arbeitsgruppen der DK zur Erarbeitung der AGB Vertragswerke und insoweit zunächst auch an der rechtswidrigen Absprache beteiligt. Die vom VÖB im Bereich des Zahlungsverkehrs vertretenen Kreditinstitute bieten allerdings Online-Banking entweder nur in geringem Umfang an oder verwenden die Klauseln nicht mehr, die Gegenstand des Beschlusses der DK und der in ihr zusammenarbeitenden Verbände sind. Die Beschlussabteilung hat dem VÖB, der anfänglich als Beteiligter am Verfahren geführt wurde, daher mit Schreiben vom 27.06.2016 mitgeteilt, dass er nicht länger am Verfahren beteiligt ist und keine Rechte aus dem Beschluss gegen ihn hergeleitet werden.

2. Verband deutscher Pfandbriefbanken

18. Gänzlich nicht beteiligt an dem Kartellverstoß war der Verband deutscher Pfandbriefbanken. Der Verband der Pfandbriefbanken ist ebenfalls in der DK organisiert, hat jedoch nicht an den Arbeitskreisen im Bereich des Zahlungsverkehrs teilgenommen. Die in diesem Verband organisierten Institute bieten keine Zahlungsverkehrsleistungen an und wenden die Sonderbedingungen für das Online-Banking in der beanstandeten Form nicht an.

3. Einzelne Kreditinstitute der Spitzenverbände

19. Nicht beteiligt am Verfahren sind die von den Spitzenverbänden vertretenen einzelnen Kreditinstitute, die rein formal eigenständig darüber entscheiden, ob sie die in der DK erarbeiteten Muster-AGB übernehmen. Zur Überarbeitung der AGB-Vertragswerke verfügen die Spitzenverbände über ein Mandat der unmittelbar oder mittelbar angeschlossenen Kreditinstitute, so dass die inhaltliche Festlegung – von den Kreditinstituten gewollt – und auch die Beschlussfassung im Rahmen der DK durch die in der DK organisierten Verbände erfolgten. Auf Grund der Komplexität der in den AGB-Vertragswerken geregelten rechtlichen Fragestellungen haben einzelne Kreditinstitute aber tatsächlich allenfalls geringe Spielräume, von den für das Online-Banking vereinbarten Regelungen abzuweichen, und machen von dieser Möglichkeit in der Praxis kaum Gebrauch.

III. Die Beigeladenen

1. Sofort GmbH

20. Die Sofort GmbH, Gauting (im Folgenden: Sofort oder Beigeladene zu 5.), ist ein Dienstleistungsunternehmen und betreibt seit 2005 ein bankenunabhängiges Bezahlverfahren für den Internethandel unter der Marke „sofortueberweisung.de“. Dabei handelt es sich um einen Zahlungsauslösedienst[10], über den Zahlungen im Internethandel über das Online-Banking-Konto des Kunden ausgelöst werden. Kunden nutzen ihre Personalisierten Sicherheitsmerkmale (PIN und TAN)[11] für das Online-Banking, indem sie der Sofort damit den Zugang zu dem kontoführenden Kreditinstitut ermöglichen, so dass Sofort die Kontodeckung prüfen und die Zahlung zu Gunsten des Internethändler auslösen kann. Der Internethändler ist Vertragspartner von Sofort und zahlt für die Nutzung des Bezahlverfahrens ein Entgelt an Sofort, das in der Regel umsatzabhängig berechnet wird und deutlich preisgünstiger für Online-Händler ist, als z.B. bei einer Zahlung mit Paypal oder Kreditkarten. Das Bezahlverfahren wurde entwickelt, um für Online-Händler und Kunden die Nachfrage nach einem schnellen, sicheren und unkomplizierten Bezahlverfahren zu bedienen.

21. Sofort bietet das Bezahlverfahren seit mehr als 10 Jahren am Markt an. Neben Deutschland ist Sofort mittlerweile in weiteren 12 europäischen Ländern tätig, darunter in Österreich und der Schweiz. Insbesondere in Österreich ist der Marktanteil von Sofort signifikant höher als in Deutschland.[12] In Deutschland wird sofort von einer wachsenden Zahl von Händlern als Bezahlverfahren angeboten und wächst auch hinsichtlich der tatsächlich getätigten Transaktionen kontinuierlich. Derzeit wird Sofort nach eigener

---

[10] Zahlungsauslösedienste werden mit dem Inkrafttreten der überarbeiteten Zahlungsdiensterichtlinie im Jahr 2016 als Zahlungsdienste definiert. Sie ermöglichen den Zugang zu einem Zahlungskonto, das bei einem anderen Zahlungsdienstleister geführt wird. Der Begriff erfasst etwa Dienste, die eine Softwarebrücke zwischen der Website des Internet-Händlers und der Website des kontoführenden Instituts einrichten. Über diese Softwarebrücke kann der Zahler dann entweder selbst den Zahlungsvorgang autorisieren oder er gibt personalisierte Sicherheitsmerkmale wie z. B. PIN und/oder TAN an den dritten Zahlungsdienstleister weiter, damit dieser für den Zahler die Zahlung beim kontoführenden Institut einleitet. Vgl. http://wirtschaftslexikon.gabler.de/Archiv/-2046338290/zahlungsausloesedienst-v1.html, Stand 14.05.2016.

[11] Zu den Personalisierten Sicherheitsmerkmalen gehören u.a. die zur Autorisierung des Kunden verwendete Persönliche Identifikationsnummer (PIN) und die einmal verwendbaren Transaktionsnummern (TAN) zur Autorisierung von Geschäftsvorfällen gegenüber dem kontoführenden Kreditinstitut (im Beschluss werden Personalisierte Sicherheitsmerkmale vereinfachend mit PIN und TAN bezeichnet).

[12] EPSM Market Research Newsletter 03-04/16, S. 3 ff. Internet Payment in Germany: Diversity is king.

Darstellung von mehr als 35.000 Händlern angeboten.[13] Monatlich werden mehr als 3 Mio. Transaktionen mit dem Bezahlverfahren durchgeführt. Das Unternehmen beschäftigt mehr als 150 Mitarbeiter.[14]

22. Seit der Einführung des Bezahlverfahrens sind bisher keine Sicherheitsprobleme bekannt geworden. Zur Sicherung des Verfahrens betreibt Sofort Server, über welche die Kundendaten, ohne an den Internethändler übermittelt zu werden, an das jeweilige Kreditinstitut geschickt werden. Sofort hat vom TÜV Saarland die TÜV-Siegel „Geprüftes Zahlungssystem“ und „Geprüfter Datenschutz“ erhalten. Die Systeme des Unternehmens werden auf Servern betrieben, die sich innerhalb eines Bankenrechenzentrums befinden.[15]

23. Die Sofort gehört seit 2013 mittelbar, über eine 100%ige Beteiligung der Klarna Germany Holding GmbH, Berlin, zur schwedischen Klarna AB, Stockholm.[16] Die Klarna Gruppe ist einer der führenden europäischen Anbieter für Zahlungslösungen für Online-Händler. Zentrales Produkt von Klarna ist der Rechnungskauf, bei dem das Unternehmen alle Leistungen des Rechnungskaufs bis hin zum Inkasso übernimmt. Klarna arbeitet mit rund 50.000 Online-Händlern zusammen und bietet ihre Lösungen in 15 europäischen Ländern an. Klarna beschäftigt mehr als 1200 Mitarbeiter. Insgesamt nutzen 35 Mio. Kunden Dienstleistungen von Klarna.[17] Klarna erzielte nach öffentlich verfügbaren Informationen im Jahr 2013 einen Umsatz von mehr als 200 Mio. €.

24. Sofort bietet einen Zahlungsauslösedienst an, der von den den Regelungen der PSD2 für die Übergangsphase zwischen Inkrafttreten der Richtlinie und deren Umsetzung in nationales Recht erfasst ist und daher einen Bestandsschutz genießt. Denn die Übergangsregelungen legen fest, dass bereits am Markt tätige Zahlunsauslösedienste bis zur Umsetzung der Regelungen der PSD2 in nationales Recht beim Angebot ihrer Dienstleistungen nicht ungerechtfertigt behindert werden dürfen (vgl. Fn. 69).

---

13 https://www.sofort.com/ger-DE/ueber-uns/ueber-marktfuehrer-sofort-gmbh/, Stand 14.05.2016.

14 Neben dem Zahlungsauslösedienst bietet Sofort noch „PayCode“ an, eine Dienstleistung, bei der der Kauf von Waren oder Dienstleistungen im Internethandel über Rechnung abgewickelt wird, bei der die Zahlung aber ebenfalls über das Online-Banking des Kunden ausgelöst wird, für das Sofort ein Überweisungsformular bereitstellt. Außerdem bietet Sofort das Verfahren „Sofort Ident“ an, bei dem Kunden über das Online-Banking eine Altersverifizierung durchführen können.

15 Auch wenn diese spezifischen Anwendungen nicht unmittelbar der Bankenaufsicht unterliegen, besteht hier ein vergleichbarer sicherheitstechnischer Ansatz zu Produkten der deutschen Kreditwirtschaft (vgl. Rz 119).

16 Email, Kapellmann Rechtsanwälte, 30.01.2015, Bl. 6490 d.A., gemeint ist wohl die Klarna Germany Holding GmbH, Berlin, Amtsgericht Charlottenburg, HRB 153963 B.

17 https://www.klarna.com/de/ueber-uns/fakten-zahlen, Stand 03.06.2015.

2. giropay GmbH

25. Die giropay GmbH, Frankfurt am Main, (im Folgenden: giropay oder Beigeladene zu 6.) ist entstanden aus einem Projekt der Spitzenverbände der deutschen Kreditwirtschaft, mit dem diese das Ziel verfolgten, alternativ zur Sofort ein Bezahlverfahren im Internethandel durch die Bankenseite einzuführen. Auch bei dem von giropay angebotenen Bezahlverfahren handelt es sich um einen Zahlungsauslösedienst. Gesellschafter von giropay sind die Deutsche Postbank AG, Bonn, das genossenschaftliche Rechenzentrum Fiducia & GAD IT AG, Karlsruhe, (Fiducia & GAD), sowie die Star Finanz-Softwareentwicklung und Vertrieb GmbH, Hamburg, ein Tochterunternehmen der Finanz Informatik GmbH & Co. KG, Frankfurt, (FI), dem technischen Dienstleister und Rechenzentrum der Sparkassengruppe.

26. giropay bietet das Bezahlverfahren seit 2006 an. Es kann derzeit von rund 35 Mio. Online-Banking-Kunden genutzt werden. Dass nicht alle sondern lediglich rund 70% der Online-Banking-Kunden giropay nutzen können, liegt in der Organisation des Bezahlverfahrens begründet. Teilnehmen können nur Kunden solcher Kreditinstitute, die einen Vertrag mit giropay abgeschlossen haben.

27. Da sich giropay an deutsche Kreditinstitute wendet, erstreckt sich das Verbreitungsgebiet des Verfahrens im Wesentlichen auf das Gebiet der Bundesrepublik Deutschland. Darüber hinaus wird giropay beispielsweise in Österreich über eine Kooperation mit dem in Österreich von Banken betriebenen Bezahlverfahren „eps“ tätig. Beide Verfahren arbeiten über eine gemeinsame Schnittstelle zusammen, so dass Internethändler mit diesem Verfahren sowohl Kunden in Österreich als auch in Deutschland erreichen und Zahlungen aus beiden Ländern abgewickelt werden können.

28. Auch giropay verlangt ausschließlich von Internethändlern ein Entgelt, das sich an der Höhe des im Rahmen des Bezahlverfahrens bezahlten Preises orientiert. Kunden wird für die Nutzung von giropay kein unmittelbares Entgelt in Rechnung gestellt. Im Zusammenhang mit der Nutzung von giropay hat die DK einen speziellen Textschlüssel für unwiderrufbare Überweisungen entwickelt.[18] Da die durch giropay initiierten Transaktionen nicht widerrufen werden können, erhält der Händler eine besonders hohe Sicherheit über den bevorstehenden Zahlungseingang (Zahlungsgarantie).

---

[18] [redacted]

29. Genau wie Sofort bietet auch giropay den Online-Banking-basierten Rechnungskauf und die Altersverifikation des Kunden über das System an. Nach einer Studie der Bundesbank verwenden rund 3% der Kunden, die Internetbezahlverfahren generell nutzen, das von giropay angebotene Verfahren. Sofortüberweisung wird demgegenüber von 23% und Paypal von 88% dieser Kundengruppe genutzt.[19]

IV. Sorgfaltspflichten der Kunden in Bezug auf die Nutzung von Zahlungsauslösediensten im Internethandel

30. Mit den Online-Banking-Bedingungen als Teil der Allgemeinen Geschäftsbedingungen schaffen Kreditinstitute standardisierte Vertragsbeziehungen zu ihren Kunden als Nutzern des Online-Bankings[20].

31. Die in Deutschland tätigen Kreditinstitute haben – soweit sie ihren Kunden Online-Banking zur Nutzung anbieten – die von der Deutschen Kreditwirtschaft erarbeiteten OBB als Teil der Allgemeinen Geschäftsbedingungen (im Folgenden: AGB) zur vertraglichen Grundlage für die Geschäftsbeziehungen zu ihren Kunden gemacht. Die AGB-Regelwerke werden in der DK als Branchenstandards erarbeitet und den angeschlossenen Kreditinstituten von den der DK angeschlossenen und an der Erarbeitung beteiligten Spitzenverbänden zur Nutzung empfohlen.

1. Sorgfaltspflichten

32. In den im Jahre 2009 beschlossenen Online-Banking-Bedingungen haben die Beteiligten im Zusammenhang mit den für die Authentifizierung des Nutzers und der Autorisierung von Aufträgen im Online-Banking zentralen Personalisierten Sicherheitsmerkmalen eine Reihe von Sorgfaltspflichten festgelegt. Die Sorgfaltspflichten enthalten Vorschriften zu den Vorkehrungen, die zum Schutz von PIN und TAN zu beachten sind, sowie Regelungen, in welcher Weise diese zu nutzen sind bzw. welche Nutzung ausgeschlossen ist.

33. Im Einzelnen muss der Online-Banking-Nutzer Folgendes beachten: Er hat die Personalisierten Sicherheitsmerkmale geheim zu halten und nur im Rahmen einer

---

[19] Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2014, Dritte Studie über die Verwendung von Bargeld und unbaren Zahlungsinstrumenten, Frankfurt a.M. 2015, S. 73, Mehrfachnennungen bei der Nutzung von Bezahlverfahren im Internethandel waren möglich.

[20] Der Begriff des „Online-Bankings“ bezieht sich auf die Abwicklung von Bankgeschäften auf elektronischem Wege über das Internet. Im laufenden Text werden die Nutzer verschiedener Anwendungen stets als Kunden bezeichnet, da die Nutzung im Rahmen der Online-Banking-Kundenbeziehung erfolgt.

Auftragserteilung über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie sein Authentifizierungsinstrument vor dem Zugriff anderer Personen sicher zu verwahren (Ziff. 7.1 OBB). Insbesondere darf das Personalisierte Sicherheitsmerkmal nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden, ausdrücklich nicht auf Online-Händlerseiten (Ziff. 7.2 3. Spiegelstrich OBB).

34. Mit den 2009 beschlossenen OBB ist eine materielle Verschäfung der Sorgfaltspflichten verbunden, die auf die technische Fortentwicklung der Nutzungsmöglichkeiten des Online-Bankings (vgl. hierzu nachfolgende Gliederungspunkt IV. 5.) und der Marktgängigkeit von Zahlungsauslösediensten im Internethandel Bezug nimmt (vgl. hierzu nachfolgend Gliederungspunkt V.).

35. Bereits in den Vorversionen der OBB waren Regelungen zur Geheimhaltung von PIN und TAN enthalten. Die Btx[21]-Bedingungen von 1984 enthalten Regelungen, die sich auf den damals aktuellen Stand der von der DK wahrgenommenen Gefährdungslage bezogen:

„*Btx-Pin und Transaktionsnummern sind zur Vermeidung von Missbrauch geheimzuhalten. Sie dürfen Dritten nicht zugänglich gemacht werden; denn jede Person, die diese Berechtigungsmerkmale kennt, kann das Btx-Angebot in Anspruch nehmen*“.[22]

36. In den „Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ aus dem Jahre 2000 reagierte die DK bei der Formulierung der Sorgfaltspflichten auf Veränderungen des Online-Bankings. Da der Zugang auch außerhalb des Btx-Systems möglich war, nämlich über Internet-Provider, sollte - so die Darstellung der DK - sichergestellt werden, dass Kunden keine betrügerischen Server-Betreiber für den Zugang zum Konto nutzten. Hierzu enthielten die Bedingungen eine Regelung, die sich auf diese von der DK empfundene Gefahr und auf die Nutzung sicherer Zugangskanäle bezog:

„Der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot der

---

[21] Bildschirmtext gilt als Vorläufer des Online-Bankings. Dieses Verfahren wurde von der Deutschen Bundespost angeboten. Kunden konnten hiermit in beschränktem Umfang Zahlungsverkehrsaufträge an ihr Kreditinstitut senden und Kontoinformationen empfangen.

[22] Schreiben der DK vom 02.11.2010, S.3, Bl. 434 d.A.

Bank nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen."

2. Haftungsfragen

37. Die Einhaltung der Sorgfaltspflichten steht im Zusammenhang mit der Haftungsverteilung zwischen Kreditinstitut und Kunden in Schadensfällen. Der Nutzer haftet ohne Rücksicht auf Verschulden bis zu einem Betrag von 150 €, soweit nicht-autorisierte Zahlungsvorgänge auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments vor Sperranzeige beruhen.[23] In anderen Fällen missbräuchlicher Nutzung des Authentifizierungsinstruments haftet der Nutzer ebenfalls bis zu einem Betrag von 150 €, soweit er seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.[24] Im vollen Umfang muss der Nutzer den Schaden aus nicht autorisierten Zahlungsvorgängen vor Sperranzeige tragen, wenn er seine Sorgfaltspflichten vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt hat.[25] Als Fall der groben Fahrlässigkeit wird insbesondere die erkennbare Eingabe der Personalisierten Sicherheitsmerkmale außerhalb der gesondert vereinbarten Internetseiten genannt,[26] das umfasst insbesondere die Eingabe auf Online-Händlerseiten.[27]

38. Demgegenüber haften Kreditinstitute entsprechend der OBB bei nicht autorisierten Online-Banking-Verfügungen und/oder fehlerhaft ausgeführten Online-Banking-Verfügungen sowie nach Sperrung der Authentifizierungsinstrumente für Schäden in voller Höhe.

3. Folge für die Nutzung von Zahlungsauslösediensten auf dem Markt für Bezahlverfahren im Internethandel

39. Die Regelungen in Bezug auf die genannten Sorgfaltspflichten der Nutzer schließen die Nutzung bankenunabhängiger Produkte (z.B. Zahlungsauslösedienste) aus, solange deren Internetseiten nicht explizit von den einzelnen Kreditinstituten als solche benannt werden, auf denen Kunden ihre Personalisierte Sicherheitsmerkmale eingeben dürfen.

---

[23] Ziff. 10.2.1 Abs. 1 Online-Banking-Bedingungen.
[24] Ziff. 10.2.1 Abs. 2 Online-Banking-Bedingungen
[25] Ziff. 10.2.1 Abs. 5 Online-Banking-Bedingungen.
[26] Ziff. 10.2.1 Abs. 5 Satz 2 4. Spiegelstrich Online-Banking-Bedingungen.
[27] Ziff. 7.2 Abs. 2 3. Spiegelstrich Online-Banking-Bedingungen.

40. Die Regelungen betreffen nur die Zahlungsauslösedienste auf dem Markt für Bezahlverfahren im Internethandel. Die Sorgfaltspflichten beziehen sich nicht auf andere Produkte, bei denen Kunden ebenfalls Personalisierte Sicherheitsmerkmale im Rahmen der Nutzung lokal installierter Softwareprodukte oder auf Internetseiten eingeben, z.B. bei Online-Banking-Softwareprodukten.[28]

V. Entwicklung und Rahmenbedingungen des Online-Bankings in Deutschland

1. Wachsende Bedeutung des Online-Bankings bei der Abwicklung von Bankgeschäften

41. Traditionell wurden Bankdienstleistungen in Bankfilialen erbracht. Neben dem Filialgeschäft haben sich in den vergangenen 30 Jahren verschiedene andere Möglichkeiten zur Inanspruchnahme von Bankdienstleistungen etabliert. Einen wesentlichen Zugangskanal bildet heute das Online-Banking.[29] Hierbei erfolgt der Zugriff auf Konten über PCs, Smartphones oder vergleichbare mobile Endgeräte, mit denen eine Internetverbindung hergestellt werden kann. Alternativ werden neben dem Online-Banking-Zugang über einen Internetbrowser auch spezielle Softwareprodukte genutzt, welche den Zugang zum Online-Banking über eine Internetverbindung und eigens von der Kreditwirtschaft zu diesem Zwecke gestalteter Schnittstellen (HBCI/FinTS) herstellen.

42. Online-Banking hat sich in den letzten Jahren stark verbreitet. Während die Zahl der Girokonten in Deutschland in den Jahren zwischen 2003 und 2012 von 84 Mio. auf 96,1 Mio. um rund 14% gestiegen ist, nahm die Zahl der „Online-Konten“[30] im gleichen Zeitraum von 30,8 Mio. auf 50,3 Mio. zu. Dies entspricht einer Zunahme von mehr als 63%. Damit wurden 2012 mehr als die Hälfte der Girokonten als Online-Konten geführt.

---

[28] Sonstige Produkte werden entweder als Anwendung im Internet genutzt oder als Software auf Geräten des Kunden installiert und betrieben. Die Gefahren der Verarbeitung, Nutzung und Speicherung Personalisierter Sicherheitsmerkmale bei der Nutzung dieser Systeme wird in den Online-Banking-Bedingungen nicht thematisiert.

[29] Eine weitere Möglichkeit ist das Telefonbanking, bei dem Kunden telefonischen Zugang zu ihrem Kreditinstitut entweder über Call-Center oder Sprachcomputer erhalten.

[30] Zahlungsverkehrskonten, bei denen der Kontozugriff über das Internet erfolgen kann.

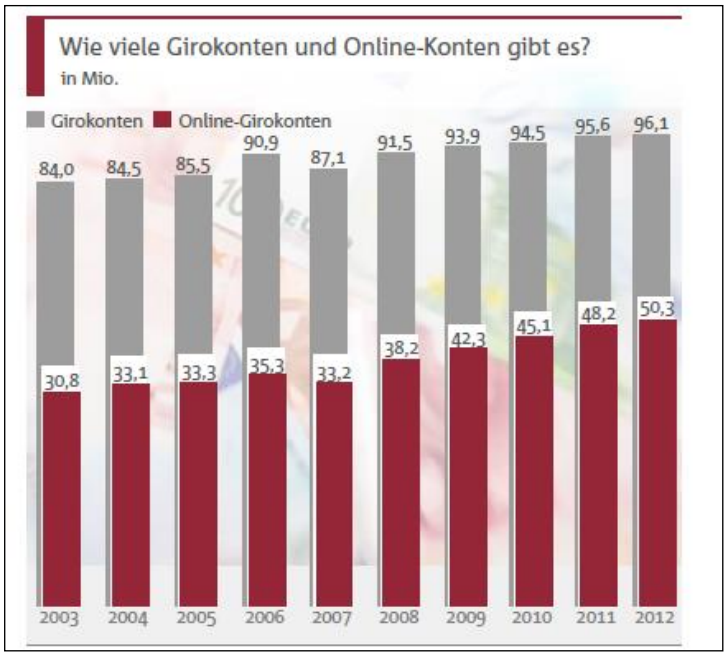


Abb. 1 - Online-Girokonten bei deutschen Kreditinstituten[31]

43. Mit der Bereitstellung der Infrastruktur hat sich im Zeitverlauf das Nutzungsverhalten der Kontoinhaber verändert. Der Anteil der Online-Banking-Kunden in Deutschland ist zwischen 2003 und 2013 von 26% auf 45% gestiegen.

---

[31] Zahlen, Daten, Fakten der Kreditwirtschaft, hrsg. vom Bundesverband deutscher Banken e.V., Berlin November 2013, S. 12, (http://bankenverband.de/publikationen/shopitem/dd247802306c4f789dd44b15417ed8de; Stand 21.02.2014), Bl. 4598 d.A.

Abb. 2 - Anteil der Online-Banking-Kunden in Deutschland[32]

44. Online-Banking ermöglicht Kunden den Zugriff auf verschiedene Kontoarten und Dienstleistungen, je nach Umfang des Angebots des kontoführenden Kreditinstituts. Im Bereich des Zahlungsverkehrs erhalten Kunden Zugriff auf Girokonten und die Möglichkeit z.B. zur Abfrage von Kontoständen und Umsätzen sowie zur Erteilung von Überweisungsaufträgen oder der Einrichtung und Bearbeitung von Daueraufträgen. Auch die Beantragung von Dispositionskrediten kann über diesen Zugang erfolgen. Online-Banking kann aber auch den Zugriff auf andere Kontoarten umfassen, wie z.B. Einlagenkonten, Kreditkonten und Wertpapierdepots. In der Regel werden über das Online-Banking alle Konten des Kunden bei dem entsprechenden Kreditinstitut zugleich eingebunden.

45. Online-Banking-fähige Girokonten können vom Kontoinhaber zudem für die Abwicklung von Bezahlprozessen im Internethandel, auch im Zusammenhang mit dem Angebot von Zahlungsauslösediensten, genutzt werden.

46. Für Online-Banking nutzbare Girokonten eröffnen Kunden die Möglichkeit, Produkte Dritter in Anspruch zu nehmen, mit denen z.B. Kontoinformationen nicht ausschließlich

---

[32] Zahlen, Daten, Fakten der Kreditwirtschaft, hrsg. vom Bundesverband deutscher Banken e.V., Berlin November 2013, S. 13, (http://bankenverband.de/publikationen/shopitem/dd247802306c4f789dd44b15417ed8de; Stand 21.02.2014), Bl. 4599 d.A.

über die vom Kreditinstitut zur Verfügung gestellten Zugangsmöglichkeiten (z.B. Internetseite des kontoführenden Kreditinstituts) abgerufen werden können. Solche von Dritten zur Verfügung gestellten **Kontoinformationsdienste** werden als Softwareapplikationen auf Kundengeräten, z.B. PCs, mobilen Geräten oder über Internetanwendungen betrieben. Kunden können so Informationen über verschiedene Konten bei unterschiedlichen Kreditinstituten zusammenfassen, darstellen und auswerten.

a) Zugang zum Online-Banking und Auslösung von Geschäftsvorfällen

47. Voraussetzung für die Nutzung des Online-Bankings ist die Verfügbarkeit eines Internetzugangs über einen PC oder ein vergleichbares mobiles Endgerät und eine Internetverbindung.

48. Der Zugang zum Online-Banking des jeweiligen Kreditinstituts wird entweder über eine Software hergestellt, die auf dem Endgerät des Kunden installiert wird und die durch Nutzung einer gemeinsamen Schnittstelle der DK (FinTS) mit dem Kreditinstitut des Kunden bzw. dessen Rechenzentrum kommuniziert, oder über die Nutzung eines Internetbrowsers, welcher die Verbindung zur Online-Banking-Website des Kreditinstituts aufbaut.

49. Soweit der Kunde spezielle Software auf seinem Endgerät nutzt, gibt er seine Zugangsdaten für das Online-Banking auf seinem Endgerät ein, bevor die Software diese an das Kreditinstitut sendet.

50. Auf der Internetseite des Kreditinstituts gibt der Online-Banking-Kunde seine Zugangsdaten unmittelbar in die von dem Kreditinstitut bereitgestellte Infrastruktur ein, damit das Kreditinstitut die Authentizität des Kunden prüfen und so sicherstellen kann, dass nur der Berechtigte Zugang zum Konto erhält.[33] Es handelt sich dabei in der Regel um die Kontonummer oder eine spezielle Zugangsnummer[34] für das Online-Banking, die zusammen mit der PIN den Zugang zum Konto und den damit verbundenen Anwendungen ermöglicht.[35]

---

[33] http://www.die-deutsche-kreditwirtschaft.de/uploads/media/DK_Kompendium_Online-Banking-Sicherheit_V1.2.pdf, (Version: Februar 2014), Stand 11.06.2014.

[34] Zum Beispiel im Online-Banking der comdirect.

[35] Zum Teil wird von Kreditinstituten neben der PIN zusätzlich noch die Eingabe einer weiteren Zahlen- oder Buchstabenkombination oder Teilen davon verlangt, die nur per Mausklick und nicht per Tastatur erfolgen kann, um ein erhöhtes Sicherheitsniveau zu gewährleisten (https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniert DasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst=true&docId=3589572), Stand 11.06.2014.

51. Um nach Authentifizierung im Online-Banking des Kreditinstituts einen Auftrag an das Kreditinstitut zu erteilen, gibt der Kunde – unabhängig davon, ob eine Software genutzt oder die Verbindung über den Internetbrowser hergestellt wurde – eine TAN ein, die der Bank als Nachweis dafür dient, dass es sich um eine Willenserklärung des Online-Banking-Kunden handelt. Die TAN kann Kunden auf unterschiedlichen Wegen zur Verfügung gestellt werden.[36] Die TAN-Verfahren werden von der Kreditwirtschaft gemeinsam fortentwickelt, insbesondere um zu verhindern, dass die bestehenden Verfahren kein ausreichendes Sicherheitsniveau mehr gewährleisten.

b) Gefahren des Online-Bankings

52. Mit der Eingabe von PIN und TAN für die Authentifizierung und Bestätigung der Willenserklärung sind Missbrauchsrisiken verbunden. Kriminelle, denen es gelingt, die relevanten Daten zu erlangen, können damit auf Kontoinformationen zugreifen und missbräuchlich über die Konten verfügen. Die Beschaffung von PIN und TAN auf elektronischem Wege zur Durchführung von Straftaten wird als **Phishing**[37] bezeichnet. Dabei werden Online-Banking-Kunden dazu veranlasst, PIN und TAN ungewollt an Dritte weiterzugeben. Dies kann durch gefälschte Emails oder Internetseiten geschehen, die Kunden fälschlicherweise suggerieren, es handle sich um eine Nachricht oder Internetseite seines Kreditinstituts. Kunden werden in beiden Fällen dazu aufgefordert, PIN und TAN in einer Antwortmail zu übersenden oder auf der gefälschten Internetseite einzugeben.[38]

53. Auch über Schadsoftware kann die Eingabe von Aufträgen manipuliert werden. Unter anderem bei den sogenannten „Man-In-The-Middle-Angriffen“[39] geht die Gefahr von

---

[36] Zu den in der Praxis verwendeten Verfahren zur Übermittlung der TAN vgl. unter Rz. 54ff.

[37] Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln" (https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html, Stand 12.06.2014).

[38] https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/GefahrenUndSicherheitsrisiken/Gefahren_Sicherheitsrisiken.html?notFirst=true&docId=3605830, Stand 12.06.2014.

[39] Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer "in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind. (Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkatalog,

Schadsoftware aus, die sich auf dem Endgerät des Kunden befindet, das für den Zugang zum Online-Banking verwendet wird. Durch die Schadsoftware kann der Datenverkehr zwischen dem Kunden und seinem Kreditinstitut manipuliert werden, indem z.B. Empfängerkontoverbindung und Überweisungsbetrag verändert weitergeleitet werden.

c) Sicherungsverfahren im Online-Banking

54. Um angemessen auf die Bedrohungsszenarien und -entwicklungen reagieren zu können, hat die Kreditwirtschaft die Verfahren, mit deren Hilfe Aufträge an das Kreditinstitut über das Online-Banking freigegeben werden können, in den vergangenen Jahren permanent fortentwickelt. Während in der Anfangszeit einfache TAN-Listen an Kunden verschickt wurden,[40] werden durch den Einsatz weiterer Medien zur TAN-Erzeugung und –Übertragung zusätzliche Sicherheitsstandards realisiert,[41] um Missbräuche, insbesondere durch Schadsoftware, zu verhindern.[42]

55. Zur Reaktion auf die Man-in-the-Middle Angriffe wurde das sogenannte **iTANplus-Verfahren** eingeführt, bei dem der Online-Banking-Kunde vor der TAN-Eingabe die Transaktionsdaten am Bildschirm kontrollieren kann, was die Manipulation der eingegebenen Daten durch Schadsoftware erschwert.[43]

---

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html, Stand 16.07.2014.

40 Beim klassischen TAN-Verfahren aus den Anfängen des Online-Bankings erhielten Kunden per Post eine Liste mit einer größeren Anzahl von TAN, die sukzessive für die Auftragserteilung genutzt wurden. Die einmal verwendbaren TAN wurden vom Kunden in beliebiger Reihenfolge ausgewählt und nach Gebrauch aus der Liste gestrichen. Dieses Verfahren war besonders anfällig für Phishing-Angriffe, da mit der PIN und jeder erbeuteten TAN eine neue Verfügung des Angreifers vom Kundenkonto möglich war. Um die Missbrauchsmöglichkeiten zu reduzieren wurde das iTAN-Verfahren (indizierte-TAN-Verfahren) entwickelt. Hierbei erhält der Kunden eine nummerierte TAN-Liste. Beim Auslösen einer Transaktion wird der Kunde aufgefordert, eine bestimmte TAN einzugeben. Auch wenn es durch einen Phishing-Angriff gelingt, eine TAN eines Online-Banking-Kunden zu erbeuten, kann damit keine Transaktion ausgelöst werden, wenn dem Angreifer die dazugehörige Indizierung nicht bekannt ist. Damit beinhaltet dieses TAN-Verfahren eine zusätzliche Sicherheitsschwelle.

41 Bereits im Jahre 2009 hat das Bundeskriminalamt aber darauf hingewiesen, dass das iTAN-Verfahren nicht als sicher anzusehen sei, weil die Verbreitung von Schadsoftware stetig zugenommen habe (https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniert/DasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst=true&docId=3600852, Stand 12.06. 2014).

42 Die folgende Darstellung soll einen exemplarischen Überblick über die Verfahren und deren Entwicklung durch die DK geben, ohne dass die Darstellung der Verfahrensvarianten einen vollständigen Überblick geben kann.

43 https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniert DasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst=true&docId=3600852 Stand 12.06.2014.

56. Der weiteren Verbesserung der Online-Banking-Sicherheit dient das sogenannte **mTAN oder SMS-TAN**-Verfahren, bei dem ein eigenständiger Übertragungsweg für die Mitteilung der zu nutzenden TAN eröffnet bzw. zur Bedingung gemacht wird. Kunden registrieren zu diesem Zweck eine Mobilfunknummer, über die die entsprechende TAN für die Autorisierung eines Auftrags gegenüber dem Kreditinstitut mitgeteilt wird. Dabei entfällt die Übersendung einer TAN-Liste. Zusammen mit der TAN erhalten Kunden Angaben zu Auftragsdetails (z.B. die Angabe der Höhe des Überweisungsbetrags und/oder die Empfängerkontonummer), mit deren Hilfe Manipulationen durch Schadsoftware weiter erschwert werden sollen.

57. Ein weiteres Verfahren zur Erhöhung der Sicherheit gegen Phishing und Schadsoftware stellt die Nutzung eines **TAN-Generators** dar, der auf Knopfdruck oder durch Eingabe einer von der Bank für den konkreten Auftrag übermittelten Kontrollnummer eine TAN erzeugt. Auch bei der Nutzung eines TAN-Generators hat die DK die bestehenden TAN-Verfahren fortentwickelt. Bei dem **Chip-TAN-Verfahren** (auch als **smart-TAN-Verfahren** bezeichnet) wird die TAN über die Nutzung eines TAN-Generators erzeugt. Zunächst wird hierbei die Bank- oder girocard in den TAN-Generator eingeführt, mit deren Hilfe das Gerät die TAN errechnet. Die hierfür benötigten Auftragsdetails werden entweder manuell eingegeben oder per Flickercode vom Bildschirm des Geräts, über welches der Online-Banking-Zugang hergestellt worden ist, als Lichtsignale über eine optische Schnittstelle am TAN-Generator übertragen. Die Auftragsdetails werden auf dem TAN-Generator angezeigt und können vom Kunden überprüft werden.

58. Neben den TAN-Verfahren hat die DK gemeinsam weitere Sicherungsverfahren zum Schutz des Online-Bankings entwickelt. Hierzu zählt die **FinTS-(HBCI)-Karte**, die mit einem Signaturkarten-Lesegerät genutzt wird, durch welches der Auftrag an die Bank vor der Übertragung verschlüsselt und mit einer Signatur versehen wird. Die Signatur wird mit dem Auftrag an das Kreditinstitut geschickt und dort entschlüsselt. Da die Auftragsdetails mit der Signatur zusammenhängen, ist eine Veränderung des Auftrags nach dem Versand nicht mehr möglich.[44]

59. Die DK hat Standards für ein eigenes Signaturkarten-Lesegerät entwickelt. Der sogenannte **Secoder** zeigt auf dem integrierten Bildschirm die Transaktionsdaten an und sendet die Auftragsdaten verschlüsselt und signiert an das kontoführende Kreditinstitut.[45]

---

[44] http://www.die-deutsche-kreditwirtschaft.de/uploads/media/DK_Kompendium_Online-Banking-Sicherheit_V1.2.pdf, S. 2f., Stand 12.06. 2014.

[45] https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst=true&docId=3602916,

Dabei führt die DK ein Freigabe- und Zertifizierungsverfahren zur Gewährleistung der Sicherheit der am Markt erhältlichen Secoder-Produkte durch.[46] Die DK testet die Funktionen und die Sicherheit der am Markt angebotenen Geräte und verleiht daraufhin ein Siegel als Empfehlung der Banken und Sparkassen.[47]

2. Rechtlicher Rahmen für die Ausgestaltung der Sorgfaltspflichten beim Online-Banking im Jahre 2009

60. Aufgrund der mit der Nutzung des Online-Bankings verbundenen Risiken des missbräuchlichen Zugangs zu Konten und der Durchführung rechtswidriger Verfügungen über ihre finanzielle Mittel werden Online-Banking-Kunden besondere Sorgfaltspflichten in Bezug auf die Verwendung der Zugangsdaten auferlegt. Diese ergeben sich zum Teil aus gesetzlichen Regelungen und – soweit diese nicht abschließend sind - zusätzlich aus den von der Kreditwirtschaft in den AGB konkretisierten Pflichten.

61. Die gesetzlichen Regelungen in Bezug auf die Nutzung der von Kreditinstituten ausgegebenen Zugangsdaten basieren auf europäischem Recht. Die erste europäische Zahlungsdiensterichtlinie (auch hierfür wird im Folgenden die Abkürzung PSD für die englische Bezeichnung der Richtlinie verwendet)[48] wurde hinsichtlich der für die Sorgfaltspflichten der Zahlungsdienstenutzer (Online-Banking-Kunden) relevanten Teile im Bürgerlichen Gesetzbuch[49] in nationales Recht umgesetzt. Die zivilrechtlichen Vorschriften regeln schwerpunktmäßig die Stärkung der Rechte der Zahlungsdienstenutzer unter besonderer Berücksichtigung des Verbraucherschutzes in den §§ 675 c ff. BGB.[50] Die im BGB eingefügten Vorschriften legen aber gleichfalls Pflichten von Zahlungsdienstenutzern fest, welche dort, wo sie unbestimmt formuliert sind,

---

Stand 12.06. 2014 sowie http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html, Stand 12.06.2014.

46 http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html, DK Kompendium Online-Banking Sicherheit, S. 3.

47 http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html.

48 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13.11.2007 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 Text von Bedeutung für den EWR, Amtsblatt Nr. L 319 v. 05.12.2007, S. 1-36.

49 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 16 des Gesetzes vom 29.06.2015 (BGBl. I S. 1042) geändert worden ist.

50 Findeisen in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, § 1 ZAG, Rz. 15.

von Kreditinstituten als Zahlungsdienstleistern und Betreibern von Zahlungsdiensten im Rahmen ihrer Allgemeinen Geschäftsbedingungen präzisiert werden.

a) Zahlungsdiensterichtline (alt)

62. Kreditinstitute, die sowohl das Einlagen- als auch das Kreditgeschäft anbieten und ihren Kunden im Rahmen des Online-Bankings die Möglichkeit eröffnen, Zugriff auf die bei ihnen geführten Konten zu nehmen sowie die Erteilung elektronisch übermittelter Überweisungsaufträge mittels Zahlungsinstrumenten vorzunehmen, erbringen als Zahlungsdienstleister[51] einen Zahlungsdienst[52] gegenüber einem Zahlungsdienstenutzer (z.B. Bankkunden). Die Pflichten der Zahlungsdienstenutzer und der Zahlungsdienstleister, die den Schutz der Zahlungsinstrumente und hier insbesondere die Personalisierten Sicherheitsmerkmale betreffen, waren früher in der PSD geregelt.

63. Die 2007 in Kraft getretene Richtlinie hatte das Ziel, einen Rechtsrahmen für unbare Zahlungen im europäischen Binnenmarkt zu schaffen.[53]

64. In Art. 56[54] regelte die PSD die Pflichten des Zahlungsdienstenutzers in Bezug auf die Verwendung der Zahlungsinstrumente. Entsprechend Artikel 56 Abs. 1 lit. a) PSD hatte der zur Nutzung eines Zahlungsinstruments berechtigte Zahlungsdienstenutzer die Pflicht, die Bedingungen für deren Ausgabe einzuhalten und zu diesem Zweck gem. Absatz 2 unmittelbar nach Erhalt eines Zahlungsinstruments insbesondere alle zumutbaren Vorkehrungen zu treffen, um die Personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

65. Keine Zahlungsdienstleister im Sinne der PSD waren Dienstleister wie Zahlungsauslösedienste (z.B. Sofort oder giropay), welche Überweisungen an das kontoführende Kreditinstitut weiterleiten und dem Händler auf der Basis einer Kontodeckungsprüfung eine Mitteilung darüber geben, ob mit dem Eingang der Zahlung zu rechnen ist. Auch Anbieter von Kontoinformationsdiensten erfasste die PSD nicht.

---

[51] Die von der DK bei der Ausgestaltung der AGB-Vertragswerke vertretenen Kreditinstitute sind Zahlungsdienstleister in Sinne der PSD. Gemäß Art. 1 Abs. 1 lit. a) PSD handelt es sich bei Kreditinstituten im Sinne von Art. 4 Nr. 1 lit. a) der Richtlinie 2006/48/EG bzw. § 1 Abs. 1 Nr. 1 ZAG um Zahlungsdienstleister.

[52] Zahlungsdienste sind gem. Art. 4 Nr. 3 PSD jede gewerbliche Tätigkeit, die im Anhang zur Richtlinie aufgeführt ist. Dazu zählt auch die unter Nr. 3 des Anhangs genannte Ausführung von Zahlungsvorgängen einschließlich des Transfers von Geldbeträgen auf ein Zahlungskonto bei einem Zahlungsdienstleister durch die Ausführung von Überweisungen.

[53] Findeisen, in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, § 1 ZAG, Rz. 3.

[54] Teil IV, Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten, Kapitel 2, Autorisierung von Zahlungsvorgängen.

Solche Dienstleister unterfielen damals keiner spezifisch finanzwirtschaftlichen Aufsicht. Dies galt auch dann, wenn die Angebote von Dienstleistern aus dem Bankensektor stammten. Die finanzwirtschaftliche Aufsicht über diese Anbieter erstreckte sich nicht auf diese Angebote.

66. Die Novellierung der PSD wurde auch vor dem Hintergrund der bestehenden Tätigkeit von Zahlungsauslösediensten mit dem Ziel geführt, diese Dienstleistungen in den rechtlichen Handlungsrahmen zu integrieren und sie einer Aufsicht zu unterstellen. Dies ist mit Inkrafttreten der PSD2 geschehen (siehe dazu Rd. 83ff.).

b) Zivilrechtliche Umsetzung der Zahlungsdiensterichtlinie (alt) in nationales Recht

67. Der Gesetzgeber hat die Regelungen der PSD durch das Gesetz zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zahlungsdiensterichtlinie (Zahlungsdiensteumsetzungsgesetz) [55] in nationales Recht umgesetzt. Aufsichtsrechtliche Regelungen werden im Gesetz über die Beaufsichtigung von Zahlungsdiensten (ZAG)[56] sowie Änderungen im Gesetz über das Kreditwesen (Kreditwesengesetz – KWG)[57] geregelt. Die Umsetzung des zivilrechtlichen Teils für Zahlungsdiensteanbieter erfolgte in einem eigenständigen Gesetz, dem Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie, sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29.07.2009. [58] Die entsprechenden Regelungen wurden in das Bürgerliche Gesetzbuch (BGB) aufgenommen.[59]

68. Die zivilrechtlichen Vorschriften zur Umsetzung der Zahlungsdiensterichtlinie im BGB regeln u.a. Fragen zum Zugang zu Online-Banking-Systemen der Kreditwirtschaft und der

---

55 Zahlungsdiensteumsetzungsgesetz vom 29.06.2009 (BGBl. I 1505).

56 Zahlungsdiensteaufsichtsgesetz vom 25.06.2009 (BGBl. I S. 1506), das durch Artikel 342 der Verordnung vom 31.08.2015 (BGBl. I S. 1474) geändert worden ist.

57 Kreditwesengesetz in der Fassung der Bekanntmachung vom 09.09.1998 (BGBl. I S. 2776), das durch Artikel 339 der Verordnung vom 31.08.2015 (BGBl. I S. 1474) geändert worden ist.

58 Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie, sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29.07.2009 (BGBl I 2355).

59 Der konkrete hier dargestellte Sachverhalt bezieht sich auf das Verhältnis zwischen Kreditinstituten und ihren Kunden, die Online-Banking in Anspruch nehmen. Gem. § 675 c Abs. 3 BGB sind die Begriffsbestimmungen des KWG und des ZAG entsprechend für die Regelungen im BGB anzuwenden. Soweit daher im Gesetzestext von Zahlungsdienstleistern (§ 1 Abs. 1 ZAG) und Zahlungsdiensten (§ 1 Abs. 2 ZAG) die Rede ist, wird im Folgenden der Begriff Kreditinstitut verwendet. Der Begriff des Zahlungsdienstnutzers wird in § 675 f Abs. 1 BGB als Person, die einen Zahlungsdienst u.a. als Zahler in Anspruch nimmt, definiert. Im Folgenden wird in diesem Zusammenhang der Begriff des Online-Bankings Nutzers (bzw. Kunde) benutzt. Vgl. dazu Palandt (74. Auflage), § 675 c BGB, Rz. 10.

Autorisierung von Überweisungsaufträgen im Rahmen der Online-Banking-Nutzung in Kapitel 3, „Erbringung und Nutzung von Zahlungsdiensten“, insbesondere im Unterkapitel 1 die Autorisierung von Zahlungsvorgängen und Zahlungsauthentifizierungsinstrumente.[60]

69. Konkrete Regelungen bezüglich der Pflichten des Online-Banking-Kunden im Rahmen der Nutzung des Online-Bankings ergeben sich aus § 675 Abs. 1 S. 1 BGB, in dem die Sorgfaltspflichten in Bezug auf die Zahlungsauthentifizierungsinstrumente[61] geregelt sind. Danach ist der Online-Banking-Kunde verpflichtet, unmittelbar nach Erhalt eines Zahlungsauthentifizierungsinstruments alle zumutbaren Sicherheitsvorkehrungen bezogen auf die Personalisierten Sicherheitsmerkmale zu treffen, um diese vor unbefugtem Zugriff und damit vor Missbrauch zu schützen. Die Vorschrift setzt Artikel 56 Abs. 1 lit. a) und Abs. 2 der Zahlungsdiensterichtlinie um. Die Vorschrift ist auf Girokontoverträge mit der Nutzung von Online-Banking-Diensten anwendbar, da es sich hierbei um Zahlungsdiensterahmenverträge im Sinne des § 675f Abs. 2 BGB handelt.

70. Der Begriff der Personalisierten Sicherheitsmerkmale wird weder in der Zahlungsdiensterichtlinie, in §§ 675c ff. BGB noch im ZAG oder KWG näher bestimmt. Das Personalisierte Sicherheitsmerkmal wird als Teil des Zahlungsauthentifizierungsinstruments angesehen und stellt eine Wissenskomponente dar, die dem Zahler vom Zahlungsdienstleister zugeteilt wird, nur ihm bekannt ist und zum Zwecke der Authentifizierung von Zahlungsaufträgen genutzt wird.[62] Im Rahmen des Online-Bankings kommen als Personalisierte Sicherheitsmerkmale z.B. PIN, TAN, elektronische Signatur oder Passwörter in Betracht.

---

60 Nach § 675j Abs. 1 S.1 BGB bedarf ein wirksamer Zahlungsvorgang der Zustimmung des Zahlers (Autorisierung). Zur Art und Weise der Zustimmung müssen zwischen dem Zahler und seinem Zahlungsdienstleister entsprechende Vereinbarungen getroffen werden. Der Wortlaut der gesetzlichen Regelung sieht vor, dass die Erteilung der Zustimmung mittels eines bestimmten Zahlungsauthentifizierungsinstruments vereinbart werden kann. Ob die Autorisierung einer Zahlung nur durch den Zahler oder auch durch eine dritte Person erfolgen kann, regelt das Gesetz nicht. Nach § 675k BGB kann die Bank durch Vereinbarung dazu ermächtigt werden, das Zahlungsauthentifizierungsinstrument zu sperren, wenn der Verdacht einer nicht-autorisierten oder einer betrügerischen Verwendung des Zahlungsauthentifizierungsinstrumentes besteht. Als nicht-autorisierte Verwendung gilt dabei die Nutzung des Zahlungsauthentifizierungsinstruments gegen oder ohne den Willen des Zahlers (z.B. in Bezug auf die Verwendung von PIN und TAN im Online-Banking). Vgl. Frey in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, § 675k BGB, Rz. 10.

61 Entsprechend § 1 Abs. 5 ZAG handelt es sich bei Zahlungsauthentifizierungsinstrumenten um jedes personalisierte Instrument, das zwischen Zahlungsdienstnutzer und dem Zahlungsdienstleister für die Erteilung von Zahlungsaufträgen vereinbart wird und das vom Zahlungsdienstnutzer eingesetzt wird, um einen Zahlungsauftrag zu erteilen.

62 Frey in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, § 675l BGB, Rz. 5.

71. Neben der Definition der Personalisierten Sicherheitsmerkmale lassen die gesetzlichen Regelungen ebenfalls offen, welchen Umfang die „zumutbaren Sicherheitsvorkehrungen“ umfassen und was unter „unbefugtem Zugriff“ zu verstehen ist. Als unbefugter Zugriff wird in der Kommentierung jeder nicht von vertraglichen Vereinbarungen gedeckte Zugriff verstanden.[63] Insoweit erfordern die gesetzlichen Vorschriften die Ausgestaltung und Präzisierung durch vertragliche Regelungen. Die Kreditwirtschaft verwendet hier keine einzelvertraglichen Regelungen sondern greift standardmäßig auf die Sonderbedingungen für das Online-Banking als Teil der AGB-Vertragswerke zurück.

c) AGB zur Vereinheitlichung der Vertragsbeziehung und zur Definition offener Rechtsbegriffe

72. Die DK hat die Allgemeinen Geschäftsbedingungen und die Online-Banking-Bedingungen (OBB) bis zum Jahre 2009 überarbeitet. Seitdem verwenden Mitgliedsinstitute der einzelnen Spitzenverbände diese gegenüber ihren Kunden. Die OBB sind Bestandteil des Vertrages zwischen Bank und Kunde und regeln die vertraglichen Rechte und Pflichten bei der Nutzung des Online-Bankings.

73. Die von der DK erarbeiteten OBB regeln grundsätzliche Fragestellungen der vertraglichen Beziehung zwischen Kreditinstitut und Kunde bei der Nutzung des Online-Banking-Angebots. Die OBB definieren das Leistungsangebot (Nr. 1). Danach können Kunden Bankgeschäfte abwickeln und Informationen der Bank abrufen. Den Umfang der über Online-Banking abzuwickelnden Bankgeschäfte legt das jeweilige Kreditinstitut dagegen individuell fest.

74. Des Weiteren enthalten die OBB Regelungen zu den Voraussetzungen für die Nutzung des Online-Bankings (Nr. 2), dem Zugang zum Online-Banking (Nr. 3) und zur Erteilung und zum Widerruf von Aufträgen (Nr. 4.1 und 4.2). Danach gilt, dass für die Abwicklung von Bankgeschäften mittels Online-Banking die vereinbarten Personalisierten Sicherheitsmerkmale zur Authentifizierung und Autorisierung benötigt werden, um sich gegenüber dem Kreditinstitut als berechtigter Teilnehmer[64] auszuweisen und Aufträge zu autorisieren (vgl. oben unter Rz. 69). Die Mittel, durch die Teilnehmer die TAN bzw. eine elektronische Signatur zur Ausführung von Aufträgen im Rahmen des Online-Bankings

---

[63] Sprau in: Palandt (74. Auflage), § 675l,Rz 2; Vgl. Frey in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht,, § 675l BGB, Rz. 9.

[64] Der Begriff Teilnehmer wird unter Ziffer 1 Abs. 2 der OBB definiert. Darunter gefasst werden neben dem Konto- bzw. Depotinhaber auch Bevollmächtigte, die das Online-Banking-Angebot der Kreditinstitute nutzen.

erhalten, werden durch die OBB als Authentifizierungsinstrumente definiert. Hierbei kann es sich um eine Liste mit einmal verwendbaren TAN handeln, einen TAN-Generator, über den Chip-TAN erzeugt werden, bzw. um ein mobiles Endgerät, über welches TAN per SMS („SMS-TAN“) an den Teilnehmer des Online-Bankings geschickt werden.

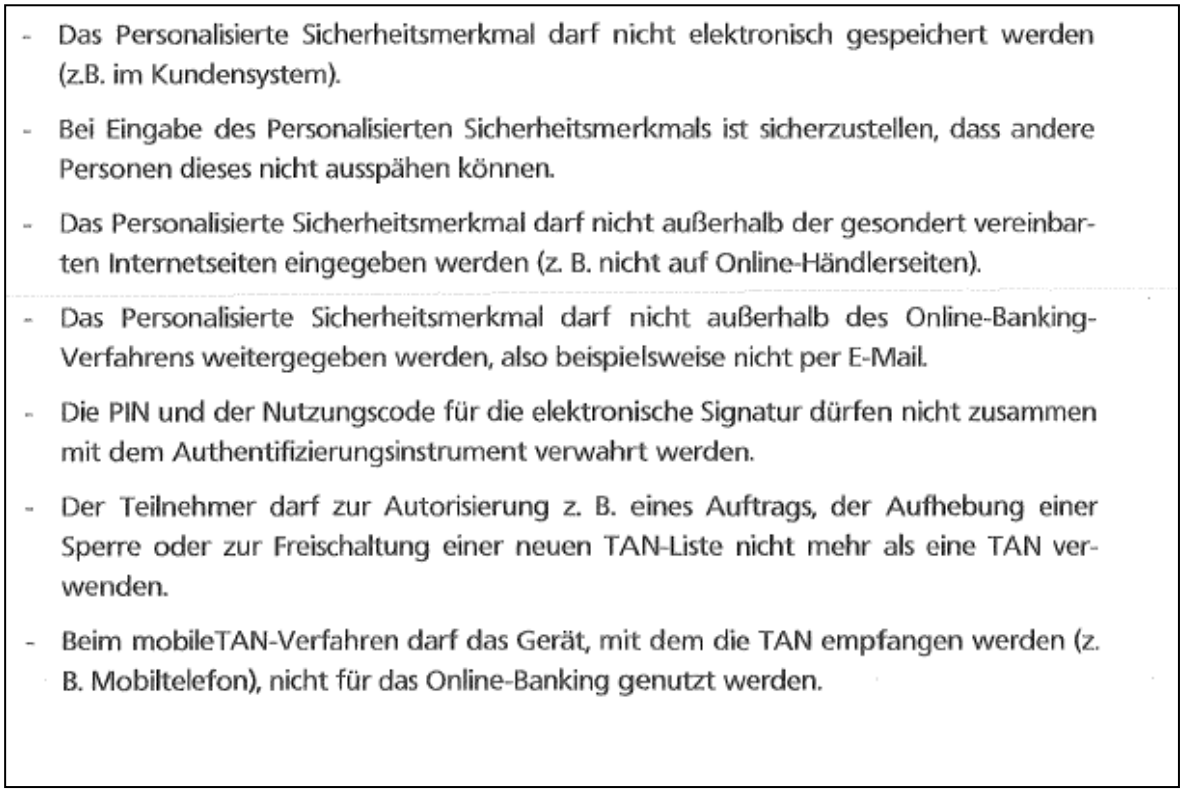
75. Neben Regelungen zur Bearbeitung von Online-Banking-Aufträgen durch das Kreditinstitut (Nr. 5) und zu Informationen des Kontoinhabers über Online-Banking-Verfügungen (Nr. 6) enthalten die OBB auch Sorgfaltspflichten des Teilnehmers (Nr. 7). Zu den Sorgfaltspflichten gehört die Herstellung der technischen Verbindung zum Online-Banking über die von dem Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle. Exemplarisch wird hier die Internetadresse genannt. Eine weitere Pflicht des Teilnehmers bezieht sich auf den Umgang mit den Personalisierten Sicherheitsmerkmalen und den Authentifizierungsinstrumenten.

76. In Bezug auf die Personalisierten Sicherheitsmerkmale sehen die Regelungen eine Pflicht zur Geheimhaltung vor. Die Übermittlung an das Kreditinstitut hat danach im Rahmen der Auftragserteilung nur über die gesondert mitgeteilten Online-Banking-Zugangskanäle zu erfolgen. Begründet werden diese Pflichten mit der Gefahr, dass Personen, die im Besitz des Authentifizierungsinstruments sind, in Verbindung mit den Personalisierten Sicherheitsmerkmalen das Online-Banking missbräuchlich nutzen können.[65]

77. Zum besonderen Schutz Personalisierter Sicherungsmerkmale und Authentifizierungsinstrumente enthalten die OBB einen Katalog besonderer Schutzvorschriften, die Online-Banking-Kunden zu beachten haben. Hierzu gehören:

---

[65] Online-Banking-Bedingungen Ziffer 7.2 Abs. 1 S. 2.



- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z.B. im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Online-Banking genutzt werden.

Abb. 3 - OBB Nr. 7.2 Abs. 2[66]

78. Daneben hat der Kunde die Sicherheit der eingesetzten Hardware zu gewährleisten und dazu die Sicherheitshinweise des Kreditinstituts zu beachten (Nr. 7.3). bzw. die Auftragsdaten – soweit diese über ein anderes als dem zur Eingabe verwendeten Gerät angezeigt werden – zu überprüfen. Die OBB verpflichten den Kunden vor Bestätigung des Auftrags zur Prüfung, ob die von dem Kreditinstitut angezeigten Auftragsdaten mit den für die Transaktion vorgesehenen Daten übereinstimmen (Nr. 7.4).

79. Schließlich enthalten die OBB unter Nr. 8 Anzeige- und Unterrichtungspflichten des Kunden sowie unter Nr. 9 die Pflicht bzw. das Recht des Kreditinstituts, die Nutzung des Online-Bankings auf Veranlassung des Kunden oder auf eigene Veranlassung zu sperren. Abschließend regeln die OBB unter Nr. 10 die Haftung der Bank bei einer nicht autorisierten bzw. einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung (Nr. 10.1) sowie die Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments (Nr. 10.2).

---

[66] Schreiben der DK vom 05.08.2009, Änderungen in den Allgemeinen Geschäftsbedingungen und den Sonderbedingungen mit Zahlungsverkehrsrelevanz, Anlage 19, Sonderbedingungen für das Online-Banking, Bl. 6470ff d.A.

3. Entwicklung des Rechtsrahmens nach dem Beschluss über die Sorgfaltspflichten im Jahre 2009

a) Empfehlungen für Sicherheit bei Internetzahlungen von Seiten der Europäischen Zentralbank und der für Zahlungsdienstleister relevanten Aufsichtsbehörden

80. Eine gemeinsame Arbeitsgruppe der europäischen Notenbanken und Bankenaufsichtsbehörden (European Forum on the Security of Retail Payments, kurz SecuRe Pay Forum) hat im Jahr 2013 Empfehlungen für die Sicherheit bei Internet-Bezahlverfahren veröffentlicht. Die Empfehlungen des SecuRe Pay Forums verfolgen das Ziel, ein harmonisiertes europaweites Sicherheitsniveau für Internet-Zahlungen zu fördern. Sie richten sich an Zahlungsdienstleister im Sinne der Zahlungsdiensterichtlinie.[67] Zahlungsauslösedienste gehören derzeit nicht zum Adressatenkreis der Empfehlung.

81. Die Empfehlungen basieren auf vier Prinzipien:

- Zum einen sollen Zahlungsdienstleister und Zahlungssysteme regelmäßig die Risiken überprüfen, die mit Internet-Zahlungen verbunden sind, und dabei aktuelle Sicherheitsbedrohungen und Betrugsmechanismen im Internet berücksichtigen.

- Zweitens sollen das Auslösen von Internet-Zahlungen und der Zugriff auf sensible Zahlungsdaten – gemeint sind solche Daten, die für Betrugszwecke missbraucht werden können – durch eine starke Authentifizierung der Kunden geschützt werden.

- Das dritte Prinzip stellt auf die Effektivität der von Zahlungsdienstleistern etablierten Prozesse zur Autorisierung von Transaktionen und zur Überwachung von Transaktionen und Systemen ab. Hierdurch sollen ungewöhnliche Zahlungsmuster erkannt und Betrug wirkungsvoll entgegengewirkt werden.

- Schließlich sollen Zahlungsdienstleister – als viertes Prinzip – Kunden für eine sichere und effiziente Nutzung der Dienste zur Durchführung von Internet-Zahlungen sensibilisieren und schulen.

82. Ausgehend von den Empfehlungen hat die Europäischen Bankenaufsichtsbehörde (EBA) 2014 nahezu wortgleiche Empfehlungen in ihren Leitlinien zur Sicherheit von Internetzahlungen übernommen. Den Text der EBA-Leitlinien in der deutschen

---

[67] Die Empfehlungen entfalten daher derzeit keine unmittelbare Wirkung für die Tätigkeit von Zahlungsauslösediensten, da diese keine Zahlungsdienstleister im Sinne der geltenden Zahlungsdiensterichtlinie sind.

Übersetzung hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Mai 2015 als Rundschreiben mit Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi) in die eigene Verwaltungspraxis umgesetzt, um zum Schutz vor Cyber-Kriminalität beizutragen.[68]

b) Novellierung der Zahlungsdiensterichtlinie 2015

83. Im Jahr 2015 wurde die Zahlungsdiensterichtlinie PSD novelliert. Mit Inkrafttreten der (neuen) PSD2 wurde die Definition, welche Arten von Zahlungsdiensten von der Richtlinie erfasst und der Aufsicht unterstellt werden sollen, erweitert. Sie gilt nunmehr auch für Zahlungsauslösedienste und Kontoinformationsdienste (vgl. Rn. 46).

84. Als Zahlungsauslösedienst definiert die PSD2 Zahlungsdienste, die auf Antrage eines Zahlungsdienstenutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslösen (Art. 4 Nr. 15 PSD2). Die Zustimmung zu Zahlungsvorgängen wird in der zwischen Zahler und Zahlungsdienstleister (Kunde und Bank) vereinbarten Form erteilt (Art. 64 Abs. 2 PSD2). Art. 66 PSD2 konkretisiert den Zugang zum Konto im Fall der Einschaltung von Zahlungsauslösediensten. Nutzt der Zahler einen Zahlungsauslösedienst und erteilt über diesen seine ausdrückliche Zustimmung zur Ausführung einer Zahlung entsprechend Art. 64 PSD2, muss der kontoführende Zahlungsdienstleister Handlungen vornehmen, um die Nutzung von Zahlungsauslösediensten durch den Zahler zu gewährleisten (Art. 66 Abs. 2 PSD2). Konkrete Pflichten des kontoführenden Zahlungsdienstleisters werden in Art. 66 Abs. 4 PSD2 festgelegt. Hiernach muss der kontoführende Zahlungsdienstleister auf sichere Weise mit dem Zahlungsauslösedienst kommunizieren sowie unmittelbar nach Eingang des Zahlungsauftrags von einem Zahlungsauslösedienst diesem alle Informationen über die Auslösung des Zahlungsvorgangs und alle ihm zugänglichen Informationen hinsichtlich der Ausführung des Zahlungsvorgangs mitteilen oder zugänglich machen. Der kontoführende Zahlungsdienstleister muss Zahlungsaufträge, die über einen Zahlungsauslösedienst übermittelt werden, in Bezug auf die zeitliche Abwicklung, Prioritäten oder Entgelte in der gleichen Weise behandeln wie direkt übermittelte Aufträge, es sei denn, es liegen objektive Gründe für eine Andersbehandlung vor.

---

[68] Zahlungen im Internet – Neues Rundschreiben: Mindestanforderungen an die Sicherheit, BaFin Journal, Mai 2015, S. 12.

85. Das Erbringen von Zahlungsauslösediensten ist nicht vom Bestehen einer vertraglichen Beziehung zwischen dem Zahlungsauslösedienstleister und dem kontoführenden Dienstleister abhängig (Art. 66 Abs. 5 PSD2).

86. Nach europäischem Recht haben Kunden nach Inkrafttreten der im Jahre 2015 überarbeiteten PSD2 damit das Recht, bestehende Zahlungsauslösedienste zu nutzen und hierdurch Zahlungsaufträge auf die von der Bank vorgesehene Art und Weise zu erteilen. Banken als kontoführende Dienstleister haben die Pflicht, ohne das Bestehen einer vertraglichen Grundlage Aufträge, die über Zahlungsauslösedienste eingereicht werden, auszuführen und Zahlungsauslösediensten alle notwendigen Informationen zur Verfügung zu stellen. Zahlungsauslösedienste dürfen entsprechend der PSD2 von Kunden PIN und TAN entgegennehmen und sind nicht als Dritte zu behandeln, gegenüber denen diese Personalisierten Sicherheitsmerkmale geheim zu halten sind.

87. Erst mit der Novellierung der PSD2 wurde somit der Rechtsrahmen geschaffen, in dem Zahlungsauslösedienste als Zahlungsdienste (Art. 4 Nr. 3 iVm Anhang I PSD2) eine Zulassung für eine unionsweite Tätigkeit benötigen und erhalten sowie einer permanenten Aufsicht durch staatliche Stellen unterliegen (Artikel 11 Abs. 1, Artikel 1 (d) PSD2).

88. Das Angebot der Sofort fällt in den Anwendungsbereich der PSD2. Die Regelungen zur Rollenverteilung zwischen Zahlungsauslösedienst, Zahler und kontoführendem Zahlungsdienstleister entsprechen denen zwischen Sofort, Zahler und kontoführender Bank. Die PSD2 legt für diese Art der Dienstleistungen Rechte und Pflichten der beteiligten Unternehmen fest und verpflichtet die Mitgliedstaaten, bei der Umsetzung der Richtlinie in nationales Recht sicherzustellen, dass Zahler das Recht haben, einen Zahlungsauslöse- bzw. Kontoinformationsdienst zu nutzen, sofern das entsprechende Konto online geführt wird.

89. Für die Kommunikation zwischen Zahlungsauslösedienstleister und kontoführendem Zahlungsdienstleister (Art. 66 Abs. 4 lit. a) PSD2) werden entsprechend Art. 98 Abs. 1 lit. d) PSD2 von dafür zuständigen öffentlichen Stellen technische Regulierungsstandards ausgearbeitet, die Anforderungen an gemeinsame und sichere offene Standards für die Kommunikation zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern zum Zwecke der Identifizierung, der Authentifizierung, der Meldung und der Weitergabe von Informationen sowie der Anwendung von Sicherheitsmaßnahmen konkretisieren. Neben z.B. der Gewährleistung eines angemessenen Sicherheitsniveaus für Zahlungsdienstleister sollen sich diese Regulierungsstandards auch auf eine Sicherstellung und Aufrechterhaltung

eines fairen Wettbewerbs zwischen allen Zahlungsdienstleistern richten und dabei die Neutralität im Hinblick auf Technologie und Geschäftsmodell gewärleisten (Art. 98 Abs. 2 lit. c) und d) PSD2).

90. Eines der Ziele der PSD2 ist es, die Kontinuität im Markt bis zur Umsetzung der Richtlinie in nationales Recht sicherzustellen und gleichzeitig bestehenden Dienstleistern unabhängig von ihrem Geschäftsmodell die Möglichkeit zu geben, ihre Dienste zu einem klaren und harmonisierten Rechtsrahmen anzubieten (siehe Erwägungsgrund 33 PSD2[69]). Soweit die PSD2 also festlegt, in welcher Form und unter welchen Bedingungen Zahlungsauslösedienste zukünftig genutzt werden dürfen, stehen Regelungen dazu, welche Pflichten Zahlungsdienstenutzern in Bezug auf Zahlungsinstrumente und personalisierte Sicherheitsmerkmale nach Art. 69 PSD2 obliegen, nicht im Widerspruch zur Sicherung des Fortbestehens von Zahlungsauslösediensten bis zur Erarbeitung von Regulierungsstandards und zur Umsetzung der Regelungen in nationales Recht. Soweit der Zahlungsdienstenutzer verpflichtet ist, die Bedingungen für die Ausgabe und Nutzung eines Zahlungsinstrumentes einzuhalten, muss er unmittelbar nach dessen Erhalt alle zumutbaren Vorkehrungen treffen, um seine Personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

91. Wegen der erklärten Zielsetzung der PSD2 in Erwägungsgrund 33, bestehende Geschäftsmodelle von Zahlungsauslösediensten zu erhalten, zielen die Regelungen in Art. 69 PSD2 gerade nicht darauf ab, die Weitergabe von Personalisierten Sicherheitsmerkmalen an Zahlungsauslösedienste grundsätzlich zu verbieten. Denn dies würde zu einer Diskriminierung der bestehenden Anbieter am Markt führen, welche der europäische Gesetzgeber durch die Übergangsregelungen zur Erhaltung des Wettbewerbs am Markt explizit verhindern will.

---

[69] Erwägungsgrund 33 der PSD2 lautet: „Diese Richtlinie sollte darauf abzielen, die Kontinuität im Markt sicherzustellen und gleichzeitig bestehenden und neuen Dienstleistern unabhängig von ihrem Geschäftsmodell die Möglichkeit zu geben, ihre Dienste in einem klaren und harmonisierten Rechtsrahmen anzubieten. Unbeschadet der Notwendigkeit, die Sicherheit von Zahlungsvorgängen und den Schutz der Verbraucher vor nachweislichen Betrugsrisiken zu gewährleisten, sollten die Mitgliedstaaten, die Kommission, die Europäische Zentralbank (EZB) und die Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA), errichtet mit der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates Vorschriften) (1) bis zur Anwendung dieser Vorschriften den fairen Wettbewerb in diesem Markt sicherstellen und dabei eine ungerechtfertigte Diskriminierung der vorhandenen Marktteilnehmer vermeiden. Jeder Zahlungsdienstleister, auch der kontoführende Zahlungsdienstleister des Zahlungsdienstnutzers, sollte Zahlungsauslösungsdienste anbieten können."

92. Die EBA wird bis zum 13.01.2017 in Zusammenarbeit mit der Europäischen Zentralbank technische Regulierungsstandards für Zahlungsdienstleister im Sinne der PSD2 erarbeiten und an die Europäische Kommission übermitteln, welche diese erlassen wird. Hierin werden unter anderem die Anforderungen an Verfahren zur starken Kundenauthentifizierung eines Zahlungsdienstleister präzisiert sowie die Anforderungen an Sicherungsvorkehrungen zum Schutz von Personalisierten Sicherungsmerkmalen der Zahlungsdienstleister, wenn Zahlungen z.B. über Zahlungsauslösedienste ausgelöst werden (Art. 98 Abs. 1 lit. c) i.V.m. Artikel 97 Abs. 2 und 3 PSD2). Die technischen Regulierungsstandards werden Anforderungen an die Sicherheit offener Standards für die Kommunikation präzisieren. Damit wird sich der technische Regulierungsstandard auf alle an einem durch Zahlungsauslösedienste ausgelösten Bezahlvorgang beteiligten Parteien beziehen. Die EBA wird die Erarbeitung der technischen Standards an der Zielsetzung von Artikel 98 Abs. 2 PSD2 ausrichten und neben der Sicherstellung eines angemessenen Sicherheitsniveaus auch auf die Aufrechterhaltung eines fairen Wettbewerbs zwischen Zahlungsdienstleistern (Artikel 98 Abs. 2 lit c) PSD2), auf die Gewährleistung der Neutralität der Standards im Hinblick auf Technologien und Geschäftsmodelle (Artikel 98 Abs. 2 lit d) PSD2) und auf die Ermöglichung der Entwicklung benutzerfreundlicher, allgemein zugänglicher und innovativer Zahlungsmittel (Artikel 98 Abs. 2 lit e) PSD2) abzielen.

4. Organisation des Online-Bankings durch die Deutsche Kreditwirtschaft

Die DK übernimmt für die angeschlossenen Kreditinstitute zentrale Aufgaben zur Organisation und Schaffung eines einheitlichen und sicheren Rahmens zur Durchführung des Zahlungsverkehrs. Dabei gestalten die Verbände in der DK gemeinsam Zahlungssysteme und vereinbaren hierfür Standards sowie Verfahren zur Einhaltung solcher Standards durch Zertifizierung von technischen Produkten (vgl. nachfolgend unter a)). Auch im Rahmen des Online-Bankings erarbeiten die in der DK organisierten Verbände branchenweite Sicherheitsstandards und stellen einheitliche Schnittstellen zur Kommunikation mit anderen Marktteilnehmern zur Verfügung (vgl. dazu nachfolgend unter b)). Daneben trägt die Tätigkeit der Rechenzentren der Sparkassen und Genossenschaftsbanken zur Vereinheitlichung der technischen Umsetzung des Online-Bankings bei (vgl. dazu nachfolgend unter c)). Der DK kommt damit eine zentrale organisatorische Rolle bei dem Betrieb des Online-Bankings zu.

a) Aufgabenwahrnehmung durch die DK bei bankfachlichen und –technischen Themen im Rahmen des Zahlungsverkehrs

93. Die Spitzenverbände der Kreditwirtschaft arbeiten in der DK zusammen und verantworten eine Vielzahl von Aufgaben mit grundsätzlichem Charakter, die für die gesamte Kreditwirtschaft wahrgenommen werden.

94. Die DK stellt sich selbst als Interessenvertretung zur gemeinsamen Meinungs- und Willensbildung in bankfachlichen, bankpolitischen und bankpraktischen Fragen dar, wobei sie Schwerpunkte ihrer Tätigkeit in den Bereichen Aufsichts-, Wertpapier- und Steuerrecht sieht. Nach eigener Darstellung liegt ein weiterer Schwerpunkt ihrer Tätigkeit in der Erarbeitung „standardisierter Regelungen im Zahlungsverkehr einschließlich der Kartenzahlungssysteme“.[70]

95. Der Aufgabenwahrnehmung der DK im Bereich des Zahlungsverkehrs kommt eine zentrale Rolle für die angeschlossenen Kreditinstitute zu. Die DK übernimmt in diesem Zusammenhang nicht ausschließlich klassische Aufgaben einer Interessenvertretung, sondern agiert als zentrale Koordinierungsinstanz in Fragen, die alle angeschlossenen Kreditinstitute betreffen und für die Entwicklung gemeinsamer Projekte von zentraler Bedeutung sind. Hierbei handelt es sich häufig um Projekte, die einheitliche technische Lösungen für die große Zahl in Deutschland tätiger Kreditinstitute erforderlich machen [redacted] Im Bereich des Zahlungsverkehrs verfügt die DK über umfangreiche Erfahrungen bei der Koordinierung gemeinsamer Projekte. Hierzu gehören bspw. ein System zum bargeldlosen Bezahlen (Debitkartensystem)[71] und ein Zahlungssystem zur

---

[70] http://www.die-deutsche-kreditwirtschaft.de/dk/die-deutsche-kreditwirtschaft.html, Stand 16.072014.

[71] Gemeinsam verantworten die in der DK organisierten Spitzenverbände der Kreditwirtschaft die bundesweite Einführung des electronic cash-Verfahrens. Vertragliche Grundlage des electronic cash-Verfahrens ist die „Vereinbarung über ein institutsübergreifendes System zur bargeldlosen Zahlung an automatisierten Kassen (electronic cash-System)“.

Bargeldbeschaffung an Geldautomaten.[72] Für die Zulassung von Dienstleistern und Produkten betreibt die DK ein zentrales Zulassungsbüro.[73]

b) Aufgabenwahrnehmung der DK im Rahmen der Organisation des Online-Bankings

96. Die DK übernimmt im Rahmen des Online-Bankings grundlegende Aufgaben zur Realisierung der technischen Umsetzbarkeit und der Sicherheit des Systems für die angeschlossenen Mitgliedsinstitute. Die von der DK erarbeitete technische Schnittstelle zur Kommunikation zwischen Bankkunden und Kreditinstitut über Finanzverwaltungssoftware und andere Produkte wird von nahezu allen deutschen Kreditinstituten eingesetzt. Auch die (Fort-)Entwicklung von Sicherungsverfahren bei der Nutzung des Online-Bankings stellt die Erarbeitung eines branchenweit geltenden Standards durch die DK dar. Die Erarbeitung gemeinsamer Geschäftsbedingungen für die angeschlossenen Spitzenverbände stellt eine Aufgabe dar, welche die DK seit mehreren Jahrzehnten gemeinsam umsetzt.

aa) Schnittstellendefinition

97. Um den Bankkunden die Nutzung des Online-Bankings auch nach Erweiterung des von der Deutschen Bundespost in den 90er Jahren angebotenen Bildschirmtext (Btx) mit eigenen Anwendungen im Zuge des Ausbaus des Internets (z.B. durch Internet-Browser

---

[72] Die DK betreibt ein weiteres Zahlungssystem zur Bargeldbeschaffung an Geldautomaten. Dazu hat die DK die Vereinbarung über das deutsche Geldautomatensystem geschlossen, auf deren Grundlage alle in Deutschland betriebenen Geldautomaten zur gegenseitigen Nutzung in ein gemeinsames System einbezogen werden. Auch für dieses System hat die DK zudem eine Reihe vertraglicher Vereinbarungen zur Ausweitung der Nutzungsmöglichkeiten an den von deutschen Kreditinstituten betriebenen Geldautomaten geschlossen. Das deutsche Geldautomatensystem ist z.B. Bestandteil des weltweiten Maestro- und Cirrus-Geldautomatensystems der Master Card Worldwide, wodurch die Debit- und Kreditkarten mit diesem Logo weltweit an Geldautomaten genutzt werden können. (Vereinbarung über das „Deutsche Geldautomaten-System“ vom 15.01.2011, Nr. 1 c), in: Zahlungsverkehr, Richtlinie, Abkommen, Bedingungen, hrsg. vom Bundesverband deutscher Banken e.V., Berlin).

[73] Die DK erteilt durch das vom VÖB betriebene zentrale Zulassungsbüro die Zulassungen für Geldautomaten für den Betrieb im Deutschen Geldautomatensystem. Zum Zwecke der Kommunikation zwischen den am Geldautomaten-System Beteiligten hat die DK in den Technischen Anlagen und Anhängen zum Regelwerk über das Deutsche Geldautomaten-System eine einheitliche Schnittstelle definiert. Zum Nachweis der Einhaltung dieser Anforderungen führt der VÖB für die DK ein Zulassungsverfahren durch. Dies beinhaltet einen Konformitätsnachweis, der mit einem Funktionstest sowie einer Sicherheitsevaluierung verbunden ist. Erst nach Durchlaufen der Typen-Zulassung dürfen Geldautomaten im Deutschen Geldautomaten-System betrieben werden. Dabei umfasst die Zulassung zusätzlich auch die Anforderungen der internationalen Kartensysteme wie z.B. MasterCard und JCB für den Einsatz an Geldautomaten in Deutschland, wodurch eine gesonderte Zulassung der Geräte nicht erforderlich ist. (http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/geldautomaten.html, Stand 21.07.2014.

und Finanzverwaltungssoftware) zu ermöglichen, hat die DK Mitte der 90er Jahre eine Schnittstelle unter der Bezeichnung **H**ome**b**anking **C**ommon **I**nterface (HBCI) entwickelt.[74]

98. Für die Einführung und branchenweite Nutzung von HBCI zur Abwicklung von Bankgeschäften im Wege des elektronischen Dialogs (Homebanking) mit allen Kreditinstituten hat die DK das Homebanking-Abkommen geschlossen. Die Spitzenverbände der DK als Vertragspartner stellen dadurch sicher, dass dieses von jedem Kreditinstitut anerkannt wird, welches seinen Kunden den Datenaustausch im Rahmen des Homebankings ermöglicht. Erklärtes Ziel des Abkommens war es, die Schnittstellenspezifikationen um weitere Geschäftsvorfälle zu ergänzen. Zu diesem Zweck war auch die Bildung eines Arbeitskreises in der DK vorgesehen, der für alle Fragen zuständig ist, die im Zusammenhang mit dem Abkommen auftreten.[75]

99. HBCI wurde 2002 weiterentwickelt und durch den **Fin**ancial **T**ransaction **S**ervices-Standard (FinTS) ersetzt. FinTS stellt auch gegenwärtig die zentrale multibankenfähige Schnittstelle dar, die von Nutzern und bei Angeboten Dritter Dienstleister für die Kommunikation im Rahmen des Online-Bankings genutzt wird.[76]

100. Mit FinTS hat die DK einen branchenweiten Schnittstellenstandard weiterentwickelt, der von mehr als 2000 Kreditinstituten unterstützt wird und den Hersteller von Online-Banking-Softwareprodukten nutzen, mit der Folge, dass Kunden eine Vielzahl von Produkten zur Anwendung zur Verfügung steht.[77] Erst die Erarbeitung dieses einheitlichen Standards ermöglichte die Erstellung branchenweiter Lösungen durch eine Vielzahl von privatwirtschaftlichen Angeboten. Die DK weitet mit FinTS die Kommunikation, die sich im Rahmen der HBCI-Schnittstelle lediglich auf die Kommunikation des Kunden mit seinem Kreditinstitute bezog, auch auf Fälle aus, in denen Kunden sich sogenannter Intermediäre

---

[74] Die Entwicklung von HBCI sollte eine sichere und leistungsfähige Kommunikationsschnittstelle zum Online-Banking der Kreditinstitute anbieten. Die DK verfolgte das Ziel, Online-Banking mit Sicherheitsfunktionen auszustatten, die das Angebot auch in ungesicherten Netzen ermöglicht. Zentraler Ansatz war es dabei, einen einheitlichen branchenweiten Standard zu erstellen, um Kontoverbindungen mit identischen Mechanismen verwalten zu können und dabei unabhängig von den verwendeten Endgeräten zu sein. Durch den einheitlichen Standard wurde der damals übliche Umfang des Online-Bankings (Erteilung von Überweisungsaufträgen und Abruf von Kontoinformationen) mit dem Ziel ausgeweitet, die Attraktivität des Online-Bankings zu steigern. Die Online-Banking-Kunden konnten so bei allen Banken gleiche Funktionalitäten unabhängig von den eingesetzten Endgeräten nutzen. Für die Kreditinstitute führte der einheitliche Standard zu einer Vereinfachung bei der Erstellung von Anwendungen und der Wartung der Systeme. Auch die Vorteile für die Hersteller hatte die DK bei der Erarbeitung von HBCI im Blick, um Planungssicherheit bei der Gestaltung kundenfreundlicher Homebanking-Programme zu erreichen;http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf. S. 2f.

[75] http://www.hbci-zka.de/dokumente/diverse/hb-abkom.pdf, Stand 30.07.2014.

[76] B4-71/10, Bl. 1677.

[77] www.hbci-zka.de, Stand 23.02.2011.

bedienen. Angelegt ist der FinTS-Standard auch für Fälle, in denen Intermediäre Auftragsdaten des Kunden inklusive PIN und TAN im Rahmen einer FinTS-Nachricht an das kontoführende Kreditinstitut weiterleiten.[78]

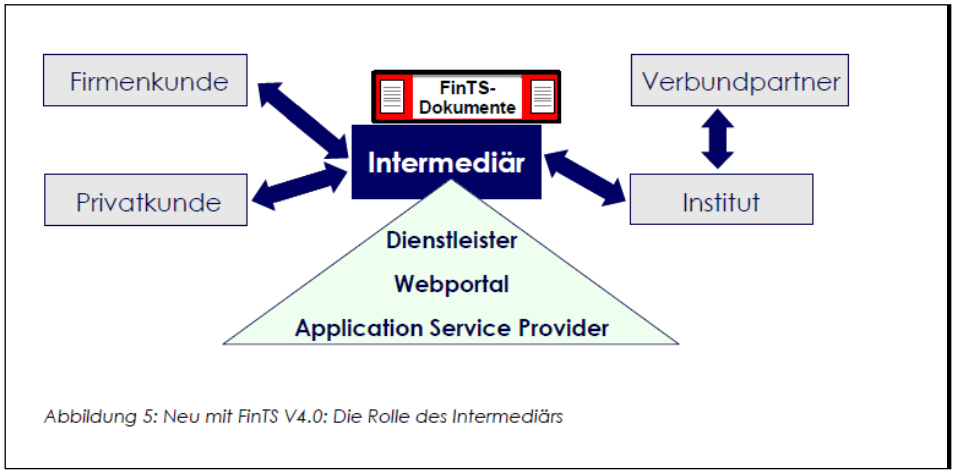


Abb. 4:, FinTS V4.0 Kompendium, S. 15, Die Rolle des Intermediärs.

bb) Definition von Sicherheitsstandards

101. Die DK hat im Bereich der Sicherheitsstandards maßgeblich dazu beigetragen, Online-Banking fortzuentwickeln, indem beispielsweise gemeinschaftlich neue Verfahren zur TAN-Übermittlung erarbeitet wurden.

102. In der DK wurden Standards für das SMS-TAN-Verfahren (vgl. Rz. 56) von den Spitzenverbänden gemeinsam entwickelt.[79] Für die Nutzung des mobile-TAN-Verfahrens hat die DK gemeinsame Mindestsicherheitsanforderungen formuliert und auf ihrer Internetseite veröffentlicht.[80] Damit hat die DK auf die Anfälligkeit anderer TAN-Verfahren für Missbrauch reagiert, damit Kreditinstitute ihren Kunden weiterhin sichere Verfahren im Rahmen der Nutzung des Online-Bankings anbieten können. Dass den in der DK

---

78 FinTS V4.0 Kompendium, Financial Transaction Services, Der Einstieg in die neue Welt des Online-Banking, http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf, 20.09.2015, S. 16.

79 Pressemitteilung der DK, Auch mit mobiler TAN beim Online Banking sorgfältig umgehen – Deutsche Kreditwirtschaft gibt Sicherheitstipps, 28.04.2011, http://www.die-deutsche-kreditwirtschaft.de/dk/pressemitteilungen/volltext/backpid/29/article/zka-auch-mit-mobiler-tan-beim-online-banking-sorgfaeltig-umgehen-deutsche-kreditwirtschaft-gibt-si.html?tx_ttnews[pS]=1293836400&tx_ttnews[pL]=31535999&tx_ttnews[arc]=1&cHash=a1748c4d51ec60e780c4e2582aecd9b5, Stand 25.06.2015.

80 http://www.die-deutsche-kreditwirtschaft.de/uploads/media/Mindestsicherheitsanforderungen_mobileTAN_V1_20110621.pdf, Stand 25.06.2015.

zusammenarbeitenden Verbänden eine zentrale organisatorische Rolle beim Betrieb des Online-Bankings und der Festlegung der Nutzungsbedingungen zukommt, zeigt sich auch daran, dass sie auf ihrer Internetseite explizit darauf hinweisen, dass die Nutzung des SMS-TAN-Verfahrens z.B. über nur ein Endgerät für beide Kommunikationsstrecken nicht zulässig ist und daher in den Kundenbedingungen für das Online-Banking explizit ausgeschlossen wird.[81]

cc) Erarbeitung gemeinsamer Geschäftsbedingungen

103. Die Spitzenverbände der Kreditwirtschaft erarbeiten gemeinsam für die angeschlossenen Kreditinstitute AGB-Regelwerke.

104. Die DK erstellt seit Einführung des Online-Bankings zunächst für die von der Deutschen Post angebotenen Btx-Dienste und später auch für die hinzukommenden Angebote über Internet und Softwareprodukte einheitliche, von den Kreditinstituten übernommene Kundenbedingungen.

105. Die Überarbeitung der aus dem Jahre 1984 stammenden (Sonder-) Bedingungen für die Benutzung von Bildschirmtext[82] im Jahre 2000 hat die DK gemeinsam durchgeführt und ihren angeschlossenen Kreditinstituten zur Nutzung empfohlen. Die „Bedingungen für die konto- und depotbezogene Nutzung des Online-Bankings mit PIN und TAN“ wurden am 03.03.2000 beim Bundeskartellamt als gemeinsames Vertragswerk der Kreditwirtschaft zur Freistellung angemeldet und am 06.06.2000 vom Kartellverbot freigestellt.[83] Die DK begründete die zentrale Überarbeitung mit der Angleichung an Vorgaben vergleichbarer Bedingungswerke und führte in diesem Zusammenhang exemplarisch die „Bedingungen für ec-Karten“ auf, die von allen deutschen Kreditinstituten an ihre Kunden zur Nutzung von Kontodienstleistungen sowie zur Durchführung von Bezahlvorgängen an ihre Kunden ausgegeben werden. [84]

c) Aufgabenwahrnehmung durch Rechenzentren und Kreditinstitute

106. Neben den Spitzenverbänden, die in der DK eine Reihe zentraler Aufgaben für die Gesamtheit der im Bereich Retailbanking tätigen Kreditinstituten übernehmen, kommen

---

81 http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/electronic-banking/mobiletan.html, Stand 30.07.2014.

82 Schreiben der DK vom 02.11.2010, Anlage 1.

83 B4-167/04.

84 Außerdem werden Empfehlungen der Europäischen Kommission vom 30.07.1997 zu elektronischen Zahlungsinstrumenten sowie Neuerungen der Verfahrensabläufe und schließlich die Verbesserung der Transparenz durch übersichtliche Gestaltung und sprachliche Überarbeitung als wesentliche Gründe für die gemeinsame Überarbeitung genannt.

auch den Rechenzentren der Sparkassen und Genossenschaftsbanken zentrale Aufgaben zu, welche die angeschlossenen Institute dieser Bankengruppen aufgrund ihrer Größe und ihrer Ressourcen nicht eigenständig erbringen. Hierzu gehört insbesondere der Betrieb eines Kernbanksystems[85], aber auch die Entwicklung und technische Realisierung neuer Anwendungen wie Software-Applikationen für die Nutzung im Zusammenhang mit dem Online-Banking. [86]

107. In der Sparkassenorganisation betreibt die FI Rechenzentren und Systeme, welche von den in Deutschland tätigen Sparkassen in Anspruch genommen werden. Im Bereich des Genossenschaftssektors ist die Fiducia&GAD als Dienstleister für die angeschlossenen Kreditinstitute tätig.

108. FI und Fiducia&GAD betreiben auch Kernbanksysteme für die ihnen angeschlossenen Kreditinstitute und bieten in diesem Zusammenhang bankfachliche Anwendungen an, die für die technische Umsetzung des Online-Bankings und damit für die Abwicklung des Kundengeschäfts eines Kreditinstituts zwingend erforderlich sind. [redacted] [87]

109. FI betreibt ein Kernbanksystem unter der Bezeichnung „One System Plus“ (OS Plus), Fiducia&GAD betreibt derzeit zwei Kernbanksysteme unter der Bezeichnung „agree“ und „Bank21“[88]. Diese Kernbanksysteme werden im Zusammenhang mit der Inanspruchnahme der jeweiligen Rechenzentrumsdienstleistungen angeboten.

---

[85] Der Begriff des Kernbanksystems, der in verschiedenen Fusionskontrollverfahren vor dem Bundeskartellamt von den Beteiligten verwendet wurde, bei dem es sich allerdings nicht um einen feststehenden Begriff handelt, wird im Folgenden als Gesamtheit der Anwendungen für Retailbanken verstanden, die es den Instituten erlauben, Geschäftsvorfälle in der Datenverarbeitung elektronisch abzubilden und umzusetzen. Je nach Bedarf der angeschlossenen Kreditinstitute kann der Umfang der angebotenen Dienstleistungen variieren.

[86] Auch wenn die Situation für einige der Mitgliedsinstitute des BdB aufgrund ihrer Größe anders zu beurteilen ist, da Unternehmen wie [redacted] u.a. viele Leistungen selbständig realisieren, nehmen einige kleinere Kreditinstitute dieser Bankengruppe ebenfalls Leistungen der genossenschaftlichen Rechenzentren in Anspruch.

[87] [redacted]

[88] Die Fiducia&GAD ist aus einem Zusammenschluss zweier genossenschaftlicher Rechenzentren Fiducia IT AG, Karlsruhe, und GAD eG, Münster, hervorgegangen, die unterschiedliche Kernbankanwendungen unter den Marken „agree“ und „Bank 21“ betrieben haben. Zukünftig sollen die beiden Kernbanksystem der zusammengeschlossenen Fiducia&GAD von dem Produkt „agree 21“ abgelöst werden (https://www.fiduciagad.de/ueber-uns.html).

110. Bei den beiden Dienstleistern werden eine Reihe von Angeboten von allen angeschlossenen Kreditinstituten in Anspruch genommen. Die FI stellt mehr als [redacted] ihres gesamten Dienstleistungsportfolios allen Sparkassen zur Verfügung. Auch der Online-Banking-Auftritt der Sparkassen im Bereich des Online-Bankings wird durch eine Anwendung umgesetzt, die von allen Sparkassen genutzt wird. Gleiches gilt für Fiducia&GAD, die für die genossenschaftliche Bankengruppe vollständig die technische Realisation des Online-Bankings übernimmt.

5. Fortentwicklung des Online-Bankings durch zusätzliche Nutzungsmöglichkeiten

111. Das Online-Banking stellt ein Angebot der Kreditwirtschaft mit einer hohen Entwicklungsdynamik dar, die sich aus technischen Innovationen ergibt, die sowohl die genutzte Hardware als auch die Applikationen betreffen. Über die ursprünglichen Nutzungsmöglichkeiten des Online-Bankings auf den Internetseiten des kontoführenden Kreditinstituts hinaus wurden in den vergangenen Jahren weitere Angebote etabliert, die Kunden im Rahmen des Online-Banking-Angebots nutzen können. Vielfach werden diese Angebote auf mobilen Endgeräten (z.B. Smartphones) betrieben. Neben den Produkten, die von Bankenseite bereitgestellt und vertrieben werden, handelt es sich dabei auch um Produkte bankenunabhängiger Anbieter. Den Zugang zum Online-Banking realisieren diese Produkte in der Regel über die gemeinsame FinTS-Schnittstelle der DK sowie die Eingabe der Personalisierten Sicherheitsmerkmale. Soweit diese Produkte Angaben wie PIN und TAN abfragen und verarbeiten, sind hierfür verschiedene Vorgehensweisen möglich. Dies kann auf der durch den Kunden genutzten Hardware oder auch auf der Infrastruktur des Anbieters einer Applikation erfolgen. Zahlungsauslösedienste stellen den Zugang zum Online-Banking demgegenüber über die Online-Banking-Internetseite des Kreditinstituts her, die der Kunde auch für den eigenen Kontozugang nutzt.

a) Beispiele für Angebote der Sparkassengruppe

112. Die Star Finanz GmbH („StarFinanz“), ein Tochterunternehmen der Finanzinformatik (FI), entwickelt und vertreibt verschiedene Softwareprodukte unter der Bezeichnung Starmoney zum persönlichen Finanzmanagement der Kunden. Die Software wird in einer auf dem Endgerät des Kunden zu speichernden Version (Starmoney) und in einer Online-Version (Starmoney.web) vermarktet. Im Rahmen der Nutzung dieser Produkte, die multibankenfähig sind und für Konten aller Banken in Deutschland genutzt werden können, muss der Kunde auch seine Personalisierten Sicherheitsmerkmale eingeben.

aa) Starmoney

113. Bei Starmoney handelt es sich um eine Software, die vom Kunden auf seinem Endgerät installiert wird. Sie bietet die Möglichkeit, verschiedene Konten zu verwalten und aktiv zu führen. Der Kunden erhält die Möglichkeit, offline- und online-geführte Konten zu verwalten. Während bei offline-geführten Konten die Eingabe der Buchungen und Einträge durch den Kunden selbst erfolgt, werden bei online-geführten Konten die Informationen aus den Systemen der kontoführenden Unternehmen ausgelesen. Es handelt sich dabei nicht ausschließlich um Konten der DK-Mitgliedsinstitute, sondern auch um Konten bei Unternehmen wie Ebay und PayPal. Den Zugang zu den Konten der Kreditinstitute stellt Starmoney über die von der Kreditwirtschaft bereitgestellte FinTS-Schnittstelle her, die ihrerseits den Zugang zu dem Rechenzentrum des kontoführenden Kreditinstituts ermöglicht. Über die jeweiligen Schnittstellen ruft Starmoney die Kontodaten über das Internet ab. Anschließend können die Daten auf dem Gerät des Kunden ausgewertet werden. Neben dem Abruf der Kontodaten ermöglicht Starmoney ebenfalls die Erteilung von Zahlungsverkehrsaufträgen (z.B. Überweisungen).[89]

114. Um den Zugang zu den Konten zu erlangen und die Daten übertragen bzw. die Aufträge erteilen zu können, ist es erforderlich, dass der Kunde seine Legitimationsdaten über das System eingibt. Es handelt sich dabei um die Daten, die auch bei dem Direktzugriff auf das Konto im Internetbrowser eingegeben werden müssen (Kontonummer, PIN und eventuell weitere Zugangsinformationen). Bei der Erteilung von Aufträgen an das kontoführende Kreditinstitut gibt der Kunde über die Software Starmoney auch die entsprechenden Autorisierungsinformationen – in der Regel handelt es sich um eine TAN - ein, welche ihm durch das kontoführende Kreditinstitut zur Verfügung gestellt werden. Die Kommunikation erfolgt verschlüsselt, ohne Einschaltung einer dritten Partei, zwischen dem Rechner des Nutzers und dem kontoführenden Kreditinstitut, ohne dass Star Finanz über die Software eine Zugriffsmöglichkeit oder Kenntnis von den Personalisierten Sicherheitsmerkmalen des Kontoinhabers erhält.

115. Die Star Finanz hat zur Sicherung der Software eine Reihe zusätzlicher Maßnahmen und Mechanismen entwickelt, um Missbrauch der Personalisierten Sicherheitsmerkmale zur Identifizierung und Autorisierung im Online-Banking zu verhindern. Neben anderen gehört hierzu die eigenständige Entwicklung aller Komponenten, mit denen Starmoney mit den

---

[89] Produktbeschreibung unter www.starmoney.de.

Schnittstellen der Rechenzentren der kontoführenden Kreditinstitute kommuniziert (sog. Kernel, vgl. dazu auch Ausführungen zu den Angeboten der DATEV unter Rz. 166).

bb) Starmoney Web

116. Star Finanz bietet Starmoney auch als browsergestütztes Programm in einer kostenfreien Basisversion sowie einer kostenpflichtigen Vollversion unter der Bezeichnung Starmoney Web an. Die Nutzung beider Versionen setzt die Registrierung des Nutzers über ein von der Star Finanz betriebenes Internetportal voraus. Die Software, die ausschließlich über eine Applikation im Internet erreichbar ist, ermöglicht die Kontoverwaltung, d.h. den Abruf von Kontodaten sowie deren Auswertung. Gleichzeitig ist auch die Erteilung von Zahlungsverkehrsaufträgen über die Software möglich.

117. Starmoney Web wird nicht auf der Hardware der Kunden, sondern in Rechenzentren der Finanzinformatik betrieben. Die Kommunikation des Nutzers mit dem Rechenzentrum der Finanzinformatik erfolgt über eine im Internetbrowser integrierte Software (Java-Applikationen [90]) der Star Finanz, die eine verschlüsselte direkte Kommunikation mit dem Rechenzentrum des jeweils kontoführenden Kreditinstituts herstellt, ohne dass PIN und TAN an die Star Finanz übermittelt werden. Dabei ist die Kommunikation nur mit solchen Kreditinstituten möglich, deren Online-Banking über eine FinTS-Schnittstelle verfügt. Über diese Verbindung gibt der Kunde seine Zugangsdaten zum Konto, inklusive der Personalisierten Sicherheitsmerkmale, ein. Diese beinhalten sowohl die PIN zur Identifizierung als auch die TAN zur Autorisierung von Aufträgen gegenüber dem kontoführenden Kreditinstitut. Die abgerufenen Kontodaten werden mit Ausnahme der Personalisierten Sicherheitsmerkmale an die Server der Star Finanz übertragen und gespeichert. Der Anwender kann die auf den Servern gespeicherten Daten jederzeit löschen.

118. Mittels Starmoney Web können verschiedene Kontenarten gleichzeitig genutzt und verwaltet werden. Infrage kommen sowohl Girokonten als auch Einlage-, Kreditkarten-, Bauspar- und Kreditkonten.

119. Die Kontodaten werden auf Servern der Star Finanz gespeichert, bei denen es sich nicht um Bankenserver handelt. Da Star Finanz insoweit keine Bankdienstleistungen anbietet, unterliegen die Server nicht der Aufsicht durch die BaFin.

---

[90] Ein in der Programmiersprache Java geschriebenes Programm, welches über einen Webbrowser in einer standardisierten Laufzeitumgebung ausgeführt wird, ohne dass Daten vom Endgerät des Nutzers oder vom Server (hier der Finanzinformatik) bereitgestellt werden müssen.

120. Für die Eingabe der Personalisierten Sicherheitsdaten in der von Star Finanz bereitgestellten Software (Java-Applikationen) sowie die Speicherung der Kundendaten auf den Servern der Star Finanz werden die Daten nicht, wie in den Sonderbedingungen für das Online-Banking vorgesehen, auf der Seite des jeweils kontoführenden Kreditinstituts eingegeben. Die Star Finanz unterhält keine vertraglichen Beziehungen zu den kontoführenden Kreditinstituten, deren Daten sie auf eigenen Servern speichert. Gesonderte Vereinbarungen existieren nicht.

b) Beispiele für Angebote der genossenschaftlichen Bankengruppe

121. Die Fiducia&GAD betreut sämtliche Genossenschaftsbanken. Vormals haben Fiducia IT AG und GAD eG jeweils gegenüber einem Teil der Institute eigenständige technische Dienstleistungen angeboten (vgl. Fußnote 88). Zu diesem Zweck haben die beiden Unternehmen bisher eigene technische Produkte für ihre Kunden entwickelt, welche die jeweiligen verbundweiten Produkte der genossenschaftlichen Bankengruppe ergänzen.

aa) „ELAXY Finanzmanager"

122. Die GAD vertreibt den „ELAXY Finanzmanager" als Personal Finance Management-System. Entwickelt und betrieben wird das Produkt von einer Tochtergesellschaft der GAD, die es an Finanzdienstleister innerhalb und außerhalb der genossenschaftlichen Bankengruppe vertreibt. Das Produkt ist multibankenfähig. Derzeit wird das Produkt innerhalb des genossenschaftlichen Bankensektors den Kreditinstituten jedoch nur zur Nutzung mit eigenen Konten zur Verfügung gestellt. [redacted] Außerhalb des genossenschaftlichen Bankensektors wird das Produkt jedoch mit uneingeschränkter Multibankenfähigkeit vertrieben.

123. Bei dem „ELAXY Finanzmanager" handelt es sich um ein System z.B. zur Analyse und Kategorisierung von Kontoumsätzen oder zur Darstellung der Vermögensentwicklung. Das Produkt wird als Web-Anwendung betrieben und ist über einen Internetbrowser über alle gängigen Endgeräte nutzbar. Der Abruf der Kontoinformationen erfolgt durch den „ELAXY Finanzmanager" über die FinTS-Schnittstelle. Die Erteilung von Aufträgen an das kontoführende Kreditinstitut ist nicht vorgesehen, sodass es hier nicht zur Eingabe von TAN zur Autorisierung von Aufträgen kommt.

124. [redacted]

bb)„Online-Filiale+“

125. GAD vertreibt ebenfalls eine Software-Applikation (kurz: App) unter der Bezeichnung „Online-Filiale+“ zur Nutzung auf mobilen Endgeräten (z.B. Smartphones). Die App wird über die Online-Stores z.B. für die Betriebssysteme iOS und Android vertrieben, auf den jeweiligen Geräten der Kunden installiert und von dort aus genutzt. Für den Zugang zum Programm vergibt der Kunde ein Passwort, das jeweils vor Beginn der Nutzung eingegeben werden muss.

126. Mit der Software können Kunden auf Kontoinformationen zugreifen und eine Vielzahl von Aufträgen wie z.B. Überweisungen, Umbuchungen oder Daueraufträge erteilen. Ebenso können grundlegende Sicherheitseinstellungen des Online-Bankings über die Software angepasst werden. Hierzu gehört bspw. die Änderung der PIN. [91]

127. Aufgrund der Multibankenfähigkeit der App haben Kunden die Möglichkeit, alle Konten bei verschiedenen Kreditinstituten parallel zu nutzen, soweit die jeweils kontoführenden Kreditinstitute die Schnittstelle FinTS unterstützen.

128. Unabhängig von der kontoführenden Bank erfolgt der Zugang zum Konto über die für das Online-Banking des jeweiligen Kreditinstituts üblichen Zugangsdaten und die Eingabe der PIN. Die Software bietet die verschlüsselte Speicherung der PIN auf dem jeweiligen Endgerät als Alternative an. In der Anwendung wird der Kunde darauf hingewiesen, dass das Speichern der HBCI-PIN den Sicherheitsbestimmungen der meisten Banken widerspricht. Der Kunde kann durch Anklicken eines Kontrollfeldes die Speicherung der PIN auf eigenes Risiko bestätigen. Dies gilt sowohl für genossenschaftliche Konten als auch für Konten anderer Kreditinstitute.

---

[91] Bl. 6719f. d.A.

Abb. 4, **Screenshot** aus Anwendung „Online-Filiale+“

129. Für die Freigabe der Aufträge benötigt der Kunde eine TAN, wobei die Software lediglich das smart-TAN-Verfahren unterstützt, d.h. der Kunde kann lediglich solche TAN verwenden, die er durch die Nutzung der Chip-Karte und des TAN-Generators selbst erzeugt hat. Die Kommunikation zwischen der Anwendung und dem kontoführenden Kreditinstitut erfolgt über die Web-Schnittstelle. Die verschlüsselten Daten werden ausschließlich vom Endgerät des Nutzers an das kontoführende Kreditinstitut übertragen.

c) Beispiele für Zahlungsauslösedienste im Internethandel

aa) Sofortüberweisung.de als bankenunabhängiger Zahlungsauslösedienst

130. Sofort betreibt u.a. einen Zahlungsauslösedienst für den Internethandel unter der Marke sofortueberweisung.de. Das Angebot dient zur Bezahlung von Waren und Dienstleistungen in Online-Shops oder auch zur Auffüllung von elektronischen Geldbörsen, welche wiederum zur Bezahlung im Internethandel eingesetzt werden.

131. Sofort vermarktet das Bezahlverfahren gegenüber Händlern und nutzt alternativ das Angebot sogenannter Payment Service Provider (PSP). Bei PSP handelt es sich um Unternehmen, die Händlern die Annahme von elektronischen Zahlungen ermöglichen. PSP verantworten dabei die vertragliche und technische Anbindung des Händlers in der Regel an verschiedene Bezahlverfahren. Hierfür halten PSP die technischen

Schnittstellen der Bezahlverfahren vor, an die Händler angebunden werden.[92] Soweit die Sofort ihr Bezahlverfahren selbst vermarktet, hält sie den Vertrag mit dem Händler und realisiert ebenfalls die technische Anbindung des Händlers an das Bezahlsystem.

132. Wird dem Kunden das Bezahlverfahren sofortueberweisung.de als Möglichkeit beim Kauf von Waren angezeigt, wird er nach Auswahl des Verfahrens zum technischen System von Sofort weitergeleitet, in welches er die notwendigen Daten für die Auslösung des Bezahlprozesses eingibt. Zu Beginn der Transaktion erhält der Kunde in den Datenschutzhinweisen Angaben dazu, wie das Verfahren sofortueweweisung.de durchgeführt wird, welche Prüfungen stattfinden und welche personenbezogenen Daten erhoben werden. Der Kunde wird ebenfalls darüber informiert, welche personenbezogenen Daten wann und an wen weitergegeben werden. Die Datenschutzhinweise enthalten darüber hinaus Angaben zu der Art und der Dauer der Speicherung personenbezogener Daten sowie dem Vorgehen der Sofort bei nachträglicher Meldung gescheiterter Überweisungen, die mit sofortueberweisung.de in das Online-Banking beauftragt worden sind, sowie eine Kontaktemailadresse für weitere Fragen an Sofort.

133. Der Kunde wählt bei der Nutzung von sofortueberweisung.de sein Kreditinstitut aus und gibt die entsprechende Kontonummer und zunächst die Personalisierten Sicherheitsmerkmale zur Authentifizierung gegenüber dem Kreditinstitut ein. Das Bezahlverfahren stellt den Zugang zum Online-Banking des entsprechenden Kreditinstituts über die von der DK zur Kommunikation mit Drittanbietern definierten Schnittstellen (FinTS oder HBCI) oder das sogenannte Screen-Scraping[93] her, sofern einzelne Kreditinstitute die Schnittstellenstandards der DK nicht nutzen. Die Kontodaten und Personalisierten Sicherheitsmerkmale leitet sofortueberweisung.de verschlüsselt an das eigene Rechenzentrum weiter, von wo aus diese wiederum verschlüsselt an das Kreditinstitut weitergegeben werden. Bei dem von der Sofort genutzten Rechenzentrum handelt es sich um ein Bankenrechenzentrum (Rechenzentrum der Deutsche Kontor Bank AG), das hinsichtlich der Sicherheitsstandards der Aufsicht durch die BaFin

---

92 http://www.bvdw.org/die-bezahlverfahren/dienstleister-des-zahlungsverkehrs/payment-service-provider.html, Stand 29. 01. 2015.

93 Beim sogenannten „Screen Scraping“ handelt es sich um eine Technologie zum Extrahieren von Daten von Internetseiten, vgl. dazu BGH, Flugvermittlung im Internet (I ZR 224/12), 30. 04. 2014, Leitsatz, zitiert nach juris.

unterliegt, auch wenn diese speziellen Dienste derzeit nicht in die Aufsicht integriert sind.[94]

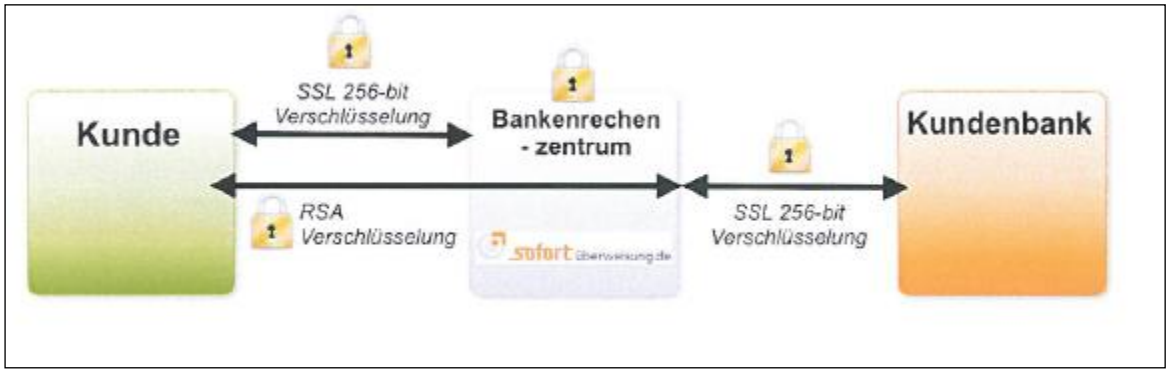


Abbildung 5: Verschlüsselung bei Nutzung von sofortüberweisung.de[95]

134. Nach Übertragung der erforderlichen Daten stellt der Zahlungsauslösedienst den Überweisungsauftrag in das System des Kreditinstituts ein und prüft dabei bankenindividuell, ob eine Ausführung der Überweisung möglich ist. Die Prüfung erfolgt dabei entweder durch Feststellung, dass der Überweisungsauftrag vom Kreditinstitut angenommen wurde oder das Konto über entsprechende Deckung verfügt, ggf. durch eine explizite Prüfung des Verfügungsrahmens auf dem Konto des Kunden. Letzteres erfolgt in Fällen, in denen Kreditinstitute Transaktionen nur zu bestimmten Zeiten verbuchen, der Kontostand also nicht bereits vorgemerkte Buchungen berücksichtigt und daher allein kein hinreichendes Indiz für den Verfügungsbetrag darstellt.

135. Bei Transaktionen, die erfahrungsgemäß ein erhöhtes Missbrauchsrisiko beinhalten, prüft die Software, ob in den letzten 30 Tagen vom entsprechenden Konto Transaktionen mit sofortueberweisung.de durchgeführt und ob diese tatsächlich auf dem Konto verbucht wurden. Hierzu wird die für die anstehende Zahlung genutzte Kontonummer mit den im System zu Dokumentationszwecken gespeicherten Daten verglichen. Sofern in den Systemen der Sofort gespeicherte Transaktionen der letzten 30 Tage vorliegen, wird die ordnungsgemäße Verbuchung auf dem Konto des Kunden nachvollzogen. Die Software nimmt dies, neben der Information des - möglicherweise nicht aktuellen - Verfügungsrahmens, als zusätzlichen Hinweis dafür, dass auch im vorliegenden Fall die Verbuchung der Zahlung erfolgen wird.

---

[94] Gleiches gilt z.B. für die von der StarFinanz angebotene Dienstleistung starmoney.web, die ebenfalls auf Servern in einem Bankenrechenzentrum betrieben werden. Auch diese Server unterliegen insoweit aber nicht der Aufsicht durch die BaFin.

[95] Bl. 725 d.A.

136. Nach Feststellung der Annahme der Überweisung durch das real-time buchende kontoführende Kreditinstitut[96] oder der Prüfung des Verfügungsbetrags auf dem Konto des Kunden bzw. der Ausführung der sofortueberweisung.de-Transaktionen der letzten 30 Tage wird dem Kunden das ausgefüllte Überweisungsformular auf dem Bildschirm angezeigt. Über das Bezahlverfahren gibt der Kunde daraufhin eine entsprechende TAN ein, die wiederum über das System von sofortueberweisung.de verschlüsselt an das Kreditinstitut weitergeleitet wird; der Kunde löst damit den Geschäftsvorfall gegenüber seinem Kreditinstitut aus.

137. Der Händler erhält von sofortueberweisung.de als Bestätigung die Rückmeldung, dass die Überweisung erfolgreich eingestellt wurde.

138. Im System der Sofort werden diejenigen Informationen aus der Transaktion gespeichert, über die die Kunden vorab in den Datenschutzhinweisen informiert werden. Zu den über die Transaktion gespeicherten Informationen gehören der Name des Kontoinhabers, die Kontonummer und Bankleitzahl (IBAN), der Betreff, der Überweisungsbetrag sowie das Überweisungsdatum und die Bezeichnung des Händlers.

139. Das System sendet dem Händler damit keine Garantie über den Eingang des Rechnungsbetrags auf dessen Konto, sondern lediglich die Bestätigung darüber, dass die Überweisung erfolgreich in das Online-Banking des Kundenkontos eingestellt wurde und die Bank die Überweisung dem Ergebnis der Prüfung der Kontodeckung entsprechend mit hoher Wahrscheinlichkeit ausführen wird.

140. Seine Dienstleistung bietet Sofort den Internethändlern im Vergleich zu PayPal und Kreditkarten zu deutlich günstigeren Preisen an.

bb) Zahlungsauslösedienste von Kreditinstituten

(1) giropay

141. Der Zahlungsauslösedienst giropay[97] gibt Händlern ebenfalls die Möglichkeit, Kunden die Bezahlung von Waren oder Dienstleistungen über das Online-Banking ihres Kreditinstituts anzubieten.

---

[96] Real-time buchende Kreditinstitute sind solche, deren Systeme Zahlungsvorfälle unmittelbar ausführen und verbuchen und daher neue Geschäftsvorfälle stets anhand eines aktuellen Kontostandes disponieren.

[97] Die nachfolgende Darstellung zum Bezahlverfahren giropay basiert, soweit keine anderen Quellen herangezogen werden, auf den Antworten der giropay GmbH zum Auskunftsersuchen des Bundeskartellamtes vom 05.10.2010 im Kartellverwaltungsverfahren B4-72/10.

142. Betreiber von giropay sind derzeit die Gesellschafter des Unternehmens, Star Finanz und Fiducia&GAD. Der Betrieb des Systems erfolgt dabei jeweils in der gesicherten Umgebung eines Bankenrechenzentrums, dessen Sicherheit aber nicht der Prüfung durch die Bankenaufsicht unterliegt.[98] Der technische Betrieb umfasst die technische Anbindung derjenigen Kreditinstitute, die sich für die Teilnahme an dem Zahlungsauslösedienst entschieden haben, sowie derjenigen Acquirer und Payment Service Provider[99], die die vertragliche und technische Anbindung von Händlern realisieren.

143. Soweit die Betreiber des Zahlungsauslösedienstes unterschiedliche technische Systeme einsetzen, sind diese über Schnittstellen miteinander verbunden, um Transaktionen abwickeln zu können, bei denen die Kreditinstitute des Kunden und des Händlers Verträge mit jeweils unterschiedlichen Betreibern abgeschlossen haben.

144. Die Entscheidung zur Bezahlung von Waren oder Dienstleistungen mit giropay trifft der Kunde. Nach Auswahl des Zahlungsauslösedienstes als Bezahlverfahren erhält der Kunde Zugang zur giropay-Seite seines Kreditinstituts auf den Systemen des Betreibers, auf der er seine Online-Banking-Zugangsdaten eingibt. Nach Eingabe seiner PIN zeigt ihm das System eine vorausgefüllte Überweisungsmaske und fordert den Kunden zur Autorisierung der Überweisung durch Eingabe einer TAN auf. Das Kreditinstitut disponiert die Überweisung nach der TAN-Eingabe und nimmt diese nach positiver Prüfung entgegen.

145. Das Kreditinstitut des Kunden gibt bei erfolgreicher Disposition des Rechnungsbetrags eine Zahlungsgarantie gegenüber dem Internethändler oder dessen Acquirer ab.[100] Für diesen Zweck hat die DK einen speziellen Textschlüssel für unwiderrufbare Internetüberweisungen definiert und eingeführt, den die giropay nutzt.

(2) Paydirekt

146. Paydirekt ist ein Bezahlverfahren der deutschen Privatbanken, genossenschaftlichen Kreditinstitute sowie der Sparkassen. Es handelt sich um einen Zahlungsauslösedienst für Händler im Internethandel. Das System wir seit Ende 2015 auf dem Markt angeboten.

147. Bei der Nutzung des Dienstes leitet der Händler den Kunden zur Auslösung der Zahlung über das Girokonto des Kunden an das Paydirekt-System, auf dem sich der Kunde

---

98 Schreiben der BaFin vom 08.08.2012, Bl.3336ff. d.A.

99 Die giropay Rules und Regulations verstehen unter PSP einen vom Acquirer beauftragten technischen/betrieblichen Dienstleister, Rules und Regulations, S. 4, Stand 25.02.2009.

100 Schreiben der DK vom 02.11.2010, Bl. 456 d.A.

einloggen muss, um die Zahlung vom Girokonto auszulösen. Nach erfolgreicher Durchführung der Zahlung erhält der Händler eine Zahlungsgarantie.[101]

d) Beispiele für sonstige Angebote bankenunabhängiger Dienstleister im Zusammenhang mit dem Online-Banking

148. Produkte mit Bezug zum Online-Banking werden auch von bankenunabhängigen Anbietern entwickelt und vertrieben. Der Funktionsumfang reicht von der Abfrage der Kontostände bis zur Erteilung von Zahlungsaufträgen. Die Produkte unterscheiden sich auch dahingehend, ob sie auf dem Endgerät des jeweiligen Nutzers oder auf oder über Server des jeweiligen Anbieters betrieben werden. In unterschiedlicher Weise nutzen diese Angebote die Infrastruktur von Banken. In der Regel geben die Kunden auch bei diesen Angeboten die für den Zugang zum Online-Banking notwendigen Personalisierten Sicherheitsmerkmale ein. In welcher Weise der entsprechende Dienstleister diese Daten verarbeitet ist für den Kunden regelmäßig nicht überprüfbar. Die nachfolgenden Angebote sind exemplarisch zu verstehen und geben keinen vollständigen Überblick über die Produkte am Markt.

aa) WISO Mein Geld

149. Seit 1993 bietet das Unternehmen Buhl Data Service GmbH, Neunkirchen, verschiedene Softwareprodukte im Zusammenhang mit der Nutzung des Online-Bankings an. Das umsatzstärkste Produkt des Unternehmens ist die Software, die unter der Bezeichnung „WISO Mein Geld“ vertrieben wird.[102]

150. Bei der Software WISO Mein Geld handelt es sich um eine sogenannte Personal Finance Management Software, mit der Kontoumsätze, Depotbestände und Kontoauszüge von verschiedenen Kreditinstituten abgerufen, dargestellt und analysiert werden können. Der Kontozugang der Software erfolgt über die FinTS-Schnittstelle, sofern die kontoführenden Kreditinstitute die von der DK bereitgestellte Schnittstelle nutzen, andernfalls durch

---

[101] Vgl. https://www.paydirekt.de/haendler/psp-api.html#_einf%C3%BChrung, Einführung und Ablauf einer Paydirekt-Zahlung, Stand 14.05.2016.

[102] Neben „WISO Mein Geld“ vertreibt das Unternehmen Software mit spezifischen Funktionen für bestimmte gewerbliche Anwendungen („Wiso Mein Büro“, „WISO Kaufmann“), die zwar keine administrativen Kontofunktionen unterstützen oder sich auf spezifische Anwendungsbereiche beziehen, wie z.B. die Erstellung von Einkommensteuererklärungen („Wiso Steuer Sparbuch, T@x“) oder die Immobilienverwaltung („WISO Hausverwalter“) dabei jedoch auch den Abruf von Kontoumsätzen ermöglichen.

Auslesen der Website des jeweiligen Kreditinstituts (Screenscraping[103]). Dabei meldet sich die Software über den Internetzugang bei der Bank an und erhält die erforderlichen Kontodaten, welche dann ausgelesen und in die Software importiert und verarbeitet werden.

151. Über die Software können neben dem Abruf der Kontoumsätze alle gängigen Geschäftsvorfälle abgewickelt werden. Hierzu gehören z.B. die Erteilung von Überweisungs- und Daueraufträgen sowie die Einreichung von Lastschriften. Darüber hinaus ist auch die Abwicklung administrativer Aufträge mit Bezug zu Personalisierten Sicherheitsmerkmalen möglich. Die Software erlaubt die Sperrung und Änderung der PIN sowie die Anforderung und Sperrung neuer TAN-Listen.

152. Die verschiedenen Softwareprodukte leiten Kontodaten nicht über Server der Buhl Data. Die gesamte Kommunikation erfolgt zwischen Rechnern des Kunden und des Kreditinstitutes über die FinTS-Schnittstelle oder den Internetbrowser beim Auslesen der Kontodaten durch die Software. Die Software fragt Kontodaten ab, sobald der Kunden dies manuell auslöst oder in den durch den Kunden festgelegten Zeitintervallen. Die Zugangsdaten für das Online-Banking verschlüsselt die Software und speichert sie in einer Datenbank auf dem Rechner des Kunden. Lediglich die PIN wird dann gespeichert, wenn der Kunde dies explizit auswählt.

153. Zwischen Buhl Data und der Deutschen Kreditwirtschaft hat es – jedenfalls in den zehn Jahren seit Programmeinführung bis zum Jahr 2012 – keinen Kontakt oder Austausch zu den Softwareprodukten gegeben, weder hinsichtlich der Funktionalitäten noch zu Sicherheitsfragen oder anderen Themen.[104]

bb) Finanzblick

154. Neben dem Softwareangebot, das auf dem Rechner des Kunden installiert und von diesem aus betrieben wird, bietet Buhl Data ein weiteres Produkt unter dem Namen Finanzblick an. Das Programm kann auf Smartphones (iOS und Android) oder als Web-Applikation betrieben werden. Bei der Web-Applikation stellt der Kunde den Zugang zur technischen Infrastruktur von Buhl Data, auf der das Programm betrieben wird, über eine

---

103 Einsatz eines automatisierten Systems oder einer Software zum Extrahieren von Daten von einer Website, um diese auf einer anderen Website anzuzeigen ("Screen Scraping"), vgl. BGH, Beschluss vom 30.04.2014, Az I ZR 224/12, Rz. 3.

104 Schreiben der Buhl Data vom 13.07.2012, Bl. 3305 d.A.https://play.google.com/store/apps/details?id=subsembly.banking.

Internetverbindung her. Auch die Kommunikation der Applikationen für Smartphones wird zumindest teilweise über die Server des Unternehmens geleitet.

155. Die Speicherung von Zugangsdaten im Zusammenhang mit der Produktnutzung erfolgt bei der Smartphone-Applikation auf dem Gerät des Kunden und bei der Web-Applikation auf den Servern der Buhl Data. Für den Zugriff auf die Daten muss der Kunde eine Registrierung durchführen, bei der auch die Erstellung eines Passworts erforderlich ist, wodurch der Zugriff auf die Web-Applikation durch unberechtigte Dritte verhindert wird.

156. Zur Datenübermittlung nutzt Finanzblick das sogenannte Screenparsing. Hierbei werden, z.B. bei der Erteilung eines Überweisungsauftrags, zunächst die erforderlichen Daten (Kontozugangsdaten sowie PIN und ggf. TAN, Konto-Nr. des Empfängers und Verwendungszweck) verschlüsselt an den Finanzblick-Server übermittelt und von dort - nach technisch erforderlicher vorrübergehender Entschlüsselung im Server des Unternehmens – erneut verschlüsselt und an die Bank des Kunden übertragen. Die Buchungsdaten werden anschließend verschlüsselt von der Bank zurück übertragen. Auch auf dem Rückweg findet eine vorübergehende Entschlüsselung auf dem Finanzblick-Server statt. Mitarbeiter des Unternehmens haben zu keinem Zeitpunkt Zugriff auf diese Daten.[105]

157. Im Wesentlichen bietet das Produkt Finanzblick einen vergleichbaren Funktionsumfang wie die WISO-Produkte. Kunden können Kontoumsätze abfragen und Zahlungsverkehrsaufträge, z.B. Daueraufträge erteilen. Lediglich administrative Geschäftsvorfälle bildet das Programm nicht ab.

158. Für die Speicherung der Kontodaten des Kunden betreibt Buhl Data separate Server in Deutschland, auf denen die Daten für jeden Kunden getrennt verschlüsselt abgelegt werden.

cc) Sonstige Anwendungen

159. Zugang zu den Kontoinformationen der Kreditinstitute sowie die Möglichkeit zur Erteilung von Zahlungsaufträgen erhalten Bankkunden, die über ein Online-Banking -Konto verfügen, auch durch Nutzung weiterer Apps, die auf mobilen Endgeräten betrieben werden. Solche Angebote werden sowohl von Kreditinstituten[106] als auch von bankenunabhängigen Anbietern angeboten[107]. Die Angebote haben einen

---

105 https://www.finanzblick.de/datenschutz/, Stand 12.05.2016.

107 Schreiben der Buhl Data vom 13.07.2012, Bl. 3305 d.A.

unterschiedlichen Leistungsumfang. Sie lassen sich danach differenzieren, ob lediglich Umsätze abgerufen[108] oder die Abwicklung einer Vielzahl von Bankgeschäften, wie z.B. die Erteilung von Überweisungsaufträgen oder Kauf- bzw. Verkaufsaufträgen für Wertpapiertransaktionen, durchgeführt werden können. Unterschiedlich ausgestaltet sind die am Markt angebotenen Produkte auch hinsichtlich der Multibankenfähigkeit, d.h. der gleichzeitigen Verwendung für Konten bei verschiedenen Kreditinstituten. Während bspw. Produkte der Commerzbank lediglich für die Konten des eigenen Unternehmens verwendet werden können, bietet die Commerzbank-Tochter comdirect eine App an, mit der Konten und Depots bei unterschiedlichen Banken zugänglich sind. Bankfremde Produkte sind in der Regel durch die Nutzung der HBCI/FinTS-Schnittstelle der Kreditwirtschaft ebenfalls für die Zusammenfassung der verschiedenen Kontoverbindungen eines Kunden ausgestaltet.[109]

160. Über die auf dem mobilen Endgerät installierte Software hat der Kunde die Möglichkeit, Online-Banking-Zugangsdaten einzugeben, dadurch über die Software Zugang zu den Kontodaten bei unterschiedlichen Kreditinstituten zu erlangen und entsprechend dem Leistungsumfang Aufträge zu erteilen. Autorisiert werden die Aufträge über die von dem entsprechenden Kreditinstitut angebotenen TAN-Verfahren. Die Kontodaten werden, soweit erforderlich, auf den mobilen Endgeräten gespeichert, auf denen die Apps betrieben werden.

(1) Kontoblick

161. Ein weiteres Beispiel für ein ausschließlich über das Internet angebotenes Produkt ist das Programm Kontoblick, das die Kontoblick GmbH bis zum Ende des Jahres 2014 bereitgestellt hat. Das Unternehmen, das nach Eröffnung des Insolvenzverfahrens am 06.09.2012 später aufgelöst wurde,[110] bot die nachstehend beschriebene Dienstleistung weiterhin bis Ende 2014 an.[111] Die DK hat diesen Dienst als Beispiel dafür aufgeführt, wie Geschäftsmodelle ohne Verstoß gegen Sorgfaltspflichten realisiert werden können.

---

107 https://play.google.com/store/apps/details?id=subsembly.banking, Stand 20.09.2015.

108 Kontostand-App der Commerzbank, https://www.commerzbank.de/portal/de/privatkunden/service-und-hilfe/ihre-wege-zu-uns/mobile-banking-apps/apps.html, Stand 01.10.2014

109 http://www.pc-magazin.de/vergleichstest/apps-online-banking-test-android-iphone-starmoney-outbank-1944244.html, Stand 01.10.2014.

110 Handelsregisterauszug der Kontoblick GmbH, Amtsgericht Charlottenburg, HRB 133711 B, Abruf vom 24.09.2014.

111 Die Darstellung der Funktionsweise des Programms basiert ausschließlich auf der Darstellung des Unternehmens auf der eigenen Internetseite.

162. Kontoblick bot Nutzern die Möglichkeit, Umsätze online-geführter Konten zusammenzufassen und auszuwerten. Dabei wurden Umsätze kategorisiert und Gesamtsalden über die Vermögenssituation der Kunden auf den entsprechenden Konten gebildet.[112] Neben den online-geführten Konten bei verschiedenen Kreditinstituten war auch die Einbindung von Kreditkartenkonten, Tagesgeldkonten und Sparkonten vorgesehen.[113]

163. Die Dienstleistung wurde in zwei verschiedenen Versionen angeboten. Bei der kostenfreien Version konnten maximal zwei Konten verwaltet werden. In der kostenpflichtigen Version waren die Verwaltung einer unbegrenzten Kontenzahl sowie eine aufwendigere Kategorisierung der Zahlungsströme vorgesehen.[114]

164. Den Zugriff auf das Online-Banking der verschiedenen Kreditinstitute realisierte Kontoblick über die FinTS-Schnittstelle der DK.[115] Über FinTS und ein von Kontoblick in die Website integriertes Java-Applikationen erfolgten der Zugang zum Konto sowie der Abruf der Kontodaten. Weitere bestandsverändernde Transaktionen oder die Auslösung sonstiger Geschäftsvorfälle im Online-Banking waren über Kontoblick nicht möglich. Der Kontozugang erfolgte über Java-Applikationen in einer verschlüsselten Verbindung ausschließlich zwischen Kunde und Kreditinstitut. Kontoumsätze wurden über den Rechner des Kunden an Kontoblick weitergeleitet, dort für die Saldodarstellung und Kategorisierung genutzt und anschließend verschlüsselt gespeichert, ohne dass Mitarbeiter von Kontoblick Zugriff auf die persönlichen Daten erhielten.[116] Kontoblick bot den Nutzern die Speicherung der für das Online-Banking genutzten Personalisierten Sicherheitsmerkmale an, wodurch der Abruf der Kontoinformationen bei erneuter Anmeldung bei Kontoblick erleichtert wurde.

165. Mit den aus dem Online-Banking gewonnenen Informationen verband Kontoblick eine Nutzung zu Marktforschungszwecken. Der Kunden willigte im Rahmen der „Erklärung zum Datenschutz und der Einwilligung in die Erhebung, Speicherung und Verarbeitung von persönlichen Daten“ konkludent ein, dass Kontoblick die übermittelten Daten zu Marktforschungszwecken in anonymisierter Form, nur bezogen auf die Postleitzahl des Nutzers, nutzen und an Dritte weitergeben durfte.[117]

---

112 Ausdruck Kontoblick-Website Bl. 6300 d.A.
113 Ausdruck Kontoblick-Website Bl. 6299 d.A.
114 Ausdruck Kontoblick-Website Bl. 6292 d.A.
115 Schriftsatz der DK vom 09.08.2011, Bl. 1709f. d.A., Ausdruck Kontoblick-Website Bl. 6288 d.A.
116 Ausdruck Kontoblick-Website Bl. 6290 d.A.
117 Ausdruck Kontoblick-Website Bl. 6286 d.A.

(2) Datev

166. Ein weiteres Produkt mit einer Reihe von Besonderheiten bietet die Datev eG, Nürnberg, an. Bei der Datev handelt es sich um ein Unternehmen in der Rechtsform einer Genossenschaft, dessen Mitglieder weitgehend aus Steuerberatern, Rechtsanwälten und Wirtschaftsprüfern bestehen.[118]

167. Datev vertreibt Unternehmenssoftware und IT-Leistungen insbesondere an ihre Mitglieder sowie deren Mandanten. Das Angebot umfasst Zahlungsverkehrslösungen[119], welche die Möglichkeit bieten auf Online-Banking-Konten zuzugreifen und Zahlungsaufträge an Kreditinstitute zu senden. Die Anbindung zu den Bankrechenzentren erfolgt nicht über eine Verbindung zwischen Kunde und dem kontoführenden Kreditinstitut, sondern über das Datev-eigene Rechenzentrum. Die Zahlungsverkehrslösungen werden von der Datev eingesetzt, um weitere Anwendungen des Unternehmens (wie z.B. Finanzbuchhaltung und Lohnabrechnungen) mit den Banksystemen zu verbinden und bspw. Kontoumsätze zu importieren und zu verbuchen sowie Zahlungsaufträge zu erteilen.

168. Zum Zwecke der Anbindung an die Bankenrechenzentren nutzt die Datev einen sogenannten HBCI-Kernel, eine von kreditwirtschaftlichen Institutionen bereitgestellte und lizensierte Softwarekomponente. Der HBCI-Kernel stellt ein Bindeglied zwischen den beteiligten Rechenzentren dar und verschafft der Datev die Möglichkeit, Zugang zum Online-Banking aller deutschen Kreditinstitute zu erlangen und gewährleistet so die Multibankenfähigkeit der eigenen Produkte. Der HBCI-Kernel nimmt Geschäftsvorfälle und die zugehörigen Daten in einer von den Datev-Anwendungen verwendeten XML-Syntax entgegen, wandelt diese in die von HBCI geforderte entsprechende Syntax um und führt den Geschäftsvorfall aus, indem er die Verbindung zum Rechenzentrum des entsprechenden Kreditinstituts herstellt und die Daten weitergibt.

169. Datev nimmt über die von ihr angebotenen Systeme auch PIN und TAN zur Auslösung von Zahlungsverkehrsaufträgen entgegen. Diese werden über die Anwendungen verschlüsselt an das Rechenzentrum der Datev gesandt und dort vor der Übergabe an das Rechenzentrum des jeweiligen Kreditinstituts entschlüsselt. Sie liegen im Rechenzentrum der Datev vor Übergabe an den HBCI-Kernel in Klarschrift vor. Unmittelbar nach Übergabe an die entsprechenden Kreditinstitute werden die sensiblen Daten in einem automatisierten Prozess gelöscht.

---

[118] Kreditinstitute gehören nicht zum Mitgliedskreis der Datev.

[119] Datev-Zahlungsverkehr (Windows-PC Lösung) seit 2004 sowie Datev-Zahlungsverkehr online (Internet-Lösung) seit 2007.

170. Für die Entgegennahme und Weitergabe von PIN und TAN hat die Datev mit der Kreditwirtschaft weder vertragliche Vereinbarungen getroffen noch wurden gemeinsame Sicherheitskonzepte erarbeitet oder der Dienst seitens der Kreditwirtschaft geprüft und zugelassen.

VI. Reaktion der DK auf das Angebot von Dienstleistern im Zusammenhang mit dem Online-Banking

171. Die DK hat sich in den vergangenen Jahren intensiv mit der Sicherung ihrer Systeme vor dem Hintergrund missbräuchlicher Nutzung auseinandergesetzt und Sicherheitsfragen erörtert.

172. Im Zusammenhang mit Angeboten rund um das Online-Banking ist die DK über Jahre hinweg aber auch gegen Systeme vorgegangen, die als Bezahlverfahren im Internethandel tätig waren und PIN und TAN zur Auslösung von Zahlungen benutzen (dazu unten 1). Explizit hat sich die DK mit solchen Dienstleistern im Rahmen der Erstellung eines Intermediärskonzeptes auseinandergesetzt, in welchem die DK eine Positionierung gegenüber den unterschiedlichen Dienstleistern im Zusammenhang mit dem Online-Banking erarbeitet hat (dazu unter 2). Nach Beendigung der Arbeiten am Intermediärskonzept hat die DK Regelungen zum Umgang mit Zahlungsauslösediensten als Bezahlverfahren im Internethandel im Rahmen der Erarbeitung der AGB-Regelungen (Sorgfaltspflichten der Kunden bei der Nutzung des Online-Banking) formuliert (dazu unter 3). Gefahren durch andere Intermediäre als den Zahlungsauslösediensten wurden in dieser Zeit nicht thematisiert. Den Umgang mit Zahlungsauslösediensten hat die DK nach Abschluss der Arbeiten an den Online-Banking-Bedingungen auch im Rahmen der eigenen Pressearbeit weiter konkretisiert (dazu unter 4).

1. Bezahlverfahren im Internethandel im Zusammenhang mit dem Online-Banking

173. Zusammen mit der Entwicklung, Verbreitung und Nutzung des Internets wurden in den Jahren ab 2000 verschiedene Dienstleistungen entwickelt, unter anderem auch Angebote rund um das Online-Banking der Kreditinstitute. Soweit diese Angebote die Bezahlung von Rechnungen über den Zugang zum Online-Banking der Kreditinstitute oder internetbasierte Kontenaggregationsdienste umfassen, die mit der Eingabe von Personalisierten Sicherheitsmerkmalen verbunden sind, ist die DK gemeinschaftlich gegen solche Angebote vorgegangen. Die DK beruft sich dabei regelmäßig auf die Sorgfaltspflichten in den bestehenden Online-Banking-Bedingungen, welche Kunden die Eingabe von Personalisierten Sicherheitsmerkmalen auf bankfremden Internetseiten untersagen.

a) L'TUR Tourismus AG

174. Das Unternehmen L'TUR Tourismus AG (L'Tur) hatte im Jahr 2000 einen Service angeboten, um Kunden die Bezahlung von Reisebuchungen über das Online-Banking anzubieten. Die DK hat L'Tur daraufhin unter Hinweis auf die bestehenden Online-Banking-Bedingungen dazu gebracht, das Dienstleistungsangebot nicht fortzuführen. Unter Bezugnahme auf die Regelungen der „*im deutschen Kreditgewerbe Verwendung findenden Bedingungen für die konto-/depotbezogene Nutzung des Online-Bankings mit PIN und TAN*" wurde gegenüber L'TUR argumentiert, dass PIN und TAN als geheim zu haltende Medien nur gegenüber dem ausgebenden Kreditinstitut im Rahmen der Nutzung des Online-Bankings verwendet werden dürften, weshalb die AGB-Regelungen die Verpflichtung des Kunden normieren, dafür Sorge zu tragen, dass keine andere Person Kenntnis von PIN und TAN erlangt. Unter Hinweis darauf, dass es sich bei der Aufforderung zur Eingabe von PIN und TAN um eine Verleitung zum Bruch der vertraglichen Verpflichtungen handele, forderte die DK L'TUR auf, den Dienst nicht weiter anzubieten.[120] L'TUR hat zu diesem Zeitpunkt das Dienstleistungsangebot gestoppt, da entsprechende Presseberichte auf einen Verstoß der Kunden bei Eingabe von PIN und TAN auf der Seite von L'TUR gegen bestehende AGB-Regelungen der Kreditinstitute hingewiesen hatten.[121] L'TUR hat seinen Dienst im Anschluss an die Diskussion mit der DK nicht wieder aufgenommen sondern technisch so modifiziert, dass PIN und TAN bei der Nutzung unmittelbar auf der Seite des Kreditinstituts eingegeben wurden. Der Dienst erreichte danach keine Multibankenfähigkeit mehr, sondern war nur noch für Kunden der Postbank zu nutzen.[122]

b) „moneyshelf.com"

175. Ebenfalls unter Hinweis auf die bestehenden Regelungen in den Online-Banking-Bedingungen ist die DK gegen das unter der Bezeichnung „moneyshelf.com" (Money-shelf) vertriebene Produkt der Deutschen Bank vorgegangen. Moneyshelf stellte ein Finanzportal der Deutschen Bank dar, in dem Kunden ihren Finanzstatus bei verschiedenen Kreditinstituten auf einer Internetseite zusammengefasst einsehen und auch den Erwerb von Fonds, Aktien und Versicherungsprodukten abwickeln konnten. Auch hier hatte sich die DK unter Hinweis auf die Regelungen in den Online-Banking-Bedingungen und die darin enthaltene Pflicht des Kunden, PIN und TAN geheim zu halten

120 [redacted]
121 [redacted]
122 [redacted]

und keinem Dritten zugänglich zu machen, an das Unternehmen gewandt.[123] Gespräche wurden mit der Deutschen Bank in dem DK-Arbeitskreis Homebanking geführt, um eine gemeinsame Lösung zu erarbeiten.[124] Die Deutsche Bank hat das Produkt in Folge der Diskussion mit der DK wieder vom Markt genommen.

c) „Online-Überweisung“ von T-Online International AG

176. Im Rahmen von Gesprächen und Schriftwechsel hat die DK im Jahre 2001 auf die T-Online International AG, eine Tochtergesellschaft der Deutschen Telekom AG, eingewirkt, ihr Internet-Portal für Online-Banking einzustellen. Im Jahr 2003 hat die DK dem Unternehmen Bedenken hinsichtlich des angebotenen Zahlungsauslösedienstes unter der Bezeichnung „Online-Überweisung“ in verschiedenen Schreiben mitgeteilt und darauf hingewiesen, dass sie hierin einen Verstoß gegen geltendes Recht sehe. Thematisiert wurde in diesem Zusammenhang u.a. die Verleitung zum Vertragsbruch durch die an den Kunden gerichtete Aufforderung, die nach dem Online-Banking-Vertrag gegenüber Dritten geheimhaltungspflichtigen Personalisierten Sicherungsmerkmale bekannt zu geben. Der Aufforderung der DK, dieses Verhalten einzustellen, ist T-Online trotz der Drohung, die angeschlossenen Kreditinstitute zu unterrichten und sie bei der Wahrung der ihnen zustehenden Rechte zu unterstützen, nicht nachgekommen.[125] Die Deutsche Telekom bietet das Produkt weiterhin an.[126]

d) „sofortueberweisung.de“

177. Im Jahre 2004 hat die DK schließlich auch die Promido GmbH, die zum damaligen Zeitpunkt den Zahlungsauslösedienst sofortueberweisung.de betrieb, im Rahmen eines längeren Schriftwechsels erfolglos aufgefordert, diesen Dienst einzustellen, da seine Nutzung gegen rechtliche Vorgaben in den Kundenbedingungen verstoße und die Kunden zum Vertragsbruch auffordere. Auch hier wurde auf die Regelungen in den Sonderbedingungen für das Online-Banking verwiesen, nach denen die Kunden verpflichtet seien, dafür Sorge zu tragen, dass Dritte keine Kenntnis von PIN und TAN für das Online-Banking erlangen.

---

123 [redacted]
124 [redacted]
125 [redacted]
126 [redacted]

2. Erarbeitung des „Intermediärskonzepts“

178. Die inhaltliche Befassung der DK insbesondere mit bankenunabhängigen Zahlungsauslösediensten im Rahmen des sogenannten „Intermediärskonzept“ verdeutlicht das strategische Konzept, das die DK und die ihr angehörenden Spitzenverbände verfolgten und das im Einzelnen seinen Niederschlag in der hier beanstandeten Fassung der OBB gefunden hat. Das „Intermediärskonzept“ und die OBB wurden im selben Arbeitskreis (Online-Banking) der DK mit identischer Zielrichtung diskutiert.

179. [redacted][127]

180. [redacted][128]

181. [redacted]

---

127 [redacted]

128 [redacted]

[redacted]

182. [redacted]

183. [redacted]

184. [redacted]

185. [redacted]

---

129 [redacted]

[redacted][131]

186. [redacted]

187. [redacted][133]

188. [redacted][134]

189. [redacted]

130 In diesem Zusammenhang Fn. 90.

131 [redacted]

132 [redacted]

133 [redacted]

134 [redacted]

[redacted][135]

190. [redacted]

191. [redacted]

192. [redacted].[137]

193. [redacted]

---

135 [redacted]

136 [redacted]

137 [redacted]

194. [redacted]

195. [redacted][140]

196. [redacted]

138 [redacted]
139 [redacted]
140 [redacted]

[redacted][141]

3. Überarbeitung der Online-Banking-Bedingungen als Teil der Allgemeinen Geschäftsbedingungen

197. Eine weitere Reaktion der DK auf das Angebot von Dienstleistern im Zusammenhang mit dem Online-Banking war die Überarbeitung der Online-Banking-Bedingungen als Teil der Allgemeinen Geschäftsbedingungen. Die in der DK zusammenarbeitenden Verbände der Kreditwirtschaft haben die Überarbeitung der AGB-Vertragswerke entweder durch ein explizites Mandat oder im Rahmen der satzungsmäßigen Aufgaben für die angeschlossenen Kreditinstitute übernommen. Bei der Erarbeitung der Online-Banking-Bedingungen haben sie in verschiedenen Arbeitsgruppen zusammengearbeitet. In die Online-Banking-Bedingungen, die die Sorgfaltspflichten der Kunden bei der Nutzung des Online-Bankings festlegen, wurden Regelungen eingearbeitet und umgesetzt, die den Einsatz von bankenunabhängigen Zahlungsauslösediensten verhindern.

a) Mandatierung der Spitzenverbände zur Erarbeitung der Muster-AGB für die angeschlossenen Kreditinstitute

aa) DSGV

198. An der Überarbeitung der Online-Banking-Bedingungen beteiligte sich der DSGV auf der Grundlage der satzungsgemäßen Aufgaben, ein explizites Mandat zur Überarbeitung der AGB-Vertragswerke seiner Mitgliedsinstitute oder der Regionalverbände lag nicht vor.[142]

199. Das satzungsgemäße Mandat hierzu ergibt sich aus der Aufgabe, die gemeinsamen Interessen seiner Mitglieder (Regionalverbände) und deren angeschlossener Kreditinstitute durch Beratung, Erfahrungsaustausch und Unterstützung im Rahmen der gesetzlichen Bestimmungen und sonstigen Anordnungen zu fördern.[143] Explizit genannt wird in diesem Zusammenhang die Förderung des bargeldlosen Zahlungsverkehrs.[144]

---

141 [redacted]

142 [redacted]

143 [redacted]

144 [redacted]

200. Der DSGV hat mit den Regionalverbänden die Beteiligung an der Erarbeitung der Sonderbedingungen für das Online-Banking in der DK beschlossen,[145] Entwürfe der Sonderbedingungen für das Online-Banking mit den Regionalverbänden diskutiert[146] und deren Rückmeldungen wiederum zum Gegenstand der Beratungen in der DK gemacht.[147]

bb) BVR

201. Die Beteiligung des BVR an der Überarbeitung der Online-Banking-Bedingungen ergibt sich aus satzungsgemäßen Aufgaben des Verbandes, die u.a. in der Beratung der Mitglieder in rechtlichen Fragen bestehen.[148]

202. Den Auftrag zur verbundweiten Koordinierung notwendiger Arbeiten zur Überarbeitung der Online-Banking-Bedingungen in der DK erhielt der BVR [redacted] Als Ziel des Projektes wird die Umsetzung für die gesamte genossenschaftliche Bankengruppe formuliert.[151]

203. Die verbundweite Koordinierung der Überarbeitung der Online-Banking-Bedingungen wurde mit dem Projektteam Online-Banking diskutiert, das im Rahmen einer

---

145 [redacted]

146 [redacted]

147 [redacted]

148 [redacted]

149 [redacted]

150 [redacted]

151 [redacted].

Arbeitsgemeinschaft der genossenschaftlichen Rechenzentralen errichtet wurde.[152] [redacted]

cc) BdB

204. Die Interessenvertretung der Mitglieder durch den BdB im Rahmen der Zusammenarbeit mit den Spitzenverbänden der Kreditwirtschaft ergibt sich satzungsgemäß in den Fällen, die sich nicht auf den Bereich eines einzelnen Regionalverbandes beschränken.[153] Der BdB hat in den in der DK organisierten Arbeitsgruppen zur Überarbeitung der Online-Banking-Bedingungen ohne ein zusätzliches Mandat seiner Mitglieder mitgearbeitet.[154] [redacted].[155]

205. Am 25.06.2009 hat der Rechtsausschuss des BdB den Beschluss gefasst, den OBB in der von der DK beschlossenen Form zuzustimmen. [redacted].[156] Die finale Fassung der OBB datiert vom 13.07.2009.[157] Mit Rundschreiben vom 22.07.2009 hat der BdB seinen Mitgliedern die beschlossenen OBB zur Verwendung empfohlen.[158]

b) Zustandekommen der Online-Banking-Bedingungen in den relevanten Gremien der DK zwischen 2006 und 2009

206. Die DK hat in den Jahren 2006 bis 2009 die Online-Banking-Bedingungen in den beiden Arbeitskreisen Online-Banking und Online-Banking-Vertragswerke überarbeitet.[159]

207. In dem Arbeitskreis Online-Banking (im Folgenden: AK-OB) waren Vertreter der kreditwirtschaftlichen Verbände BdB, BVR und DSGV sowie Vertreter von IT-Dienstleistern der Sparkassengruppe (SIZ), des genossenschaftlichen Verbunds (GAD)

---

152 [redacted]
153 [redacted]
154 [redacted]
155 [redacted]
156 [redacted]
157 [redacted]
158 [redacted]
159 [redacted]

sowie der privaten Banken (BV-Zahlungssysteme GmbH) vertreten. Auch externe Beratungsunternehmen waren an dem AK-OB beteiligt.[160] Dem Arbeitskreis Online-Banking-Vertragswerke (im Folgenden AK-OBV) gehörten demgegenüber Vertreter externer Beratungsunternehmen nicht an. Die Verbände waren im AK-OBV jeweils auch durch die Rechtsabteilungen vertreten.[161]

208. Der AK OB befasste sich in dieser Zeit mit unterschiedlichsten Fragestellungen rund um das Online-Banking. Hierzu gehörten neben den Online-Banking-Bedingungen beispielsweise die Erarbeitung des oben dargestellten „Intermediärskonzeptes“, die Fortentwicklung der FinTS-Spezifikationen oder die durch Phishing auftretenden Probleme.

209. Die Überarbeitung der Sonderbedingungen begann in der DK im Jahre 2006 im AK-OB.[162] Die erste Sitzung, in der das Thema „Kundenbedingungen“ thematisiert wurde, fand am 30.03.2006 statt.[163] Zur Vorbereitung darauf hatte der DSGV eine Präsentation an die Teilnehmer verteilt, in der aktuelle Probleme des bestehenden Online-Banking-Vertragswerkes angesprochen werden.[164] Als besondere Probleme wurden die Komplexität der bestehenden Regelungen sowie fehlende kurzfristige Anpassungsmöglichkeiten an technische Entwicklungen, wie z.B. neueingeführte TAN-Verfahren oder giropay, genannt. Der DSGV stellte die bestehenden Sorgfaltspflichten der Kunden als nicht ausreichend dar, weshalb zusätzlich einzelvertragliche Sorgfaltspflichten zu regeln seien. Die Weitergabe von PIN und TAN an Dritte wurde im Zusammenhang mit der „Phishing- und Intermediärsproblematik“ ebenso erörtert wie die daraus abgeleitete Notwendigkeit, exaktere Formulierungen der Sorgfaltspflichten in Bezug auf die „Weitergabe von PIN und TAN an Dritte“ zu finden.[165] Als Empfehlung sprach sich der DSGV in der Präsentation für eine Verschiebung technischer Details in die von den Kundenbedingungen getrennte Verfahrensanleitung bzw. die Sicherheitshinweise aus,

---

160 [redacted]
161 [redacted]
162 [redacted]
163 [redacted]
164 [redacted]
165 [redacted]

wobei neben den allgemeinen, von der DK zu regelnden Teilen auch die Möglichkeit zu instituts- bzw. verbandsindividuellen Ergänzungen realisiert werden sollte. Der DSGV empfahl schließlich auch die Aktualisierung der notwendigen Rechte und Pflichten in den Online-Banking-Bedingungen und nannte hier exemplarisch die Sorgfaltspflichten der Kunden.[166] Die Teilnehmer des AK-OB verständigten sich in der Sitzung darauf, das weitere Vorgehen zunächst jeweils in den einzelnen Verbänden abzustimmen.[167]

210. Die weiteren Beratungen im Jahre 2006 fanden unter Teilnahme der Vertreter der Verbände BdB, BVR und DSGV im AK-OB statt. In diesen Sitzungen wurden im Wesentlichen vorbereitende Maßnahmen für die Erarbeitung gemeinsamer neuer Kundenbedingungen getroffen. Konkrete Formulierungen der Kundenbedingungen fanden in diesem Rahmen noch nicht statt. In der Sitzung von 22.08.2006 sprach sich der BVR dafür aus, die Kundenbedingungen zentral vorzugeben bzw. zu empfehlen. Der BVR betonte dabei, dass diese Regeln unter besonderer Beobachtung der Kartellbehörden stünden. Die Teilnehmer der AK-Sitzung sahen es als Aufgabe der Juristen an, gemeinsame Kundenbedingungen mit Unterstützung des Arbeitskreises zu formulieren. [168] In der Sitzung vom 14.12.2006 einigten sich die Mitglieder explizit auf die Erarbeitung gemeinsamer Kundenbedingungen im Jahr 2007.[169]

211. Einen ersten Entwurf der Kundenbedingungen hat der DSGV als Federführer im Jahre 2007 in Vorbereitung auf die Sondersitzung am 27.04.2007 an die Teilnehmer des AK-OB per Mail verschickt.[170] Bereits hier wurden weitere, über die bisherigen Regelungen hinausgehende Sorgfaltspflichten der Kunden zum Umgang mit PIN und TAN aufgeführt. In dem für die Sitzung versandten Entwurf des DSGV wurden weitere Sorgfaltspflichten zur Nutzung von PIN und TAN und zur Herstellung des Zugangs zum Online-Banking formuliert. Zum einen heißt es darin, dass der Teilnehmer verpflichtet ist, die technische Verbindung zum Online-Banking-Angebot des Kreditinstituts nur über die vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen. Zur Geheimhaltung von PIN und TAN enthalten die Sorgfaltspflichten die Vorschrift, dass

166 [redacted]

167 [redacted]

168 [redacted]

169 [redacted]

170 [redacted]

Anfragen außerhalb der vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangswege nicht beantwortet werden dürfen.[171]

212. Aufbauend auf dem Entwurf der Kundenbedingungen vom 27.04.2007 wurden die Arbeiten an den Online-Banking-Bedingungen unter Mitwirkung der Rechtsabteilungen der Verbände fortgesetzt. Angesichts der Anforderungen an den Umgang mit PIN und TAN wurde in den Arbeitskreisen diskutiert, hierzu einen einheitlichen Oberbegriff, wie z.B. „Identifikationsdaten“ oder „Sicherheitsdaten“, zu verwenden.[172] Die Sorgfaltspflichten enthielten in der Fassung Mai 2007 folgende Formulierung zur Geheimhaltung der Identifikationsdaten: „*Außerhalb der vom Kreditinstitut gesondert mitgeteilten Online-Banking Zugangswege dürfen Anfragen, insbesondere nach den vertraulichen Identifikationsdaten, nicht beantwortet werden.*“[173] In der Version Juni 2007 wurde dieser Begriff vorübergehend erneut durch separate Sorgfaltspflichten für den Umgang mit PIN bzw. TAN ersetzt.[174]

213. Im Jahre 2008 wurden die Arbeiten an den Online-Banking-Bedingungen fortgesetzt. Dabei waren auch die Auswirkungen der EU-Zahlungsdiensterichtlinie auf die Online-Banking-Bedingungen und insbesondere auf die Sorgfaltspflichten der Kunden Gegenstand der Diskussionen.[175]

214. In der Sitzung vom 11.03.2008 hat der AK-OBV die Sorgfaltspflichten der Kunden vor dem Hintergrund des Umgangs mit Intermediären diskutiert. Hierbei wurde der explizite Zusammenhang zwischen der Intermediärsproblematik und den auf die Zugänge zum Online-Banking abzielenden Sorgfaltspflichten hergestellt. [redacted]

171 [redacted]

172 [redacted]

173 [redacted]

174 [redacted]

175 [redacted]

176 [redacted]

[redacted]

215. Diese Formulierung stellt auch den Stand der Sorgfaltspflichten im Entwurf der Sonderbedingungen nach der Sitzung vom 11.03.2008 dar.[177]

216. In dem Entwurf der Sonderbedingungen vom 16.04.2008 wird der Bezug der Sorgfaltspflichten zu dem Umgang mit Intermediären noch verdeutlicht. Ergebnis der Sitzung ist nun erneut eine veränderte Formulierung, nach der die Legitimationsdaten nicht auf kreditinstitutsfremden Internetseiten (z.B. von Händlern) eingegeben werden dürfen.[178] Hierzu enthält der Entwurf eine Kommentierung als Fußnote, die den Bezug der Formulierung zum Umgang mit Intermediären klarstellt. Danach war vorgesehen, dass die Inanspruchnahme des Angebots von Intermediären einen Verstoß gegen die Sonderbedingungen darstellt. Bei der Formulierung sollte sichergestellt werden, dass insbesondere die Nutzung von Online-Banking-Software solcher Unternehmen, die mit der Kreditwirtschaft verbunden sind, nicht in Frage gestellt wird. In der Fußnote 14 heißt es dazu:

„Kommentar: Verhinderung der Einschaltung von Intermediären aus Sicherheitsgründen. Die Formulierung schließt jetzt nicht mehr den Einsatz von Online-Banking-Software (z.B. Starmoney) aus, bei der der Nutzer die Legitimationsdaten unter Nutzung dieser Software „offline“ eingibt. Der Begriff „institutsfremd“ ermöglicht es grundsätzlich, dass der Nutzer seine Legitimationsdaten auf vom Kreditinstitut zugelassenen Intermediärs-Seiten eingibt (Option bei FinTS 4.0). Hierzu bedarf es aber einer gesonderten Vereinbarung bzw. Mitteilung.“ [179]

217. Demgegenüber wurde der Bezug zu der Verhinderung einfacher Phishing-Angriffe in dem Entwurf der Sonderbedingungen mit der nachfolgenden Sorgfaltspflicht und der entsprechenden Kommentierung in der Fußnote 15 hergestellt. Die Sorgfaltspflicht schreibt den Kunden vor, dass Legitimationsdaten nicht außerhalb des Online-Banking-Verfahrens weiter gegeben werden dürfen. Als Regelungsbeispiel wird hier Bezug zu

---

177 [redacted]

178 [redacted]

179 [redacted]

einer Weitergabe per Mail genommen, einer klassischen Vorgehensweise von Phishing-Betrügern. Der Kommentar in der Fußnote hierzu lautet: *„Verhinderung der „einfachen" Phishing-Angriffe."*[180]

Erörtert wurde die Einschränkung der Tätigkeit von Intermediären bzw. eine Abgrenzung zwischen der Tätigkeit von Softwareanbietern und den Anbietern von Zahlungsauslösediensten. [redacted] Formulierungsvorschlag zu den Sorgfaltspflichten und dem Umgang mit PIN und TAN. Danach sollte es Kunden auch möglich sein, PIN und TAN auf einer lokal – auf dem Rechner des Kunden – betriebenen Software einzugeben, welche die Schnittstellen der Deutschen Kreditwirtschaft nutzt.[181] Dieser Vorschlag wurde [redacted], aufgenommen. [redacted] verwies darauf, dass der Software-Begriff insofern verändert werden müsse, als der Bezug zu der Nutzung der hinter den Softwareprodukten stehenden kreditwirtschaftlichen IT-Systeme und die unmittelbare Kontaktaufnahme mit dem kundenseitigen Institut relevant seien. Daher sprach er sich, [redacted], für eine abstraktere Formulierung anstelle eines Bezugs auf eine Software aus. Er verwies in seiner Antwort insbesondere auf die dann zu erwartende neue Diskussion [redacted] darüber, was unter der Nutzung einer Software konkret zu verstehen sei, und verwies auf die gefundene Lösung vor dem Hintergrund der Debatte um Zertifizierungsverfahren von Intermediären. [redacted]

[redacted].

180 [redacted]

181 [redacted]

[redacted][182]

218. Der AK-OBV hat in der ersten Hälfte des Jahres 2009 die Arbeiten an den Sonderbedingungen fortgesetzt und den Verbänden eine finale Fassung der überarbeiteten Bedingungen zur Abstimmung vorgelegt. In der Sitzung vom 26.01.2009 wurden die Bedingungen hinsichtlich der Änderungsvorschläge des DSGV und der Auswirkungen der Zahlungsdiensterichtlinie (PSD) diskutiert.[183] Die Formulierung der Sorgfaltspflichten der Kunden bei der Verwendung von PIN und TAN wurde dabei überarbeitet. Die Regelungen sahen danach immer noch vor, dass Personalisierte Sicherheitsmerkmale nicht außerhalb der gesondert vereinbarten Internetseiten (z.B. nicht auf Online-Händlerseiten) eingegeben werden dürfen. Die Erklärungen in dem Fußnotentext, dass hiermit Einfluss auf die Tätigkeiten von Intermediären genommen werden soll, blieben unverändert bestehen. Weitere Änderungen an der Formulierung der Sorgfaltspflichten hat es in den Folgesitzungen nicht mehr gegeben. Der AK-OBV hat in seiner Sitzung am 26.01.2009 beschlossen, die OBB in den Gremien der der Beteililgten zu 2.-4. zur verbandsinternen Beschlussfassug zu übersenden. [184] Im Anschluss daran wurden in der DK die redaktionellen Änderungen nach den Rückmeldungen aus den Verbänden diskutiert, ohne dass daraus eine inhaltliche Verändeung der OBB resultierte. Zu den nachfolgend (unter c.) nähe beschriebenen Zeitpunkten nahmen die Spitzenverbände die Bedingungen endgültig an. Am 05.08.2009 teilte die Beteiligte zu 2. als letzter Verband der DK den verbandsinternen Beschluss, die von der DK erarbeiteten OBB zu übernehmen und ihren Mitgliedern zur Nutzung zu empfehlen und zu übersenden, seinen Mitgliedern mit. Damit war, da die DK als konsensual tätiges Gremium nicht gegen die Interessen ihrer Mitglieder tätig wird, am 05.08.2009 auch auf der Ebene der DK die Beschlussfassung zur hier streitgegenständlichen Fassung der OBB zu Stande gekommen. Dementsprechen hat hat die DK die Beschlussabteilung am 05.08.2009 über die neugefassten AGB-Vertragswerke der Kreditwirtschaft informiert und die beschlossenen Mustertexte übersandt.

---

182 [redacted]

183 [redacted]

184 [redacted]

c) Abstimmung der Muster-AGB innerhalb der einzelnen Spitzenverbände der Kreditwirtschaft und Übernahme durch die angeschlossenen Kreditinstitute

219. Die von der DK zur Verwendung empfohlenen Online-Banking-Bedingungen werden von den Kreditinstituten auch tatsächlich verwendet. Die DK ihrerseits stellt die Online-Banking-Bedingungen als einheitliches Regelwerk der angeschlossenen Kreditinstitute dar.[185]

aa) Genossenschaftsbanken

220. Der BVR hat entsprechend seines Mandates für eine verbundweite Überarbeitung der OBB an dem Beschluss der DK mitgewirkt und die Arbeiten der DK in internen Gremien begleitet und beraten. Durch den BVR wurden die Regionalverbände der genossenschaftlichen Bankengruppe über den Stand und die Ergebnisse der Arbeiten an den AGB-Vertragswerken und damit auch der OBB informiert.

221. [redacted][189]

222. Mit Verbandsrundschreiben im März 2009, Juni 2009, Juli 2009 und zuletzt am 05.08.2009 hat der BVR die Mitgliedsbanken über die Umsetzung der Kundenbedingungen und deren Inhalte informiert.[190] Parallel dazu fanden verbandsinterne Vorkehrungen zur Umsetzung der notwendigen Information der Kunden über die

---

185 Vgl. Pressemitteilung ggü. Stiftung Warentest, Rz. 233ff.

186 [redacted]

187 [redacted]

188 [redacted]

189 [redacted]

190 [redacted]

anstehenden Änderungen an den AGB-Vertragswerken statt, an denen der DG Verlag als zentrale Einrichtung des Genossenschaftssektors beteiligt war.[191]

223. Von den im BVR organisierten genossenschaftlichen Kreditinstituten haben im Jahr 2012 mehr als 98%[192] das Formular „Sonderbedingungen für das Online-Banking“ vom DG Verlag bezogen und verwenden die von der DK ausgearbeiteten Regelungen gegenüber den eigenen Kunden[193]

bb) Sparkassen

224. Der DSGV hat die Arbeiten der DK parallel auch in eigenen Verbandsgremien organisiert und inhaltlich beraten.[194] Neben den verschiedenen Fachbereichen waren auch die Rechtsabteilungen des DSGV und der Regionalverbände an der Erarbeitung der OBB beteiligt.[195] Die OBB wurden in einer Kommission für Rechtsfragen mehrfach erörtert. Die hier erarbeiteten Änderungswünsche wurden erneut in die Beratungen der DK gegeben.

[redacted]

191 [redacted]

192 Gemäß eigener Statistiken des BVR waren 2009 insgesamt 1.156 Genossenschaftsbanken tätig, davon haben 1.086 das Formular bezogen und verwenden es gegenüber ihren Kunden (http://www.bvr.de/p.nsf/0/F0F8A6D1636D3A1CC1257D0A00540564/$file/3_Entwicklung-seit-1970-2014.pdf), Stand 29.05.2015. Die Quote derjenigen Institute, welche die OBB verwendeten, lag damit bei mehr als 93%.

193 [redacted]

194 [redacted]

195 [redacted]

196 [redacted]

197 [redacted]

225. Die Kommission für Rechtsfragen hat in ihrer Sitzung am 18.06.2009 den in der DK abgestimmten Entwurf der OBB letztmalig diskutiert und ihre Zustimmung erteilt[198], [redacted].[199]

226. Die Institute der Sparkassengruppe wurden seitens des DSGV durch ein Rundschreiben und „Fachmitteilungen für die Praxis“[200] am 13.08.2009 über die geänderten OBB informiert.[201] Für die angeschlossenen Kreditinstitute entwickelte der DSGV Hinweise zur Einführung der neuen OBB sowie einen Umsetzungsleitfaden. Auch im Bereich der Kundeninformation wurde der DSGV durch Erarbeitung einer Kundenbroschüre tätig.[202] Der DSGV verwies gegenüber den angeschlossenen Sparkassen auf die negativen Auswirkungen einer unterlassenen Kundeninformation und die daraus resultierende Folge, dass die bestehenden Bedingungen unwirksam werden und sich der Inhalt der Kundenverträge nach den neuen gesetzlichen Vorschriften der §§ 675 lit. c-z BGB sowie 676 lit. a-c BGB richten würde, was für die Institute zur Folge hätte, dass von den im Gesetz gewährten Abweichungsmöglichkeiten kein Gebrauch gemacht werden könnte.[203]

227. Die in Deutschland tätigen Sparkassen verwenden die von der DK erarbeiteten Bedingungen nach dem Kenntnisstand des DSGV fast ausnahmslos gegenüber ihren Kunden. Nach Einschätzung des DSGV haben von den im Jahre 2009 tätigen 458 Sparkassen und Landesbanken 429 – damit mehr als 93% der Institute - die geänderten Muster-AGB, zu denen die OBB gehören, zur Verwendung gegenüber ihren Kunden bestellt. Neben den Einzelbestellungen lagen weitere Bestellungen von Einkaufsgesellschaften vor, sodass es praktisch zu einer flächendeckenden Verwendung der OBB im Sparkassensektor kommt.[204]

---

198 [redacted]
199 [redacted].
200 [redacted]
201 [redacted].
202 [redacted]
203 [redacted].
204 [redacted]

cc) Mitgliedsinstitute des BdB

228. In den Arbeitskreisen [redacted] wurde über den Stand der Arbeiten der DK an den Bedingungswerken berichtet.[205] Der Arbeitskreis [redacted] hat die juristische Begleitung der Arbeiten übernommen. In der Sitzung vom 22.08.2007 und in der Folge während der in den Jahren 2008 und 2009 stattfindenden Sitzungen hat [redacted] das Thema der Anpassung der OBB behandelt.[206]

229. [redacted].[207]

230. Der Rechtsausschuss des BdB, [redacted], stimmte den in der DK erarbeiteten OBB in seiner Sitzung am 25.06.2009 formal zu.

231. Der BdB hat seine Mitglieder mit Rundschreiben vom 22.07.2009 über die zur Umsetzung des neuen Zahlungsdiensterechts zum 31.10.2009 erforderlichen Änderungen in den vom BdB bislang empfohlenen Bedingungswerken unterrichtet und die geänderte Fassung der OBB übersandt.[208]

232. Die Online-Banking-Bedingungen werden von den im BdB zusammengeschlossenen Kreditinstituten verwendet. Jedenfalls die im Retailbanking tätigen Kreditinstitute des BdB wie z.B. Deutsche Bank und ihre Tochtergesellschaften, Commerzbank, HypoVereinsbank, ING DiBA und eine Reihe weiterer Kreditinstitute verwenden die von der DK erarbeiteten Regelungen zu den Sorgfaltspflichten der Kunden.

4. Mediale Tätigkeit der DK im Zusammenhang mit dem Angebot von Online-Bezahldiensten

233. Gegenüber der Presse hat die DK die Tätigkeit der Sofort auf dem Markt auch nach Verabschiedung und Einführung der Online-Banking-Bedingungen und der darin enthaltenen Sorgfaltspflichten der Kunden – wie im Intermediärskonzept angedacht – kritisch begleitet.

---

205 [redacted]
206 [redacted]
207 [redacted]
208 [redacted]

234. Die Stiftung Warentest hat die DK für die Zeitschrift Finanztest im Januar 2010 angeschrieben, um deren Einschätzung zu der Tätigkeit der Sofort zu erfragen. Insbesondere ging es Finanztest um die Bewertung der Frage, wie die DK die Leistung der Sofort vor dem Hintergrund einschätze, dass Kunden, die den Zahlungsauslösedienst sofortüberweisung.de nutzen, PIN und TAN auf einer Internetseite der Sofort eingeben, deren Software die Auslösung der Transaktion bewirkt.

235. Nach Übersendung der Anfrage an den DSGV als Federführer der DK im Jahre 2010 wurde die Erarbeitung eines ersten Antwortentwurfs an den Geschäftsführer der giropay[209] übersandt, der dann zwischen den Fachebenen der einzelnen Verbände unter Beteiligung der Rechtsabteilungen abgestimmt worden ist.[210]

236. In der gemeinsamen Antwort der DK auf die Anfrage der Stiftung Warentest warnt die DK davor, die Personalisierten Sicherheitsmerkmale im Internet gegenüber Dritten zu offenbaren und verweist dabei auf die Online-Banking-Bedingungen der Kreditinstitute, nach denen die Eingabe von PIN und TAN ausschließlich auf den Internetseiten der Bank oder Sparkassen erfolgen dürfe. Die Eingabe von PIN und TAN auf Internetseiten nicht zugelassener Zahlungsauslösedienste wie dem der Sofort sah (und sieht) die DK als Verstoß gegen die Online-Banking-Bedingungen. Nicht im Sinne des Online-Bankings sei es, dass ein zwischengeschalteter Bezahldienst Zugang zum Konto erhalte, was die DK als *„quasi „phishing““* bezeichnet. Hingegen würden die Geheimhaltungspflichten der Online-Banking-Bedingungen eingehalten, wenn der Dienstleister einen Vertrag mit dem Kreditinstitut geschlossen habe, durch den die Eingabe von PIN und TAN unmittelbar auf der Seite des Kreditinstituts erfolge. Hier nennt die DK giropay als einen entsprechenden Dienst. Aus Sicht der DK bestehe grundsätzlich die Gefahr, dass die Ausbreitung von Angeboten wie dem der Sofort dazu führen könnte, dass sich Kunden an die Weitergabe ihrer vertraulichen Bankdaten gewöhnen. Diese Sorglosigkeit könnten Kriminelle gezielt ausnutzen.[211]

237. Sofort hat sich gegen die von der DK in ihrer Antwort auf die Anfrage der Stiftung Warentest verwendete Formulierung „quasi „phishing““ in Verbindung mit dem Dienst sofortüberweisung.de gewandt, da dies aus ihrer Sicht eine strafrechtlich zu würdigende Verleumdung des Dienstes darstelle.[212] Die DK hat in Folge dessen den Zusatz „quasi

209 [redacted]
210 [redacted]
211 [redacted]
212 [redacted]

„phishing““ aus dem an die Stiftung Warentest übersandten Text gelöscht und eine weitere einschränkende Änderung in Bezug auf die der Haftungsfrage bei Missbrauchsfällen eingefügt, nach der fraglich sei, ob es bei Missbrauchsfällen zu einer Erstattung durch das Kreditinstitut komme, da die Kunden entgegen den AGB gehandelt hätten.[213]

5. Vorgehen gegen Online-Bezahldienste

a) Klage vor dem Landgericht Köln

238. Am 09.10.2009 hat die giropay GmbH beim Landgericht Köln Klage gegen die damals als Payment Network AG firmierende Sofort wegen eines Wettbewerbsverstoßes gegen §§ 3, 4 Nr. 1, 9 und Nr. 10 UWG (Verleitung zum Vertragsbruch, unangemessene unsachliche Beeinflussung, Behinderungswettbewerb und Ausbeutung fremder Leistungsergebnisse) eingereicht.

239. Das Bundeskartellamt hat in diesem Verfahren am 28.02.2011 nach § 90 Abs. 2 GWB eine schriftliche Erklärung abgegeben, in dem der kartellrechtliche Vorwurf sowie der Stand des Verwaltungsverfahrens dargelegt wurden.

240. Das Landgericht Köln hat den Rechtsstreit zwischen der Klägerin giropay und der Beklagten Sofort mit Beschluss vom 29.04.2011 bis zum Abschluss des Kartellverwaltungsverfahrens ausgesetzt.[214]

b) Weitere Maßnahmen

241. Verschiedene kontoführende Kreditinstitute nutzen die bestehenden Regelungen in den Online-Banking-Bedingungen, um gegenüber Kunden von der Nutzung des von der Sofort angebotenen Bezahlverfahrens abzuraten oder davor zu warnen. Explizit werden beispielsweise Internetseiten der Sofort als „*falsche Adressen*“ bezeichnet, auf denen PIN und TAN nicht eingegeben werden dürfen.[215] Banken warnen ausdrücklich vor der

---

213 [redacted]

214 Bl. 1576 d.A.

215 Schreiben RA Kapellmann vom 24.03..2011, Anlage 2, Ausdruck der Internetseite der Raiffeisenbank Oberpfalz Süd eG, Bl. 1454 d.A.

Nutzung von „*Bezahlverfahren, bei denen die Zugangsdaten für das Online-Banking […] auf Seiten eingegeben werden, die nicht zur Bank gehören*“.[216]

242. Bankenunabhängige Bezahlverfahren im Internethandel müssen ihre Geschäftsmodelle nicht nur gegenüber Händlern vermarkten, sondern auch Kunden von der Sicherheit ihrer Dienstleistungen überzeugen. Hinweise (z.B. der Postbank), dass Verbraucher beim Bezahlen mit PIN und TAN nur Ihrer Bank oder Sparkasse vertrauen sollten und Warnungen an Verbraucher, dass neben den von Banken angebotenen Bezahlverfahren im Internethandelt auch „*Trittbrettfahrer Bezahlen mit Online-Überweisung anbieten, ohne Sicherheitsstandards der Banken und Sparkassen einzuhalten*“,[217] erfordern zusätzliche Anstrengungen derartiger Anbieter, um trotzdem im Wettbewerb zu bestehen.

C. Verfahrensgang

I. Ermittlungen

1. Ermittlungen bei der Deutschen Kreditwirtschaft und den einzelnen Spitzenverbänden

243. Nach Beschwerde der Sofort am 15.07.2010 hat die Beschlussabteilung das Kartellverfahren von Amts wegen eröffnet.

244. Zur Aufklärung des Sachverhalts hat die Beschlussabteilung von ihren Auskunftsrechten Gebrauch gemacht. Mit Schreiben vom 05.10.2010 hat sie von der DK die Übersendung von Unterlagen zur Erarbeitung der Sonderbedingungen für das Online-Banking verlangt. Am 24.09.2012 wurden die vier im Bereich des Zahlungsverkehrs (vgl. Rz. 13-17) in der DK zusammenarbeitenden Spitzenverbände ergänzend aufgefordert, dazulegen, wie der interne Verbandsprozess zur Erarbeitung der Sonderbedingungen für das Online-Banking abgelaufen ist.

245. In mehreren Gesprächen mit der Beschlussabteilung haben diese in der DK zusammengeschlossenen Spitzenverbände die Sach- und Rechtslage erörtert und diskutiert.

246. Im Verlauf des Verfahrens hat die DK verschiedene Schriftsätze übersandt, in denen Möglichkeiten zur Ausgestaltung der Zusammenarbeit zwischen Zahlungsauslösediensten

---

[216] Schreiben RA Kapellmann vom 24.03..2011, Anlage 2, Ausdruck der Internetseite der Volksbank Freiburg eG, Bl. 1455 d.A.

[217] Schreiben RA Kapellmann vom 24.03..2011, Anlage 1, Ausdruck aus dem Internetauftritt der Postbank vom 15.03.2011, Bl. 1444.

und kontoführenden Kreditinstituten skizziert worden sind. Keines dieser vorgestellten Modelle wurde als Verpflichtungszusage zur Lösung der kartellrechtlichen Bedenken abgegeben. Im Wesentlichen beruhen die bisherigen Vorschläge auf der Zulassung von Zahlungsauslösediensten durch die DK in Verbindung mit dem Abschluss bilateraler vertraglicher Vereinbarungen zwischen zugelassenen Zahlungsauslösediensten und den kontoführenden Kreditinstituten. Als weiterer möglicher Ansatz wurde die Erstellung einer eigenen Online-Banking-Seite dargestellt, über die Zahlungsauslösedienste die für den Betrieb ihres Geschäftsmodells notwendigen Informationen erlangen würden. Auch hierbei hätte die grundsätzliche Umsetzung durch die DK erfolgen sollen.

247. Mit Schreiben vom 29.07.2014 hat die Kanzlei Oppenländer, durch Übersendung anwaltlicher Vollmachten, angezeigt den BVR, den BdB, den VÖB und den DSGV zu vertreten.[218] Seit März 2016 wird der BdB von der Kanzlei Dentons Europe LLP vertreten.[219]

2. Ermittlungen bei Dritten

248. Am 20.06.2012 wurde die Buhl Data Service GmbH, Neunkirchen, aufgefordert, Angaben zu den von ihr angebotenen Produkten zu übersenden.

249. Die Beschlussabteilung hat von der Datev eG, Nürnberg, mit Auskunftsersuchen vom 17.01. 2013 und Auskunftsbeschluss vom 19.02.2013 Angaben zu deren Unternehmensorganisation und zu Produkten mit Bezug zum Online-Banking ermittelt.

250. Vor dem Zusammenschluss der genossenschaftlichen Rechenzentren Fiducia und GAD wurden diese getrennt ebenso wie die Finanzinformatik jeweils mit Auskunftsbeschluss vom 11.03.2014 zu den von ihnen angebotenen Kernbanksystemen und Produkten mit Bezug zum Online-Banking befragt.

II. Beiladungen

251. Sofort hat die Beiladung zum Verfahren am 16.11.2010 beantragt. Das Schreiben ist am 17.11.2010 im Bundeskartellamt eingegangen. Den Beteiligten zu 1.-4. sowie dem zum damaligen Zeitpunkt noch am Verfahren beteiligten VÖB wurde mit Schreiben an den Federführer der DK vom 23.10.2010 Gelegenheit zur Stellungnahme zu dem Beiladungsantrag gegeben. Mit Schreiben vom 30.11.2010 hat der DSGV für die DK

---

[218] Bl. 6200ff. d.A.
[219] Schreiben der Kazlei Dentons vom 04.03.2016.

Stellung genommen und keine Bedenken gegen die Beiladung geäußert.[220] Mit Beschluss vom 2.11.2010 wurde die Sofort zum Verfahren beigeladen.[221]

252. Die giropay GmbH hat die Beiladung zum Verfahren mit Schreiben vom 10.01.2011 beantragt.[222] Die Beteiligten zu 1.- 4., der VÖB sowie die Beigeladene zu 5. erhielten jeweils mit Schreiben vom 13.01.2011 Gelegenheit zur Stellungnahme.[223] Mit Schreiben vom 18.01.2011 hat der BdB für die DK Stellung genommen und keine Bedenken gegen die Beiladung geäußert.[224] Die Beigeladene zu 5. hat mit Schreiben vom 20.01.2011 ebenfalls eine Stellungnahme übersandt und keine durchgreifenden Einwände gegen die Beiladung geäußert.[225] Mit Beschluss vom 27.01.2011 wurde die giropay GmbH zum Verfahren beigeladen.[226]

III. Akteneinsicht

253. Die Beschlussabteilung hat den Beteiligten am 20.06.2011 mit Schreiben an den BdB als Federführer der DK und am 03.05.2012 an den BVR als Federführer der DK jeweils Einsicht in Teile der Verfahrensakte gewährt. Hierzu wurden Kopien der Verfahrensakte angefertigt und an die DK übersandt.[227]

254. Auch den Beigeladenen wurde Teilakteneinsicht gewährt. Der Beigeladenen zu 5. wurden am 01.07.2011 sowie am 03.05.2012 und der Beigeladenen zu 6. am 30.06.2011 und am 03.05.2012 Teile der Verfahrensakte in Kopie übersandt.

255. Nach Zustellung des Beschlussentwurfs am 23.09.2015 wurde den Beteiligten zu 1.-4. und dem VÖB am 21.12.2015 erneut ergänzende Akteneinsicht gewährt.[228]

IV. Beteiligung und Unterrichtung anderer Behörden

256. Am 25.03.2011 wurde die Europäische Kommission gem. Art. 11 Abs. 3 VO Nr. 1/2003 über die Verfahrenseinleitung unterrichtet.[229] Die Beschlussabteilung hat den Fall im

---

220 Bl. 685 d.A.
221 Bl. 694ff. d.A.
222 Bl. 840ff. d.A.
223 Bl. 846 und 848 d.A.
224 Bl. 862 d.A.
225 Bl. 870ff. d.A.
226 Bl. 919ff. d.A.
227 Bl. 1630 f. d.A. sowie Bl. 2985f. d.A.
228 Bl. 7509 d.A.
229 Verordnung (EG) Nr. 1/2003 des Rates vom 16.12.2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrages niedergelegten Wettbewerbsregeln, ABl. Nr. L 1/1.

Rahmen des Europäischen Wettbewerbsnetzwerks mit der Europäischen Kommission und den dort vertretenen nationalen Wettbewerbsbehörden mehrfach erörtert.

257. Am 09.10.2015 hat das Bundeskartellamt die Europäische Kommission gem. Art. 11 Abs. 4 VO 1/2003 sowie die Landeskartellbehörde Berlin über die geplante Entscheidung unterrichtet. Hierzu wurden der Entscheidungsentwurf sowie eine Zusammenfassung des Falles an die Europäische Kommission und an die Landeskartellbehörde Berlin übersandt.[230] Die Europäische Kommission hat hierzu Anmerkungen im Rahmen einer Telefonkonderenz gemacht, die in einer Email vom 19.11.2015 zusammengefasst übersandt wurden. Die LKB Berlin hat keine Stellungnahme abgegeben.

258. Die Beschlussabteilung hat im Verlauf des Verfahrens Kontakt zum Bayerischen Landesamt für Datenschutz[231] aufgenommen und hat in diesem Zusammenhang Fragen der datenschutzrechtlichen Zulässigkeit der Tätigkeit der Sofort erörtert.[232]

259. Auch mit Vertretern der Bundesbeauftragten für den Datenschutz wurden grundsätzliche Fragen zur Zulässigkeit von Zahlungsauslösediensten erörtert.

260. Im Rahmen des § 50c Abs. 2 Satz 1 GWB hat die Beschlussabteilung unter Wahrung der Geschäftsgeheimnisse der Beteiligten mit der Deutschen Bundesbank, dem Bundesministerium für Wirtschaft und Technologie, dem Bundesministerium der Finanzen und der Bundesanstalt für Finanzdienstleistungsaufsicht für das Verfahren relevante Erkenntnisse ausgetauscht.

V. Gewährung rechtlichen Gehörs

261. Am 28.07.2014 hat die DK eine Stellungnahme zur Vereinbarkeit der Sonderbedingungen für das Online-Banking mit dem deutschen und europäischen Kartellrecht übersandt. Darin stellt die DK dar, es habe sich bei den OBB nicht um den Beschluss einer Unternehmensvereinigung gehandelt. Es liege auch keine bezweckte oder bewirkte Wettbewerbsbeschränkung vor; die Sorgfaltspflichten hätten nicht den Zweck, den Wettbewerb zu beschränken, sondern Sicherheit im Online-Banking zu gewährleisten. Die Sicherheit des Online-Bankings sei ein legitimer Zweck und die Sorgfaltspflichten zu dessen Erreichen auch notwendig, angemessen und von der Rechtsprechung anerkannt. Gestützt wird die Argumentation damit, dass sich auch Europäische Zentralbank, BaFin

---

230 Vgl. Bl. 7159 d.A.
231 Sofort hat ihren Sitz im Zuständigkeitsbereich des Bayerischen landesamtes für Datenschutz.
232 Bl. 2991ff. d.A., Schreiben vom 23.05.2012.

und andere nationale europäische Zentralbanken gegen die Weitergabe von PIN und TAN ausgesprochen hätten. Die DK stellt dar, es handle sich bei den Sorgfaltspflichten um eine zulässige Nebenabrede zur Vereinbarung über die Nutzung des Online-Bankings. Die DK wendet sich gegen die Einschätzung, dass durch die gemeinsame Erstellung der Sorgfaltspflichten in den OBB der Markt für Bezahlverfahren im Internethandel verschlossen sei. Für den Fall, dass es sich bei der Abstimmung gemeinsamer Sorgfaltspflichten in den OBB doch um einen Beschluss der DK mit wettbewerbsbeschränkender Wirkung auf dem Markt für Bezahlverfahren im Internethandel handle, würde dies nicht den Tatbestand des Art. 101 Abs. 1 AEUV erfüllen, weil es sich um die Beschränkung rechtswidrigen Wettbewerbs handle. Aufgrund der dargestellten Gründe kommt die DK zu dem Ergebnis, die Beschlussabteilung könne das Verfahren nicht mit einer Entscheidung nach § 32 GWB abschließen. Die DK regt an, das Verfahren ohne Entscheidung zu beenden.[233]

262. Am 23.09.2015 hat die Beschlussabteilung den Beteiligten und auch dem VÖB den Entwurf des Beschlusses zur Stellungnahme übersandt. Die Frist für die Stellungnahme bis zum 02.11.2015 wurde auf Antrag der Beteiligten vom 13.10.2015 zunächst bis zum 28.12.2015 verlängert. Mit Schreiben vom 07.12.2015 wurde eine weitere Fristverlängerung zur Stellungnahme bis zum 22.02.2016 beantragt. Diesem Antrag hat die Beschlussabteilung entsprochen. Mit Schreiben vom 26.01.2016 haben die Beteiligten abermals die Verlängerung der Frist für die Stellungnahme bis zum 31.03.2016 beantragt. Diesen Antrag hat die Beschlussabteilung mit der Begründung abgelehnt, dass die Terminierung der zur Begründung des Antrags vorgebrachten notwendigen Gremiensitzungen für die Erarbeitung einer Stellungnahme bereits seit 5 Monaten hätte stattfinden können und die Beschlussabteilung nunmehr auch im Hinblick auf anhängige Gerichtsverfahren und die Übergangsregelungen der PSD II den Beschluss vorbereiten werde.

263. Die Beteiligten haben am 22.02.2016 zu dem Beschlussentwurf Stellung genommen und allgemein und ohne nähere Konkretisierung erklärt, dass die Beschlussabteilung ihre bisherige rechtliche und tatsächliche Argumentation zur kartellrechtlichen Zulässigkeit der Online-Banking-Bedingungen nicht hinreichend berücksichtigt habe. Sie verweisen bezüglich ihrer Beurteilung, warum es sich bei den Sorgfaltspflichten weder um eine

---

[233] Vgl. Bl. 6084ff. d.A.

bezweckte noch um eine bewirkte Wettbewerbsbeschränkung gehandelt hat, auf ihren Schriftsatz vom 28.07.2014.

264. Zuvor hatten die Beteiligten mit Schreiben vom 02.12.2015 den Entwurf eines öffentlich-rechtlichen Vertrags sowie den Entwurf einer geänderten Fassung der Sonderbedingungen für das Online-Banking zur Beendigung des Verfahrens übersandt. Von der Umsetzung dieser Änderungen in Form einer Zusage, welche die Beschlussabteilung nach § 32 GWB für bindend hätte erklären können, haben die Beteiligten Abstand genommen und den Vorschlag, der aus Sicht der Beschlussabteilung inhaltlich grundsätzlich geeignet gewesen wäre, die Beschränkung zu beseitigen, zurückgenommen.

265. Mit Schreiben vom 26.02.2016 hat der VÖB klargestellt, dass er als Mitglied der DK und als Verband an der Erarbeitung der AGB-Vertragswerke beteiligt war. Er vertrete aber nur in geringem Umfang Kreditinstitute, die Online-Bankng anbieten; er habe zu keinem Zeitpunkt die Nutzung der OBB gegenüber seinen Mitgliedern empfohlen. Auch in internen Arbeitskreisen seien die OBB lediglich als Teil der Regelungen ausgehändigt worden, die im Rahmen der Umsetzung der Zahlungsdiensterichtlinie erarbeitet worden seien.

266. Mit Schreiben vom 04.03.2016 für den BdB (Eingang am 08.03.2016) sowie für die anderen Beteiligten (Eingang am 07.03.2016), haben die Beteiligten zu 1.-4. vorsorglich die Aussetzung der sofortigen Vollziehung des Beschlusses beantragt.

267. Mit Schreiben vom 07.06.2016 und ergänzender Email vom 15.06.2016 hat die Beschlussabteilung den Beteiligten sowie den Beigeladenen mitgeteilt, dass sie erwägt, die Verfügung bei unverändertem Sachverhalt auch auf § 19 Abs. 3 GWB zu stützen. Den Verfahrensbeteiligten wurde eine Frist zur Stellungnahme bis zum 21.06.2016 gewährt.

268. Mit Schreiben vom 10.06.2016 und 20.06.2016 nehmen die Kanzlei Oppenländer[234] für die Beteiligten zu 1.-3. und die Kanzlei Detons[235] für die Beteiligte zu 4. nicht inhaltlich Stellung, rügen jedoch die unbestimmte Formulierung des Missbrauchsvorwurfs. Dentons verweist ergänzend auf ihren Antrag vom 04.03.2016 zur Aussetzung der sofortigen Vollziehung nach Erlass des Beschlusses.

---

[234] Vgl. Bl. 7621f. und 7625f. d.A.
[235] Vgl. Bl. 7619f. und 7629f. d.A.

D. Rechtliche Würdigung

269. Der Beschluss zur Erstellung einheitlicher Sonderbedingungen für das Online-Banking durch die DK sowie die Beschlüsse der Beteiligten zu 2. - 4. zur verbundweiten einheitlichen Nutzung der OBB durch die ihnen angeschlossenen Mitglieder verstoßen als Beschlüsse von Unternehmensvereinigungen unter dem Aspekt der Koordinierung des Marktverhaltens der in den Verbänden zusammengeschlossenen Kreditinstitute gegen Art. 101 Abs. 1 AEUV, § 1ff. GWB, soweit sie in Ziff. 7.2 Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich OBB, Ziff. 10.2.1 Abs. 5 vierter Spiegelstrich OBB Kunden[236] Sorgfaltspflichten auferlegen, die eine Weitergabe von Personalisierten Sicherheitsmerkmalen an Zahlungsauslösedienste im Internethandel, z.B. auf Online-Händlerseiten, ausschließen. Die Umsetzung des dahinter stehenden wirtschaftlichen Gesamtplans zur Behinderung der Tätigkeit von Zahlungsauslösediensten durch Errichtung rechtlicher Marktzutrittsschranken, stellt zudem – selbst im Falle einer unterstellten Zulässigkeit der Koordinierung – eine unbillige Behinderung von anderen Unternehmen und damit ein missbräuchliches Verhalten im Sinne von § 19 Abs 3 Satz 1 i.V.m. Abs. 1, Abs. 2 Nr. 1 GWB dar.

270. Der Beschluss der OBB durch die DK sowie die Beschlüsse der Beteiligten zu 2. - 4. zur Empfehlung der Nutzung der OBB durch ihre Mitglieder im Vertragsverhältnis zu deren Kunden ist eingebettet in eine strategisch-konzeptionelle Überlegung der DK zum Umgang mit Bezahlverfahren im Internethandel. Die im Wettbewerb stehenden Kreditinstitute koordinieren durch ihre Spitzenverbände ihr Marktverhalten und die Behinderung von bankenunabhängigen Zahlugsauslösediensten. Der Gesamtplan basiert auf den seit Jahrezehnten gemeinsam beschlossenen und praktizierten AGB-Vertragswerken, die entsprechend der festgestellten aktuellen Notwendigkeit im Zeitverlauf angepasst worden sind. Dabei definiert die DK jeweils, was als Gefährdungslage (z.B. Gefahren durch Internetbrowser, Zahlungsauslösedienste) anzusehen ist, und schafft entsprechende Regelungen, um einerseits Sicherheitsbedenken zu addressieren, zugleich jedoch den Wettbewerb für ihre Mitgliedsverbänden und die diesen angeschlossenen Kreditinstitute vorteilhaft zu gestalten. Zu dem Gesamtplan der in der DK repräsentierten Kreditwirtschaft gehört die Erarbeitung eines strategischen Konzeptes zum Umgang mit Zahlungsauslösediensten

---

[236] Der Begriff des Kunden bezieht sich auf die Vertragsbeziehung zu einem kontoführenden Kreditinstitut. Der in den Online-Banking-Bedingungen der Kreditwirtschaft verwendete Begriff des Nutzers des Online-Bankings wird zur Vereinfachung und weil diese Unterscheidung für den kartellrechtlichen Vorwurf unerheblich ist, nicht differenziert benutzt.

(Intermediärskonzept). Die Spitzenverbände haben die beschlossenen OBB gegenüber ihren Mitgliedern zur Verwendung empfohlen. Diese Empfehlungen sind auf breiter Basis umgesetzt worden. Auf der Basis dieser einheitlichen Regelungen und der in der DK erarbeiteten Kommunikationsstrategien haben Kreditinstitute gegenüber Kunden vor der Nutzung von Zahlungsauslösedienste gewarnt. Die DK hat auf der Basis der beschlossenen OBB gegenüber der Presse die angebliche Rechtswidrigkeit der Nutzung von bankenunabhängigen Zahlungsauslösediensten wie der Sofort thematisiert. Auch die Klagen vor Gerichten wegen einer vermeintlichen Verleitung der Kunden zum Vertragsbruch oder die Verunsicherung von Verbrauchern durch das Angebot von als rechtswidrig klassifizierten bankenunabhängigen Zahlungsauslösediensten resultieren aus diesem Gesamtkonzept der DK. Die mit den Sorgfaltspflichten korrespondierenden Haftungsregelungen sind in den OBB so formuliert, dass es für den Kunden, der einen Zahlungsauslösedienst in Anspruch nimmt, nicht ohne Weiteres erkennbar ist, unter welchen Voraussetzungen sein Handeln zu negativen haftungsrechtlichen Konsequenzen führen kann.

271. Die beschlossenen Online-Banking-Bedingungen der Kreditwirtschaft enthalten verschiedene Sorgfaltspflichten, welche von Kunden zu beachten sind. Da sich der kartellrechtliche Vorwurf nur auf Teile dieser Sorgfaltspflichten bezieht, werden sonstige Regelungen in der rechtlichen Beurteilung nicht geprüft. Ziff. 7.2 Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich OBB, Ziff. 10.2.1 Abs. 5 vierter Spiegelstrich jedoch verstoßen gegen Art. 101 Abs. 1 AEUV, § 1ff. GWB, soweit sich das Verbot der Eingabe Personalisierter Sicherheitsmerkmale außerhalb gesondert mitgeteilter Online-Banking-Zugangskanäle auf alle Anbieter erstreckt, die dem Käufer von Waren oder Dienstleistungen im Internethandel die Nutzung des Online-Bankings ermöglichen (sog. Zahlungsauslösedienste).

272. Die kartellrechtliche Beurteilung erfolgt auf der Grundlage von Art. 101 Abs. 1 AEUV, wonach alle Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen verboten sind, welche den Handel zwischen Mitgliedstaaten zu beeinträchtigen geeignet sind und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des Binnenmarkts bezwecken oder bewirken. Die Beurteilung auf der Grundlage von § 1ff. GWB, wonach Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken, verboten sind, kommt zu keinem abweichenden Ergebnis.

273. Der Beschluss der DK sowie die Beschlüsse der Beteiligten zu 2.-4. (dazu unter I) bezwecken den Ausschluss von bankenunabhängigen Zahlungsauslösediensten als Wettbewerber auf dem Markt für Bezahlverfahren im Internethandel (dazu unter B.II.3). Sie stellen keine Nebenabrede zu einer ansonsten kartellrechtlich zulässigen Hauptmaßnahme dar. Sie sind auch nicht vom Kartellverbot gem. Art. 101 Abs. 3 AEUV freigestellt (dazu unter IV). Die Beteiligten haben keine mit den beschlossenen Klauseln erzielten Effizienzgewinne nachgewiesen. Zumindest aber wurde von den Beteiligten nicht hinreichend dargelegt, dass die Beschränkungen des Wettbewerbs für die Erreichung eines angestrebten Effizienzgewinns unerlässlich sind. Die von den Beteiligten mit der Beschlussabteilung diskutierten Alternativen zum Umgang mit Zahlungsauslösediensten auf dem Markt für Bezahlverfahren im Internethandel zeigen vielmehr konkrete Möglichkeiten zum Umgang mit solchen Dienstleistern auf, die einerseits Sicherheit gewährleisten und andererseits den Wettbewerb auf dem Markt weniger beschränken.

274. Der Gesamtplan der Beteiligten zu 1. – 4, der als einen Baustein die rechtswidrigen Beschlüsse von DK und den Beteiligten zu 2.-4. zur Umsetzung des Gesamtkonzeptes zur Behinderung von Zahlungsauslösediensten enthält, stellt darüber hinaus auch eine unbillige Behinderung eines anderen Unternehmens im Sinne von § 19 Abs. 3 Satz 1 i.V.m. § 19 Abs. 1, Abs. 2 Nr. 1 GWB dar (dazu unter V).

I. Beschluss einer Unternehmensvereinigung

275. Die einheitliche Erstellung und Anwendung der in den Online-Banking-Bedingungen formulierten Sorgfaltspflichten (Ziff. 7.2 Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich, Ziff. 10.2.1 Abs. 5, vierter Spiegelstrich) beruht auf Beschlüssen von Untenrehmensvereinigungen im Sinne von Art. 101 Abs. 1 AEUV.

1. Bei der DK und den Spitzenverbänden der Kreditwirtschaft handelt es sich jeweils um Unternehmensvereinigungen

276. Die DK ist eine Unternehmensvereinigung. Auch die Spitzenverbände der DK handeln als Vereinigungen ihrer wirtschaftlich tätigen Mitglieder, bei denen es sich zumindest mittelbar um Kreditinstitute und damit um Unternehmen im Sinne des Wettbewerbsrechts handelt.

277. An die Organisationsform der Unternehmensvereinigung stellen weder europäisches noch deutsches Kartellrecht hohe Anforderungen. Die Vereinigung muss ein gewisses Maß an gemeinschaftlicher Organisation aufweisen, ohne dass hierfür eine bestimmte Rechtsform

erforderlich ist.[237] Es kommt nicht darauf an, dass es sich bei der Unternehmensvereinigung selbst um ein Unternehmen handelt. Entscheidend ist vielmehr, dass ihre Mitglieder unmittelbar oder mittelbar selbst Unternehmen sind. Auch Vereinigungen, deren Mitglieder selbst Vereinigungen von Unternehmen sind, fallen hierunter.[238] Der Begriff der Unternehmensvereinigung orientiert sich nicht primär an der Organisations- und Rechtsform einer Vereinigung, sondern ist vor dem Hintergrund der Erweiterung des Anwendungsbereichs des Kartellverbots zu sehen. Art. 101 Abs. 1 AEUV gilt für Unternehmensvereinigungen, deren eigene Tätigkeit oder die Tätigkeit der in ihr zusammengeschlossenen Unternehmen auf die Folgen abzielt, welche das Kartellverbot unterbinden will.[239]

278. Bei der DK - als Gesellschaft bürgerlichen Rechts - handelt es sich um eine Unternehmensvereinigung, die im Interesse ihrer Mitglieder tätig wird und über ein hohes Maß gemeinschaftlicher Organisation verfügt. Die DK verfolgt das Ziel einer gemeinsamen Meinungs- und Willensbildung der kreditwirtschaftlichen Verbände in Deutschland in bankrechtlichen, bankpolitischen und bankpraktischen Fragen. Sie vertritt die gemeinsamen Standpunkte der Spitzenverbände gegenüber Gesetzgeber, Regierung, Behörden sowie bank- und finanzwirtschaftlichen Institutionen auf nationaler, europäischer und internationaler Ebene.[240] Für die Erreichung gemeinsamer Ziele werden in den hierfür zuständigen Gremien der DK, z.B. in Arbeitskreisen, gemeinsame Positionen zwischen den Spitzenverbänden der Kreditwirtschaft erarbeitet.

279. Mitglieder der DK sind die Spitzenverbände der deutschen Kreditwirtschaft, bei denen es sich ebenfalls um Unternehmensvereinigungen handelt. Die von den Spitzenverbänden der DK vertretenen Mitglieder sind Unternehmen im Sinne des Kartellrechts. Sowohl der BVR als auch der BdB werden im Rahmen der Interessenvertretung für die ihnen angeschlossenen Mitglieder tätig, bei denen es sich um Kreditinstitute handelt. Im Falle des BVR sind dies die Genossenschaftsbanken.[241] Auch der BdB vertritt unmittelbar die Interessen der ihm angeschlossenen Kreditinstitute. Die Regionalverbände gehören

---

237 Zimmer in: Immenga/Mestmäcker, Wettbewerbsrecht, Bd. 2 GWB, Teil 1, 5. Aufl., § 1, Rz. 76.

238 Hengst in: Langen/Bunte, Kartellrecht Kommentar, Bd. 2, Europäisches Kartellrecht, 12. Aufl., Art. 101 AEUV, Rz. 68; auch öffentlich-rechtliche Körperschaften können Unternehmensvereinigungen sein, soweit sie über ihre öffentlich-rechtliche Legitimation hinausgehend in den Wettbewerb ihrer Mitglieder untereinander oder im Verhältnis zu Dritten eingreifen.

239 EuGH, Urteil vom 08.11.1983, C-96/82, IAZ, Rz. 20.

240 http://www.die-deutsche-kreditwirtschaft.de/dk/die-deutsche-kreditwirtschaft.html, Stand 16.12.2014.

241 http://www.bvr.de/Wer_wir_sind/Unsere_Aufgaben, Stand 15.12.2014.

ebenfalls zu den Mitgliedern des BdB.[242] Der DSGV vertritt die Interessen der regional tätigen Sparkassen mittelbar. Seine unmittelbaren Mitglieder sind die Regionalverbände des Sparkassenwesens, bei denen es sich um Körperschaften des öffentlichen Rechts handelt. Die Sparkassen und ihre kommunalen Gewährträger unterhalten Pflichtmitgliedschaften[243] in den jeweils für sie zuständigen Regionalverbänden. Die Regionalverbände übernehmen die Interessenvertretung der Sparkassen auf regionaler Ebene gegenüber Landesregierungen und Landesbehörden.[244]

280. Die einzelnen Kreditinstitute aller beteiligten Verbände sind Unternehmen im Sinne des Art. 101 Abs. 1 AEUV. Sie erbringen Bankdienstleistungen gegen Entgelt und werden damit wirtschaftlich tätig.

2. Die Erstellung und Anwendung gemeinsamer Online-Banking-Bedingungen erfolgte durch Beschlüsse

281. Die Online-Banking-Bedingungen wurden durch Beschlüsse von Unternehmensvereinigungen vereinbart. Dies gilt sowohl für den Beschluss auf der Ebene der DK als auch für die Umsetzungsbeschlüsse in den jeweiligen Spitzenverbänden (Beteiligte zu 2.-4.), die auch die an die jeweiligen Mitgliedsinstitute gerichteten Empfehlungen zur Nutzung der OBB umfassen.

282. Unter Beschlüssen sind alle Rechtsakte zu verstehen, durch welche Unternehmensvereinigungen ihren Willen bilden, unabhängig davon, wie der Beschluss zustande gekommen ist. Nicht unterschieden wird in diesem Zusammenhang, ob es z.B. interne Regeln zur Beschlussfassung gegeben hat und ob alle Mitglieder der Unternehmensvereinigung an den Beschlüssen, die auf Folgen abzielen, welche durch das Kartellverbot unterbunden werden sollen, beteiligt waren.[245] Für die kartellrechtliche Beurteilung ist auch der faktische Grad der Verbindlichkeit, z.B. ob mit der Nichtbeachtung durch die Mitgliedsunternehmen Sanktionen verbunden sind, nicht entscheidend. Es reicht der ernsthafte Wille der Unternehmensvereinigung aus, das

---

242 http://bankenverband.de/bankenverband/mitglieder, Stand 15.12.2014.

243 Lediglich freie Sparkassen werden auf freiwilliger Basis Mitglieder des jeweiligen Regionalverbandes. (http://www.dsgv.de/de/sparkassen-finanzgruppe/organisation/verbaende.html, Stand 15.12.2014).

244 http://www.dsgv.de/de/sparkassen-finanzgruppe/organisation/verbaende.html. Stand 22.09.2015.

245 BGH, 14.08.2008, „Lottoblock", zitiert nach juris, Rz. 21 m.w.N. zur Rechtsprechung der europäischen Gerichte.

Verhalten ihrer Mitglieder auf dem Markt zu koordinieren, um das Vorliegen eines Beschlusses zu bejahen.[246]

Die Beteiligten argumentieren unter Verweis auf die Rechtsprechung des BGH, dass allein die Empfehlung von Geschäftsbedingungen durch eine Vereinigung nicht ausreiche, einen Koordinierungswillen anzunehmen.[247] Den kartellrechtlichen Tatbestand erfüllt aber auch eine von einer Unternehmensvereinigung ausgesprochene Empfehlung, wenn diese, wie dies vorliegend geschehen ist, von den Mitgliedern übernommen und umgesetzt wurde.[248] Nach dem Ergebnis der Ermittlungen handelt es sich in Bezug auf die DK tatsächlich nicht um eine bloße Empfehlung der DK (dazu unter a)), da die Spitzenverbände gemäß ihrer Mandate die Erarbeitung der Bedingungen durchgeführt haben und die Kreditinstitute die Onlinebanking-Bedingungen in der erarbeiteten Form übernommen haben und diese anwenden (dazu unter b)).

a) Keine bloße Empfehlung der DK

283. Die von der DK und ihren Spitzenverbänden gemeinsam erarbeiteten Online-Banking-Bedingungen stellen keine bloßen Empfehlungen für Kreditinstitute dar. Die Online-Banking-Bedingungen wurden mit dem Ziel erarbeitet, eine einheitliche Anwendung in der Praxis durch die den Spitzenverbänden angeschlossenen Kreditinstitute auf möglichst breiter Basis zu erreichen. Dementsprechend tritt auch die DK gegenüber Dritten auf.

284. Bei der Erarbeitung der Sorgfaltspflichten verfolgte die DK das Ziel der Schaffung eines einheitlichen Standards zum Umgang mit Zahlungsauslösediensten für die gesamte Kreditwirtschaft. Die Notwendigkeit zur Überarbeitung der Sorgfaltspflichten leitete die DK aus der Beobachtung ab, dass in Folge von kriminellen Phishing-Angriffen auf das Online-Banking einzelne Kreditinstitute Mitte des Jahres 2005 dazu übergingen, die Sorgfaltspflichten in den Online-Banking-Bedingungen diesbezüglich *eigenständig* zu konkretisieren.[249] In der DK bestand zudem Einigkeit über eine einheitliche Umsetzung der Anforderungen aus der Zahlungsdiensterichtlinie in den AGB-Vertragswerken.

285. Regelungen im Online-Banking wurden stets in der DK gemeinsam als Branchenstandard erarbeitet. Wie die DK darstellt, handelt es sich bei Sicherheitsfragen um einen zentralen

---

246 Krauß in: Langen/Bunte, § 1 GWB, Rz. 86, m.w.N. zur nationalen und europäischen Rechtsprechung.
247 BGH, Beschluss vom 22.03.1994, KVR 23/93.
248 EuGH, Urteil vom 08.11.1983, C-96/82, zitiert nach Juris, Rz. 20f.; Krauß in: Langen/Bunte, § 1 GWB, Rz. 86.
249 Schreiben der DK, 02.11.2010, Bl. 484 d.A.

Aspekt des Online-Banking. Soweit die technische Sicherheit in Einzelfällen in Frage steht, geht die DK davon aus, dass dies das Vertrauen der Bankkunden insgesamt erschüttern würde. Daher sieht die DK es als unerlässlich an, hohe Sicherheitsstandards anzustreben, um das Vertrauen der Kunden in das Online-Banking unterschiedlicher Kreditinstitute nicht durch Sicherheitsprobleme eines einzelnen Kreditinstituts im Rahmen des Online-Bankings in Frage zu stellen.[250]

286. Die Arbeiten an den Online-Banking-Bedingungen in den verschiedenen Arbeitsgruppen der DK dauerten mehrere Jahre, in denen immer wieder über die einzelnen Spitzenverbände der DK Rückkopplungen der Arbeitsergebnisse zu den angeschlossenen Instituten stattfanden (vgl. Rz. 197ff.). Dass Institute parallel die Entwicklung eigener Online-Banking-Bedingungen betrieben, war schon aufgrund der Mandatierung der Spitzenverbände, die sich aus den satzungsgemäßen Aufgaben oder entsprechenden Gremienbeschlüssen zur Erarbeitung der Regelwerke ableitet, nicht zu erwarten und fand auch tatsächlich nicht statt und war gerade nicht gewollt (vgl. Rz. 284).

287. Entgegen der Ansicht der Beteiligten, wonach die Musterbedingungen es dem einzelnen Institut überlassen, welche Internetseiten es „*als Zugangskanal zum Online-Banking sicherheitspolitisch akzeptiert*“,[251] zielen die OBB darauf ab, die Grundlage für eine einheitliche Anwendung durch alle Kreditinstitute zu bilden. Dies folgt aus der konkreten Zielsetzung der in der DK an der Erarbeitung der Online-Banking-Bedingungen beteiligten Verbände (vgl. Rz. 284) sowie der Aufgabenverteilung bei der Organisation des Online-Banking, die einer individuellen Zulassung einzelner Angebote durch einzelne Kreditinstitute gerade entgegensteht. Es widerspräche der Ratio der Beteiligten, einheitliche AGB-Vertragswerke für die gesamte Kreditwirtschaft zu erarbeiten und die Rahmenbedingungen für das Online-Banking auszugestalten sowie Verantwortung für die (Fort-) Entwicklung von Sicherungsverfahren zu übernehmen, wenn einzelne Kreditinstitute grundsätzlich aufgefordert wären, selbständig zu entscheiden, welche Internetseiten sie als hinreichend sicher zulassen, sodass auf diesen PIN und TAN eingeben werden dürften. Gerade weil Fragestellungen im Zusammenhang mit dem Online-Banking eine besondere Komplexität beinhalten, werden die Beteiligten für die angeschlossenen Kreditinstitute tätig und füllen den Rahmen aus, in dem das Online-Banking abläuft.

---

250 Schreiben der DK, 02.11.2010, Bl. 478 d.A.
251 Schriftsatz Oppenländer Rechtsanwälte, 29.07.2014, Bl. 6151 d.A.

288. Für Zulassungsverfahren zur Beurteilung der Sicherheit von Internetseiten und Zahlungsauslösediensten fehlen den angeschlossenen Kreditinstituten zudem mehrheitlich die Ressourcen und das Know-how. Dies zeigt sich auch daran, dass Sparkassen und Genossenschaftsbanken sowie verschiedene Banken des BdB bei der technischen Realisierung des Online-Bankings externe Rechenzentren der jeweiligen Bankengruppen in Anspruch nehmen müssen (vgl. Rz. 106 ff.), die ein vollständiges technisches Dienstleistungspaket für den Bankbetrieb anbieten. Diese Institute sind nicht allein, sondern nur durch die Tätigkeit von Rechenzentren, die ihrerseits gerade wiederum in den hier relevanten Arbeitskreisen der DK an der Formulierung der Sorgfaltspflichten vertreten waren, in der Lage, Entscheidungen über die Sicherheit von Angeboten im Bereich des Online-Bankings zu treffen.

289. Dass es sich aus Sicht der DK auch bei den bis 2009 geltenden Online-Banking-Bedingungen um einen Branchenstandard und damit um weit mehr als eine bloße Empfehlung gehandelt hat, ergibt sich auch aus dem Umgang der DK mit den Online-Banking-Bedingungen gegenüber Dritten. Gegenüber der L'Tur, die einen Zahlungsauslösedienst mit Eingabe von PIN und TAN und damit unter Nutzung des Online-Banking-Zugangs durch den Kunden eingeführt hatte, verwies die DK auf die im deutschen Kreditgewerbe Verwendung findenden Online-Banking-Bedingungen, die eine Verpflichtung des Bankkunden normieren, dafür Sorge zu tragen, dass keine andere Person Kenntnis von PIN und TAN erlangt (vgl. Rz. 174).[252] Die DK kommunizierte gegenüber L'Tur gerade nicht, dass es sich bei den Bedingungswerken nur um ein von den Verbänden erarbeitetes „Muster" handelte, das ggf. nur von einem Teil der Kreditinstitute tatsächlich in dieser Form verwendet wird, so dass Kreditinstitute die Tätigkeit von L'Tur zulassen können. Die DK nimmt vielmehr ihre Funktion als Interessenvertretung der deutschen Kreditinstitute so wahr, dass nach außen deutlich wird, dass die DK auf einen grundsätzlich branchenweit gültigen Beschluss Bezug nimmt und diesen auch durchzusetzen gewillt ist. Dies zeigt, dass es sich bei den Sorgfaltspflichten tatsächlich um einen Branchenstandard handelt und die DK auf dieser Basis die Interessen aller angeschlossenen Kreditinstitute vertritt.[253]

---

[252] [redacted]

[253] Auch gegenüber der zur Deutschen Bank gehörenden Moneyshelf AG verweist die DK darauf, dass die angebotenen Produkte des Unternehmens dazu führen, dass Kunden dazu verleitet werden, gegen die in den Online-Banking-Bedingungen 2000 formulierten Sorgfaltspflichten zu verstoßen, indem sie die geheim zu haltenden PIN und TAN an Moneyshelf bzw. die Deutsche Bank AG weitergeben (vgl. Rz. 175, [redacted]). Eine Einschränkung, dass dieser Verstoß nur Kunden derjenigen Kreditinstitute betrifft, die die von der DK erarbeiteten Online-Banking-Bedingungen tatsächlich verwenden, fehlt auch hier. Ebenso verweist die DK gegenüber

290. Auch das Produkt sofortueberweisung.de stellt die DK uneingeschränkt als Verstoß gegen vertragliche Vorgaben, nämlich die Pflicht des Kunden zur Geheimhaltung von PIN und TAN, dar. Gegenüber der zum damaligen Zeitpunkt noch als Promido Internet GmbH firmierenden Betreiberin des Systems stellte die DK klar, dass die Bedenken gegen sofortueberweisung.de von allen in der DK vertretenen Verbänden gemeinsam getragen werden.[254] Eine Differenzierung zwischen Kreditinstituten, die solche Bedingungen verwenden, und denen, die andere Bedingungen nutzen, wird nicht gemacht.

291. Schließlich ergibt sich aus der Kommunikation der DK gegenüber externen Dritten, dass die Beteiligten auch nach Erarbeitung der Online-Banking-Bedingungen im Jahre 2009 von einer einheitlichen Anwendung der Online-Banking-Bedingungen in der Praxis ausgegangen sind. Wie die DK gegenüber Stiftung Warentest im Jahre 2010 darstellt, sehen die Bedingungen zum Online-Banking der Kreditinstitute einen einheitlichen Umgang mit PIN und TAN vor. Die DK führt hierzu aus:

„Werden jedoch die geheim zu haltenden Zugangsdaten auf der Internetseite eines Online-Bezahlverfahrens eingegeben, das nicht von seinem Kreditinstitut hierzu zugelassen ist (z.B. bei Sofortüberweisung.de), verstößt er damit gegen die Online-Banking-Bedingungen.“[255]

292. Schließlich belegt auch die Klage der giropay GmbH vor dem Landgericht Köln, dass in Bankenkreisen allgemein anerkannt ist, dass die Online-Banking-Bedingungen einen Branchenstandard darstellen. giropay, die unter Bezugnahme auf die Sorgfaltspflichten in den Online-Banking-Bedingungen Klage gegen die Sofort vor dem LG Köln erhoben hat, begründet die Klage damit, dass die Tätigkeit der Sofort eine Verleitung zum Vertragsbruch darstelle, da Kunden hierdurch gegen ihre in den Online-Banking-Bedingungen formulierten Sorgfaltspflichten verstoßen.[256] Die Möglichkeit abweichender Regelungen einzelner Kreditinstitute wird erst gar nicht erörtert.

---

der T-Online International AG auf die generell bestehenden Sorgfaltspflichten der Kunden des Online-Banking, die gegen die Nutzung des von T-Online angebotenen Dienstes sprechen (vgl. Rz. 176, [redacted]). Das Angebot von T-Online wertet die DK als Verstoß gegen geltendes Recht und eine an die Kunden des Online-Bankings gerichtete Aufforderung zum Vertragsbruch (vgl. [redacted]).

254 [redacted].

255 [redacted]

256 Klage der giropay vor dem LG Köln vom 08.10.2009, S. 18.

b) Übernahme und Anwendung der Online-Banking-Bedingungen durch die Kreditinstitute

Die Mitgliedsinstitute der in der DK zusammenarbeitenden Beteiligten zu 2.-4. haben die Online-Banking-Bedingungen – durch eigene Beschlüsse, die wiederum keine bloßen Empfehlungen darstellen - umgesetzt. Wie oben dargestellt (vgl. Rz. 219 ff.), finden die Online-Banking-Bedingungen im Bereich der Sparkassen und Genossenschaftsbanken flächendeckend Anwendung im Rahmen der Geschäftsverbindung gegenüber Kunden. Auch unter den privaten Banken haben jedenfalls die größten Mitgliedsinstitute (z.B. Deutsche Bank, Commerzbank, HypoVereinsbank, ING DiBa) die Online-Banking-Bedingungen und die entsprechenden Sorgfaltspflichten übernommen und auf ihren Internetseiten eingestellt.

II. Wettbewerbsbeschränkung

293. Die von der DK erarbeiteten und von den angeschlossenen Kreditinstituten verwendeten Sorgfaltspflichten stellen eine Koordinierung auf dem Markt für Privatgirokonten dar, die eine Beschränkung des Wettbewerbs auf dem bundesweiten Markt für Bezahlverfahren im Internethandel bezwecken und bewirken. Sie verhindern, dass Kunden Personalisierte Sicherheitsmerkmale im Rahmen der Nutzung bankenunabhängiger Zahlungsauslösedienste eingeben dürfen. Es handelt sich damit um eine Beschränkung des Wettbewerbs auf einem Drittmarkt (Markt für Bezahlverfahren im Internet). Derartige Drittmarktbeschränkungen sind ebenfalls vom Kartellverbot (Artikel 101 AEUV und § 1 GWB) erfasst. Die gemeinsam festgelegten Sorgfaltspflichten sind geeignet, den Handel zwischen Mitgliedstaaten zu beeinträchtigen.

1. Der sachlich relevante Markt

294. Die Grundlage der wettbewerblichen Beurteilung bildet der relevante Markt (marktbezogene Betrachtung), der zunächst in sachlicher Hinsicht abzugrenzen ist. Ausgangspunkt der Marktabgrenzung ist das Bedarfsmarktkonzept. Danach bilden sämtliche Erzeugnisse, die sich nach ihren Eigenschaften, ihrem wirtschaftlichen Verwendungszweck und ihrer Preislage so nahe stehen, dass der verständige Verbraucher sie für die Deckung eines bestimmten Bedarfs geeignet, in berechtigter Weise abwägend miteinander vergleicht und als gegeneinander austauschbar ansieht,

einen einheitlichen sachlichen Markt.[257] Maßgebend ist die tatsächliche Handhabung durch die Abnehmer, wobei auf den verständigen Durchschnittsnachfrager abzustellen ist.[258] Eine nur von wenigen Nachfragern angenommene Austauschbarkeit reicht nicht.[259]

295. Die Koordinierung des Verhaltens der Spitzenverbände der DK durch die einheitliche Definition von Sorgfaltspflichten in den OBB betrifft zunächst das Verhältnis der Anbieter Online-Banking-fähiger Girokonten zu ihren Kunden und damit den im Rahmen dieses Verfahrens nicht weiter abzugrenzenden Markt für Girokonten. Die Koordinierung bezweckt eine Beschränkung des Wettbewerbs auf dem Markt für Bezahlverfahren im Internet. Auf diesem Markt stehen sich Anbieter von abgesicherten Bezahlverfahren im Internethandel und solche Händler gegenüber, die ihre Waren oder Dienstleistungen über das Internet vertreiben und dabei die Abwicklung von Kaufpreiszahlungen über abgesicherte Bezahlverfahren nachfragen.[260]

296. Dem Markt für Bezahlverfahren im Internet zuzurechnen sind daher alle Verfahren, bei denen der Händler über die reine Abwicklung des Zahlungsverkehrs hinaus weitere Leistungen, etwa zum Schutz gegen Forderungsausfälle, nachfragt.[261] Nicht zum Markt gehören dagegen Bezahlverfahren, bei denen der Händler ohne Leistungen eines Dienstleisters sich darauf beschränkt, auch außerhalb des Internethandels verfügbare Zahlungsmöglichkeiten wie das Lastschrift- oder Überweisungsverfahren zu nutzen.

a) Rahmenbedingungen für Bezahlverfahren im Internethandel

297. Neben stationärem Handel und dem Distanzhandel hat sich in den letzten Jahren der Internethandel (E-Commerce) als weiterer Vertriebsweg mit hohen Wachstumsraten etabliert. Im Internethandel, bei dem sich Kunde und Händler nur in Ausnahmefällen

---

[257] Ständige Rspr.; vgl. BGH, Beschluss vom 05.10.2004, WRP 2004, 1502, 1504 – Staubsaugerbeutelmarkt; BGH, Urteil vom 19.03.1996, WuW/E BGH 3058, 3062 – Pay-TV-Durchleitung.

[258] Ständige Rspr., vgl. nur BGH, Beschluss vom 22.09.1987, WuW/E BGH 2433, 2436 – Gruner+Jahr / Zeit; KG, Beschluss vom 14.04.1978, WuW/E OLG 1983, 1984 m.w.N. – Rama-Mädchen; Paschke in: Frankfurter Kommentar, Kartellrecht, IV §§ 1-23 GWB, § 19 Rz. 74.

[259] Ständige Rspr., vgl. KG, Beschluss vom 19.03.1975, WuW/E OLG 1599, 1602 – Vitamin B 12; KG, Beschluss vom 05.01.1976, WuW/E OLG 1645, 1649 – Valium; Paschke in: Frankfurter Kommentar, aaO., § 19 Rz. 75. Zu dieser Rechtsfigur im common law vergleiche die Rechtsprechung in Fardell v. Potts in A.P. Herbert, Uncommon Law, 3. Auflage, 1980, Seite 7, 8 ff.

[260] Der Markt bezieht sich damit nicht auf das Vertragsverhältnis zwischen dem Händler, der im Internet seine Waren vertreibt, und dem Kunden, der ein Bezahlverfahren auswählt, um den Rechnungsbetrag zu bezahlen.

[261] Zum Beispiel kann ein Händler einen Dienstleister mit der Rechnungserstellung, dem Zahlungsmanagement und dem Inkasso bei Zahlungsstörungen beauftragen. Derartige Leistungen sind dem Markt zuzurechnen, wohingegen die Nutzung des Überweisungs- bzw. Lastschriftverfahrens ggf. ergänzt um unternehmens**intern** erbrachte Leistungen zur Verringerung des Ausfallrisikos nicht einzubeziehen sind.

persönlich begegnen oder in telefonischen Kontakt miteinander treten und die Zug-um-Zug-Erfüllung der vertraglichen Pflichten beim Kauf von Waren in der Regel nicht möglich ist, kommt dem Bezahlvorgang aus Sicht des Händlers eine besondere Bedeutung zu.

298. Das Hauptrisiko bei Abschluss eines Kaufvertrages im Internethandel liegt sowohl für Kunden als auch für Händler in der Nichterfüllung der Hauptpflichten durch den Vertragspartner. Die wesentlichen Pflichten sind hierbei die Lieferung der Ware durch den Verkäufer und die Bezahlung durch den Käufer. Dadurch, dass im Internethandel typischerweise kein physisches Aufeinandertreffen der Vertragsparteien stattfindet, ist eine unmittelbare Erfüllung der Vertragspflichten wie im stationären Handel durch Käufer und Verkäufer nicht möglich. Im Internethandel muss jeweils einer der Beteiligten in Vorleistung treten, entweder mit dem Versand der Ware oder der Zahlung des Kaufpreises.

299. Die Risiken im Internethandel lassen sich für Kunden u.a. durch die Nutzung bekannter oder mit einem Gütesiegel versehener Internetshops reduzieren oder durch Nutzung von Bezahlverfahren, die Käuferschutz beinhalten, durch den eine u.U. bedingte Rückzahlung im Fall der Nichtlieferung erfolgt. Für Händler lässt sich die Reduzierung des Risikos, dass der Kunde die erhaltene Ware nicht bezahlt, ebenfalls durch die Integration geeigneter Bezahlverfahren erreichen. Inwieweit Händler hierfür explizite Garantien oder weniger formale Zusagen über die Ausführung der Bezahlung als ausreichend ansehen, ist abhängig von ihrer jeweiligen Risikoeinschätzung und Risikopräferenz.

b) Typisierung von Bezahlverfahren im Internethandel

300. Im Internethandel werden eine Vielzahl von Bezahlmöglichkeiten angeboten, die auf klassischen Bezahlverfahren aus dem stationären Handel aufsetzen oder aus dem Distanzhandel übernommen worden sind (vgl. dazu unter c) aa)). Zu den Verfahren, die speziell für den Internethandel entwickelt worden sind, gehören solche, die über das Online-Banking des Kunden abgewickelt werden (vgl. dazu unter c) bb)) sowie über Verfahren, bei denen Kunden ein eigenes Konto führen, über das Zahlungen abgewickelt werden (vgl. dazu unter c) cc)).[262]

---

[262] Die Darstellung der im Internethandel genutzten Bezahlverfahren orientiert sich an der Online Payment Studie 2014, Daten, Fakten, Hintergründe und Entwicklungen, EHI Retail Institute e.V., Köln, S. 101f., Bl. 6336ff. d.A. Neben den genannten Verfahren existieren in den einzelnen Kategorien jeweils weitere Bezahlverfahren. Außerdem sind auch weitere Varianten wie z.B.

301. Im Internethandel steht Händlern eine Vielzahl unterschiedlicher Bezahlverfahren zur Verfügung. Händler bieten ihren Kunden in der Regel verschiedene Bezahlverfahren an. Soweit Kunden Bezahlverfahren kennen oder nutzen, kann dies zu einer Erhöhung der Konversionsrate[263] im Shop beitragen.

302. Nicht zur Verfügung steht Händlern und Kunden bisher das in Deutschland am weitesten verbreitete Instrument zur Abwicklung von bargeldlosen Zahlungen im stationären Handel, die **girocard**, die nur an von der deutschen Kreditwirtschaft zugelassenen Terminals eingesetzt werden kann.[264] Aus Praktikabilitätsgründen steht mangels physischen Kontakts zwischen den Vertragsparteien die **Barzahlung** in Form der Übergabe gesetzlicher Zahlungsmittel im Internethandel überwiegend nicht zur Verfügung.[265]

c) Bezahlverfahren im Internethandel stellen einen eigenständigen sachlichen Markt dar

303. Dem Markt für Bezahlverfahren im Internethandel sind klassische Bezahlverfahren zuzurechnen, bei denen die Zahlungsabwicklung über einen Dritten Dienstleister erfolgt (Zahlung per Rechnung, Vorkasse oder Lastschrift). Auch die im Distanzhandel gängigen Teilzahlungsverträge und die Zahlung per Nachnahme gehören zum Markt. Desweitern gehört die Abwicklung der Zahlung durch den Einsatz von Kreditkarten zum sachlich relevanten Markt. Zusätzlich gehören die für den Internethandel entwickelten Bezahlverfahren zum Markt, die über Dienstleister abgewickelt werden, deren Produkte unter Nutzung Online-Banking-fähiger Girokonten der Zahler (giropay, sofortueberweisung.de, Paydirekt) angeboten werden oder über Dienstleister, die eigene Konten für Zahler führen und die Rechnungsbeträge hierüber abrechnen (PayPal, Click&Buy, Scrill). Daneben existieren Zahlungsmöglichkeiten z.B. über die Nutzung von

---

mobiles Bezahlen über Telefone oder Gutscheinkarten denkbare, aber weniger weit verbreitete Alternativen.

263 Umwandlung eines Kaufinteresses in eine Bestellung im Rahmen der Nutzung eines Online-Shops.

264 Internationale Schemes geben Debitkarten heraus, die auch im Fernabsatz genutzt werde können. Voraussetzung hierfür ist, dass sie mit einer Primary Account Number (PAN) ausgestattet sind. Derzeit ist dies bei den in Deutschland ausgegebenen Debitkarten nicht der Fall; regelmäßig werden maestro (MasterCard) und V-PAY (Visa) nur als Co-Brand auf einer girocard verwendet.

265 Etwas andere gilt, wenn Händler neben dem Internetshop ebenfalls ein stationäres Ladenlokal betreiben und dort die Abholung und Bezahlung der Ware anbieten. In diesen Fällen kommen ausnahmsweise auch Barzahlung und die Zahlung mit Debitkarten in Frage. Nach einer Untersuchung der 1000 größten Online Shops in Deutschland betreiben davon mehr als die Hälfte neben dem Internethandel auch mindestens ein stationäres Ladenlokal (Vgl. Der E-Commerce-MarktDeutschland 2014, Weitere Vertriebskanäle von Online-Shops, Abb. 4, S. 12, hrsg. vom EHI Retail Institute e. V. und der Statista GmbH 2014).

Mobilfunkgeräten, die in der Praxis bisher jedoch nur eine untergeordnete Bedeutung erlangt haben.

aa) Nutzbarkeit von Bezahlverfahren des klassischen Distanzhandels und des stationären Handels

304. Traditionelle Bezahlverfahren des Distanzhandels sind der Kauf auf **Rechnung**, **Vorkasse,** der Einzug der Forderung per **Lastschrift** und die Zahlung per **Nachnahme**. Im stationären Einzelhandelt verbreitet ist die Akzeptanz von **Kreditkarten**. Auch der Einsatz von **Teilzahlungsverträgen** kommt zur Bezahlung von Waren in Betracht.

305. Dem Markt für Bezahlverfahren im Internethandel sind solche klassischen Bezahlalternativen nur dann zuzurechnen, wenn Händler die Abwicklung nicht intern organisieren, sondern spezialisierte Dienstleister einschalten.

(1) Überweisung (Kauf auf Rechnung, Vorkasse) und Lastschrift

306. Beim **Kauf auf Rechnung** verschickt der Händler die Ware und legt dieser eine Rechnung bei, deren Begleichung der Käufer in der Regel durch Erteilung eines Überweisungsauftrags an sein Kreditinstitut bewirkt. Hierzu kann der Verkäufer ein Zahlungsziel einräumen. Sofern der Verkäufer das Risiko des Zahlungseingangs minimieren will, kann er den Kauf auf Rechnung in Form der **Vorkasse** verlangen. Bei dem Kauf auf Rechnung überweist der Kunde den Rechnungsbetrag auf das Konto des Händlers. Der Händler benötigt zur Nutzung dieses Bezahlverfahrens lediglich ein Girokonto, um die Zahlungen entgegennehmen zu können. Beide Zahlungsarten verschieben die Risiken der Erfüllung aller Pflichten der Kaufvertragsparteien einseitig entweder zu Lasten des Käufers oder des Händlers: Bei der Vorkasse entfällt für den Händler das Risiko des Zahlungsausfalls, während er es bei Zahlung auf Rechnung vollständig tragen muss. Bei Vorkasse trägt der Käufer das Risiko der Nichtlieferung der Ware, während er beim Rechnungskauf gegen dieses Risiko vollständig abgesichert ist.

307. Die Zahlung des Kaufpreises kann ebenfalls per Lastschrifteinzug erfolgen. Dabei veranlasst der Händler nach Erteilung eines Lastschriftmandats den Einzug der fälligen Forderung vom Konto des Käufers. Auch bei der Zahlung mittels **Lastschrift** handelt es sich um ein Verfahren, das lange vor dem Entstehen des Internethandels entwickelt wurde. Hierbei muss der Käufer zur Zahlung des Kaufpreises nichts weiter veranlassen, als ein Lastschriftmandat zu erteilen und die entsprechenden Kontodaten an den Händler zu übermitteln. Der Händler generiert aus den Daten des Kunden eine Lastschrift, die er bei seiner Bank zum Inkasso einreicht. Diese schreibt den Lastschriftbetrag vorbehaltlich des Eingangs dem Konto des Händlers gut und zieht den Lastschriftbetrag von der Bank

des Kunden ein, die das Konto des Zahlungspflichtigen belastet. Das Risiko des Zahlungsausfalls liegt bei der Nutzung des Lastschriftverfahrens beim Händler, da dieser riskiert, dass eine einmal eingelöste Lastschrift nachträglich durch den Kunden zurückgegeben wird bzw. dass die Bank des Zahlers die Einlösung auf Grund mangelnder Kontodeckung ablehnt und die Lastschrift dem Händler zurückbelastet wird.

308. Sofern Händler bei der Nutzung klassischer Bezahlverfahren im Internethandel Nachteile hinsichtlich des Ausfallrisikos ihres Vertragspartners beim Kauf auf Rechnung aufgrund verfügbarer eigener Informationen nicht hinreichend beurteilen können, sind auf dem Markt Anbieter tätig, welche die Beurteilung des Ausfallrisikos des Kunden und die Abwicklung von Zahlungen gegen Entgelt anbieten. Die am Markt tätigen Unternehmen bieten dabei nicht allein die Abwicklung des Kaufs auf Rechnung an. Ihr Angebot umfasst teilweise auch die Abwicklung über Lastschrifteinzug oder den Ratenkauf. Damit führen diese Angebote zur Übertragung des Risikomanagements und von administrativen Tätigkeiten auf den externen Dienstleister gegen Zahlung eines Entgelts.

309. In der Regel bieten Dienstleister die Übernahme und Abwicklung des Bezahlprozesses in Verbindung mit Factoringmodellen an. Beim Factoring erwirbt ein Dienstleister die Forderung gegenüber dem Kunden[266] und zahlt den Rechnungsbetrag abzüglich eines Disagios an den Händler aus. Während dem Händler die Liquidität zufließt, übernimmt der Finanzdienstleister den Forderungseinzug und auch das Inkasso im Falle der Zahlungsstörung. Händler, die nicht wollen, dass ihre Kunden in Kontakt zu einem Dienstleister treten, haben die Möglichkeit, sogenannte „Whitelabel-Lösungen“ zu wählen, bei denen die Angebote der Dienstleister in den Internetshop integriert werden, und diese die Abwicklung im Namen des Händlers ausführen (vgl. Rz. 326).[267]

310. Solche Angebote kann der Händler teilweise sowohl als Marke des entsprechenden Dienstleisters in seinen Internetshop einbinden oder als Unterstützung für die eigene Abwicklung des Bezahlvorgangs einsetzen. Die RatePAY GmbH[268], Berlin, bietet Händlern im Rahmen des Bezahlvorgangs sowohl die Rechnung mit Zahlungsgarantie als auch die Lastschriftabwicklung mit Risikoprüfung oder Ratenzahlung an.[269] Die nach den

---

266 Je nach Factoringmodell kann die Forderung durch den Dienstleister auch erst übernommen werden, wenn die Fälligkeit der Zahlung überschritten worden ist, der Kunde sich somit im Verzug befindet (Fälligkeitsfactoring).

267 EHI Retail Institute e.V., Online-Payment-Studie 2014, Daten, Fakten, Hintergründe und Entwicklungen, S. 101f., Bl. 6364f. d.A.

268 Die RatePay GmbH ist ein Unternehmen des Otto-Konzerns.

269 https://www.ratepay.com/produkte, Stand 16.03.2015.

Marktstudien des EHI Retail Institute in Deutschland bekanntesten Verfahren sind Billpay[270], Klarna[271] und Paymorrow[272].

(2) Teilzahlungsverträge

311. Auch der Abschluss eines **Kreditvertrages** zur Finanzierung des Kaufpreises stellt ein alternatives Bezahlverfahren dar. Der Kaufpreis wird dem Händler dabei von einem Kreditinstitut gutgeschrieben, das mit dem Kunden einen Kreditvertrag abschließt. Der Kunde verpflichtet sich dabei zur Rückzahlung des Kreditbetrags inklusive Zinsen entweder in Raten oder zu einem vereinbarten Zeitpunkt in der Zukunft.

(3) Nachnahme

312. Ein weiteres gängiges Verfahren aus dem Distanzhandel ist der Versand mit der Zahlung per **Nachnahme**: Hierbei versendet der Händler die Ware über einen Paketdienstleister, der die Auslieferung übernimmt und die Zahlung entgegennimmt, um sie an den Händler weiterzuleiten. Durch die Zahlung per Nachnahme entfallen für Händler und Kunde die Hauptrisiken der Leistungserfüllung, da der Paketdienstleister das physische Zusammentreffen von Händler und Kunde ersetzt und die Übergabe der Ware gegen Zahlung des Kaufpreises sicherstellt. Für diese Dienstleistung erhält der Paketdienstleister ein Entgelt.[273]

(4) Kreditkartenzahlungen

313. Auch Kreditkartenzahlungen stellen ein Zahlungsinstrument dar, das vor dem Entstehen des Internethandels entwickelt wurde und das auch dem Markt zuzurechnen ist. Die

---

[270] Billpay wurde 2009 gegründet und hat seinen Sitz in Berlin. Derzeit hat das Unternehmen nach eigenen Angaben 115 Mitarbeiter und bietet seine Dienstleistungen in mehr als 4.000 Internetshops an. Billpay bietet seine Dienstleistungen in Deutschland, Österreich, der Schweiz und den Niederlanden an. Seit 2013 gehört das Unternehmen zur Wonga Group, einem britischen Online-Finanzdienstleister mit Sitz in London.

[271] Klarna, die Muttergesellschaft der Sofort, wurde 2005 in Schweden gegründet und bietet den Kauf auf Rechnung und Kauf per Ratenzahlung im Internethandel als Bezahlverfahren an. An Klarna halten verschiedene Finanzinvestoren Beteiligungen. Klarna ist neben Schweden in Dänemark, Norwegen und Finnland sowie in Deutschland, den Niederlanden und Großbritannien tätig. 2014 beschäftigte das Unternehmen mehr als 1200 Mitarbeiter. Nach Unternehmensangaben nutzen mehr als 50.000 Händler die Dienstleistungen von Klarna.

[272] Paymorrow wurde 2008 gegründet und bietet seitdem abgesicherten Rechnungskauf im Internethandel vor allem gegenüber kleinen und mittleren Händlern in Deutschland an. Nach eigenen Angaben nutzen mehr als 2.000 Händler die Angebote von Paymorrow. Seit 2013 hält die Intercard AG, Taufkirchen, (ein Netzbetreiber) eine Mehrheitsbeteiligung an dem Unternehmen. Neben dem abgesicherten Rechnungskauf bietet Paymorrow auch das Lastschriftverfahren an.

[273] Traditionell zahlt der Kunde bei dieser Bezahlform in bar, inzwischen nehmen Zustelldienste aber auch Kartenzahlungen entgegen.

überwiegende Zahl aller Kreditkarten-Transaktionen in Deutschland wird in sog. 4-Parteien-Systemen abgewickelt, in denen der Händler einen Dienstleister, den Acquirer, mit der Abwicklung der Kreditkartenzahlungen beauftragt.[274] Auf Grund des Akzeptanzvertrages wird dem Händler die Möglichkeit eröffnet, Kreditkartenzahlungen entgegenzunehmen. Bei Kreditkartenzahlungen ist zwischen der Autorisierung einer Zahlung und dem Clearing und Settlement von Kreditkartenumsätzen zu unterscheiden. Wenn ein Zahlungsvorgang mittels einer Kreditkarte durch einen Kunden des Händlers eingeleitet wird, richtet der Händler eine Autorisierungsanfrage mit den entsprechenden Daten (Betrag, Kartennummer, Gültigkeitsdauer der Karte etc.) ggf. unter Inanspruchnahme weiterer technischer Dienstleister an den Acquirer. Dieser leitet sie über die internationalen Autorisierungsnetzwerke der Kreditkartenorganisationen an die kartenausgebende Bank weiter.[275] Bei einer positiven Autorisierung des Zahlungsvorganges sagt der Acquirer dem Händler die Zahlung zu. Allerdings ist der Händler nicht vor Rückbuchungen („chargebacks“) geschützt, die darauf zurückzuführen sind, dass der Kreditkarteninhaber die missbräuchliche Nutzung seiner Kreditkartendaten geltend macht und der Belastung widerspricht.

314. In den großen Kreditkartensystemen von MasterCard und Visa erhält das kartenausgebende Kreditinstitut ein Entgelt (Interbankenentgelt) vom Acquirer. Dieses Interbankenentgelt stellt eine erhebliche Einnahmequelle für die beteiligten Banken dar. Nach Ermittlungen der Beschlussabteilung erzielten die kartenausgebenden Banken aus den Interbankenentgelten der 5 größten Acquirer im Jahre 2009 EUR 350 Mio. (nur innerdeutsche Transaktionen).[276] Ab dem 09.12.2015 begrenzt die Interbankenentgelt-VO[277] die Höhe der Interbankenentgelte für Verbraucherkreditkarten auf 0,3% des jeweiligen Umsatzes.

315. Kreditkartenzahlungen im Internet sind mit höheren Risiken verbunden als Kreditkartenzahlungen im stationären Handel, da aufgrund des fehlenden physischen Aufeinandertreffens von Händler und Kunde nicht geprüft wird, ob der Kunde tatsächlich Inhaber der betreffenden Kreditkarte ist. Auch eine Unterschriftsprüfung ist hierbei nicht

---

274 Die beiden anderen Teilnehmer in solchen Systemen sind der Karteninhaber und die kartenausgebende Bank.

275 In Deutschland ist diese Autorisierung „online zum Issuer“ nach Kenntnis des Bundeskartellamtes die Regel.

276 Das Bundeskartellamt geht derzeit davon aus, dass mindestens 20% dieser Erlöse auf Transkationen im Internethandel zurückzuführen sind.

277 Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29.04.2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge, Amtsblatt der Europäischen Union, L 213/1 vom 19.05.2015.

möglich. Aus diesen Gründen legen Acquirer bzw. die Kreditkartenorganisationen regelmäßig besondere Sorgfaltsanforderungen des Händlers für den Einsatz von Kreditkarten im Fernabsatz unter Einbeziehung des Internethandels fest und treffen ggf. weitere Maßnahmen, um Risiken zu begrenzen.[278] Neben MasterCard und VISA kommen auch andere, in Deutschland weniger verbreitete Kreditkarten im Internethandel als Bezahlalternative in Frage. Hierzu gehören beispielsweise American Express, Diners Club oder JCB.

bb) Bezahlverfahren im Internethandel mit Abwicklung über das Online-Banking

316. Im Internethandel haben sich verschiedene Verfahren etabliert, bei denen die Bezahlung des Rechnungsbetrags über einen Zugang zum Online-Banking-Konto des Kunden erfolgt. Der Kunde wird in diesem Zusammenhang von der Internetseite des Händlers auf die Internetseite des jeweiligen Bezahlverfahrens geleitet, von der aus der Bezahlvorgang initiiert wird. Da diese Verfahren eine Zahlung des Rechnungsbetrags über das Konto des Kunden auslösen, werden sie auch als Zahlungsauslösedienste bezeichnet.

317. Das von Unternehmen der Kreditwirtschaft angebotene **giropay**-Verfahren, das Paydirekt-Verfahren und das von der Sofort angebotene bankenunabhängige Verfahren **sofortüberweisung.de** basieren beide auf dem Zugang zum Online-Banking-Konto und der Erteilung von Überweisungsaufträgen. Der Kunde kann dabei im Online-Banking einen Überweisungsauftrag über den Kaufpreis an sein kontoführendes Kreditinstitut erteilen. Der Händler erhält von dem jeweiligen Systembetreiber unmittelbar die Rückmeldung, ob dieser Überweisungsauftrag von der kontoführenden Bank angenommen und ausgeführt wird. Wie bei der Vorkasse überweist der Käufer vor Lieferung den Kaufbetrag an den Händler; dieser muss für die Sicherheit, dass der Vertragspartner seine Pflichten aus dem Kaufvertrag erfüllt, nicht bis zum Eingang des Kaufbetrages mit der Lieferung warten, sondern erhält unmittelbar eine Mitteilung über die Durchführung der Überweisung im Online-Banking-Verfahren. Diese schnellere Abwicklung macht dieses Verfahren für beide Vertragsparteien deutlich attraktiver als die

---

[278] Die Kreditkartenorganisationen streben die Erhöhung der Sicherheit von Kreditkartenzahlungen an, um die Kreditkartenzahlungen im Internethandel attraktiver zu machen. Beispiele hierfür sind das „MasterCard Secure Code-Verfahren“ von MasterCard und das „Verified by Visa-Verfahren“ von Visa, bei denen Kunden bestimmte Sicherheitsmerkmale, die nur ihnen bekannt sein dürfen, zur Zahlungsauslösung eingeben.

Zahlung gegen Vorkasse mit Lieferung erst nach Eingang des Kaufbetrages auf dem Konto des Händlers.[279]

318. Bei giropay, einem Verfahren der Kreditwirtschaft, erhält der Händler eine unbedingte Zahlungsgarantie derjenigen Kreditinstitute, mit denen giropay einen entsprechenden Vertrag abgeschlossen hat. Kunden von Kreditinstituten ohne vertragliche Anbindung an giropay können das Verfahren nicht nutzen.

319. Die Sofort stellt den Händlern keine Garantie im kreditwirtschaftlichen Sinne zur Verfügung, sondern erlangt mit Einverständnis der Kontoinhaber Einsicht in das Konto und leitet einen Überweisungsauftrag des Kunden an das Kreditinstitut weiter. Sofern die Überweisung ausgeführt wird, erhält der Händler eine Bestätigung darüber, dass die Überweisung eingereicht wurde und ausreichende Deckung vorhanden war.[280] Bei der gegenüber dem Händler abgegebenen Einreichungs- und Ausführungsbestätigung handelt es sich nicht um eine Garantie im rechtlichen Sinne.

cc) Bezahlverfahren, bei denen Kunden eigene Konten zur Abwicklung führen

320. Eine weitere Möglichkeit zur Abwicklung von Bezahlvorgängen im Internethandel liegt in der Nutzung von Bezahlverfahren, bei denen Kunden ein eigenes Konto – regelmäßig neben dem Girokonto – unterhalten, über das die Begleichung der Rechnung erfolgt.

321. Das bekannteste Verfahren stellt dabei **PayPal** dar. Nach dem gleichen Prinzip arbeiten aber auch Dienste wie **Scrill**, eine in Deutschland ebenfalls im Rahmen des Internethandels von Händlern als Bezahlverfahren nachgefragte Bezahlalternative, die wie eine elektronische Geldbörse (E-Wallet) funktioniert. Zur Nutzung eines dieser Bezahlverfahren eröffnet der Kunde ein Konto bei PayPal oder Scrill. Dort hinterlegt er eine Kontoverbindung oder Kreditkartendaten, mit denen Geldbeträge per Lastschrift oder durch Kreditkartentransaktion auf das Konto des Bezahlverfahrens übertragen werden. Teilweise ist auch die Übertragung von Geldbeträgen mit Verfahren wie giropay oder

---

279 Zur Einordnung dieser Verfahren als Varianten zur Vorkasse vgl. Stahl, Krabichler, Breitschaft, Wittmann, E-Commerce-Leitfaden, 2. überarbeitete und erweiterte Auflage, Regensburg 2009, aktualisiert am 14.10.2010, ibi research 2009 (www.ecommerce-leitfaden.de), S. 114 (Anlage XXVII, Kapitel 4).

280 Die bestehende Kontodeckung prüft das System auf verschiedene Arten. Bei Banken, deren Systeme alle anfallenden Geschäftsvorfälle aktuell verbuchen (real-time buchende Kreditinstitute) umfasst die Prüfung dabei die Höhe des Verfügungsbetrags. Bei Kreditinstituten, deren Systeme nicht stets den aktuellen Kontostand anzeigen, prüft das System den Verfügungsbetrag anhand des angezeigten Kontostandes unter Berücksichtigung vorgemerkter Buchungen. Im letztgenannten Fall prüft das System ebenfalls die erfolgreiche Verbuchung von Geschäftsvorfällen des Kunden mit sofortüberweisung.de innerhalb der letzten 30 Tage.

sofortüberweisung.de möglich. Wählt der Kunde ein solches Bezahlverfahren im Internetshop aus, wird er auf die Internetseite des Bezahlverfahrens geleitet, auf der er die Zugangsdaten für das Bezahlverfahren eingibt und den Rechnungsbetrag auf das Konto des Verkäufers transferiert. Dabei wird der Rechnungsbetrag entweder zu Lasten des Guthabens auf dem Konto des Bezahlverfahrens gebucht oder in einem zusätzlichen Schritt vom Bankkonto des Kunden eingezogen bzw. seiner Kreditkarte belastet. Dem Händler, der ebenfalls ein Konto bei dem Bezahlverfahren unterhält, wird der Rechnungsbetrag gutgeschrieben.

dd) Sonstige Bezahlverfahren im Internethandel

322. Neben den vorstehendend genannten Verfahren existieren weitere, weniger verbreitete Möglichkeiten, z.B. das mobile Bezahlen oder die Bezahlung mit Prepaid-Karten, die derzeit jedoch allenfalls eine untergeordnete Bedeutung am Markt haben.

ee) Zusammenfassung

323. Zum sachlichen Markt für Bezahlverfahren im Internethandel gehören klassische, über einen Dienstleister abgewickelte Verfahren wie die Zahlungen per Rechnung, Vorkasse, Lastschrift und Nachnahme sowie Teilzahlungsverträge und Kreditkartenzahlungen. Zusätzlich sind dem Markt spezielle Bezahlverfahren zuzurechnen, die über Dienstleister abgewickelt werden, deren Produkte unter Nutzung online-banking-fähiger Girokonten der Zahler (giropay, sofortueberweisung.de, Paydirekt) erfolgt oder über Dienstleister, die eigene Konten für Zahler führen, über die die Rechnungsbeträge abgerechnet werden (PayPal, Scrill).

d) Verbreitung der Bezahlverfahren im Internethandel

324. Bei den dargestellten Bezahlverfahren im Internethandel zeigen sich deutliche Unterschiede bei der Inanspruchnahme durch Internethändler. Die auch im stationären Handel und dem Distanzhandel genutzten Bezahlverfahren sind sehr weit verbreitet. Nach Schätzung des EHI Retail Institutes in den Top-1000 Online-Internetshops stellen sie eine der bedeutendsten Gruppen dar, die von mehr als 80% der befragten Händler genutzt werden. Einen hohen Verbreitungsgrand im Internethandel erreichen insbesondere auch die Kreditkarten der Gesellschaften VISA und MasterCard, die jeweils von rund 80% der Shops als Bezahlverfahren angeboten werden. Deutlich geringer Verbreitung haben andere Kreditkarten z.B. von American Express, Diners Club, JCB.

325. E-Wallet Lösungen erreichen aufgrund der großen Bedeutung von PayPal ebenfalls in Deutschland einen hohen Verbreitungsgrad unter den Internethändlern mit über 80%. Die

sonstigen Verfahren in dieser Gruppe werden von weniger als 10% der Händler eingesetzt.

326. Ebenso liegt die Verbreitung von Rechnungsdienstleistern jeweils deutlich unter 10%. Nach der EHI-Schätzung werden aber von knapp 40% der Händler White-Label-Lösungen angeboten, also Dienstleistungen von Anbietern, die nicht unter eigenem Namen auftreten, bei denen der Kunde also nicht erkennt, dass der Händler nicht selbst tätig wird (vgl. Rn. 309).

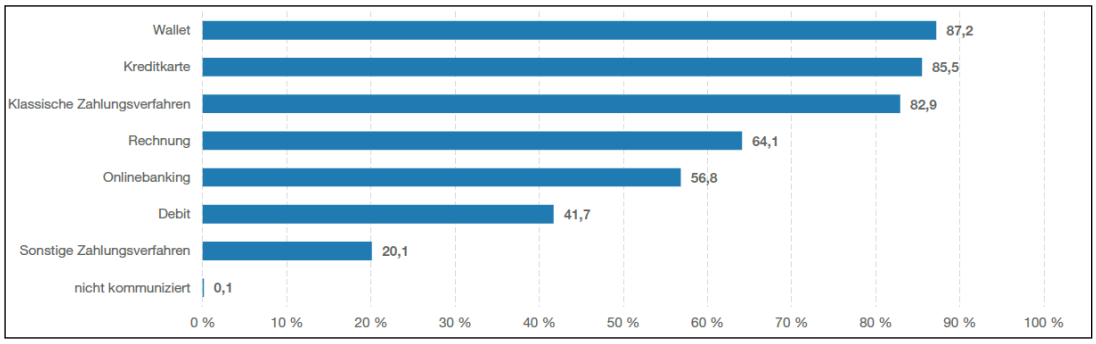


Abb. 6 - Bezahlverfahren im Internethandel 2014[281]

327. Im Bereich des „Online-Bankings“ sind als Zahlungsauslösedienste in Deutschland im Wesentlichen soforteuberweisung.de und giropay am Markt vertreten. Das bankenunabhängige Verfahren der Sofort erreicht dabei mit rund 50% eine deutlich höhere Marktdurchdringung als giropay, das von weniger als 10% der Händler angeboten wird[282]. Auch gemessen an den Wachstumsraten zeigen sich hier deutliche Unterschiede. Während giropay bei der ersten Studie des EHI 2012 bereits von weniger als 10% der Händler angeboten wurde und seinen Verbreitungsgrad nur unwesentlich steigern konnte, stieg die Verwendung von sofortueberweisung.de im Internethandel trotz der von der DK initiierten Maßnahmen deutlich an. Während 2011 lediglich 36% der Händler dieses Bezahlverfahren angeboten haben, lag dieser Wert 2012 bei rund 50%.

328. Auch die Deutsche Bundesbank hat das Zahlungsverhalten in einer Studie untersucht und kommt zu dem Ergebnis, dass es deutliche Unterschiede bei der Bezahlung von Waren oder Dienstleistungen im stationären Handel und im Internethandel gibt.

---

281 Der E-Commerce-Markt Deutschland 2014, hrsg. vom EHI Retail Institute e. V. und der Statista GmbH 2014, In Onlineshops angebotene Zahlungsverfahren, Abb. 26, S. 42.

282 Die genannten Zahlen beziehen sich auf das Angebot durch Händler und lassen als solche keine Rückschlüsse auf den Grad der tatsächlichen Nutzung durch Kunden zu.

329. Die Bundesbank stellt in ihrer Studie zum „Zahlungsverhalten in Deutschland 2014“[283] fest, dass Innovationen im Zahlungsverkehr voraussetzen, dass mit ihnen ein echter Vorteil gegenüber etablierten Verfahren verbunden ist und ein besonderes Augenmerk auf Sicherheit gelegt werden muss. Die Erfüllung dieser Voraussetzungen trägt danach zu stetigen aber langsamen Veränderungen bei, die sich insbesondere im Bereich der Bezahlverfahren im Internethandel deutlich zeigen.[284]

330. Das Bezahlverhalten der Kunden im Internethandel unterscheidet sich deutlich von dem im Distanzhandel und im stationären Handel. Knapp 85% aller Transaktionen[285] werden danach im Internethandel mit Internetbezahlverfahren[286], Überweisungen und Kreditkarten durchgeführt. Die Nutzung von Bargeld im Internethandel spielt danach keine Rolle. Demgegenüber werden im stationären Handel die meisten Transaktionen durch Barzahlung und die Zahlung mit der girocard abgeschlossen.[287]

331. Die Bundesbank-Studie belegt durch ihre Ergebnisse, dass der Internethandel ein stetig wachsendes Marktsegment darstellt, das Kunden immer stärker nutzen. Während 2008 der Anteil der Befragten, die im Internet einkauften bei 42% lag, stieg dieser Wert bis 2011 auf 57% und lag 2014 bei 63%.[288]

332. Die von der Bundesbank durchgeführte Befragung zeigt, dass diejenigen, die angegeben haben, Interneteinkäufe zu tätigen, zur Bezahlung der Waren und Dienstleistungen im Wesentlichen Überweisungen nutzen (56%) gefolgt von Internetbezahlverfahren (55%) und Zahlung per Lastschrift (25%).

---

283 Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2014, Dritte Studie über die Verwendung von Bargeld und unbaren Zahlungsinstrumenten , Frankfurt 2015.

284 Ebenda S. 6 f.

285 41,1% der Transaktionen entfallen auf Internetbezahlverfahren, 23% auf Überweisungen, 17,7% auf Kreditkartenzahlungen und 3,7% auf die Verwendung der girocard.

286 Erfasst werden hier Zahlungen, die über PayPal, Sofortüberweisung,de und giropay getätigt werden.

287 Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2014, Abb. 16 (Verwendung von Zahlungsinstrumenten nach Zahlungsort und –zweck), S. 63.

288 Ebenda, S. 70 f.

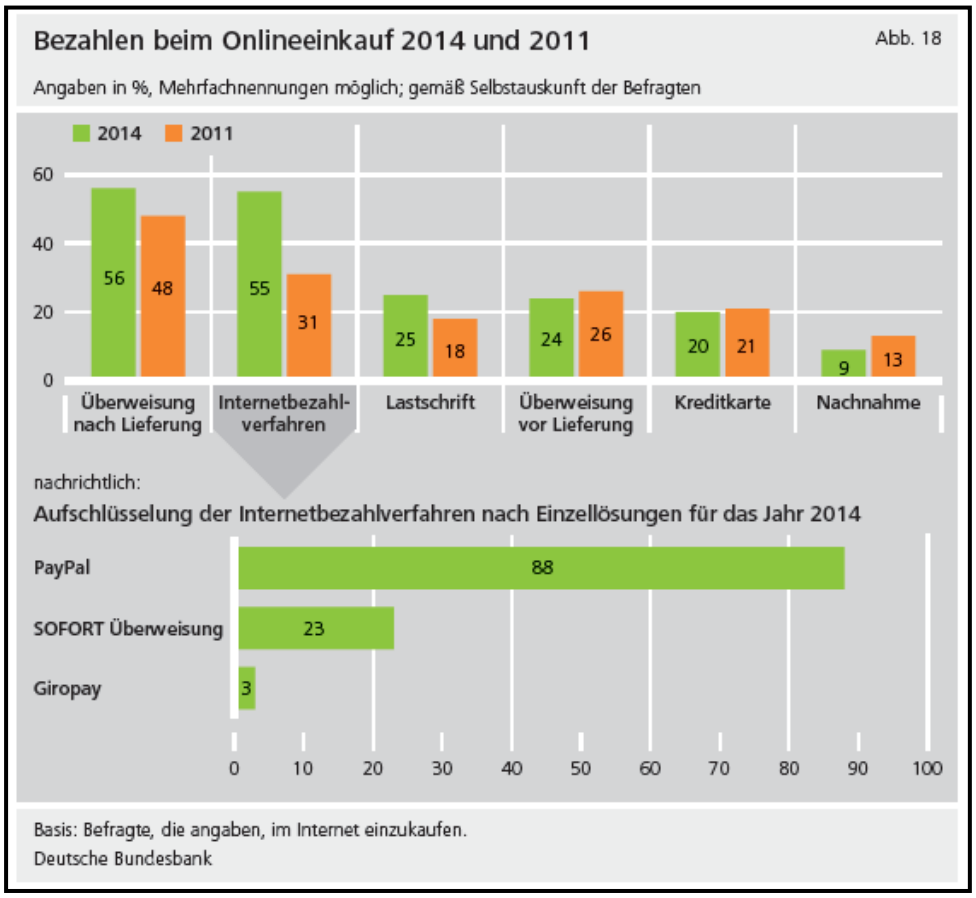


Abb. 7 - Studie Bundesbank, Zahlungsverhalten in Deutschland 2014, S. 73

333. Weiter werden als genutzte Bezahlverfahren noch die Überweisung vor Lieferung der Ware (24%), die Nutzung von Kreditkarten (20%) sowie Nachnahme (9%) genannt. Während sowohl Nachnahme, Kreditkarten und Überweisung vor Lieferung der Ware oder Erbringung der Dienstleistung im Vergleich zur zweiten Studie im Jahr 2011 rückläufige Nutzungsanteile aufweisen, konnten die am häufigsten genutzten Bezahlverfahren (Überweisung, Internetbezahlverfahren und Lastschrift) im Vergleichszeitraum steigende Anteile verzeichnen. Die Nutzung von Internetbezahlverfahren wurde 2011 lediglich von 31% der Befragten als genutzte Alternative angegeben, der Wert hat sich im Vergleich dazu 2014 auf 55% erhöht.

334. Innerhalb der Internetbezahlverfahren nimmt Paypal in den Ergebnissen der Bundesbank eine besondere Stellung ein. 88% der Befragten haben dieses Bezahlverfahren genutzt. Sofortüberweisung erreicht demgegenüber einen Anteil von 23% während giropay von lediglich 3% der Befragten genutzt wurde.

2. Der räumlich relevante Markt

335. Der Markt für Bezahlverfahren im Internethandel umfasst das Gesamtgebiet Deutschlands, geht aber, auch wenn verschiedene Zahlverfahren auch in anderen Mitgliedstaaten der Europäischen Union angeboten werden, derzeit und für den für dieses Verfahren relevanten Prognosezeitraum nicht darüber hinaus. Die Nachfragepräferenz und die Bedeutung insbesondere nationaler Zahlungsverfahren unterscheiden sich in den einzelnen europäischen Staaten ganz erheblich.

336. Auch der räumlich relevante Markt ist nach ökonomischen Kriterien abzugrenzen. Die Bestimmung des räumlich relevanten Marktes folgt grundsätzlich denselben Kriterien wie die des sachlich relevanten Marktes, d.h. nach der funktionellen Austauschbarkeit aus Sicht der Nachfrager.[289] Er umfasst das Gebiet, in dem die betreffenden Produkte regelmäßig angeboten und nachgefragt werden, in dem die Wettbewerbsbedingungen homogen sind und das sich von benachbarten Gebieten durch spürbar unterschiedliche Wettbewerbsbedingungen unterscheidet.

337. Auf dem Markt für Bezahlverfahren im Internethandel können die Bezahlverfahren zumindest bundesweit in Anspruch genommen werden. Von einer weiteren räumlichen Marktabgrenzung über Deutschland hinaus ist aber aktuell und auch im Prognosezeitraum nicht auszugehen. Bereits das Nutzerverahlten in Österreich und der Schweiz zeigt signifikante Unterschiede zu dem in Deutschland.[290]

338. Zwar sind einige Anbieter von Verfahren wie PayPal und Kreditkartenzahlungen aktuell auch in anderen europäischen Mitgliedstaaten tätig; für viele andere Unternehmen, die innovative neue Bezahlverfahren anbieten trifft die aber nicht zu; ihre Tätigkeitsbereich beschränkt sich jeweils auf einzelne Mitgliedstaaten. So bietet beispielsweise Sofort den Zahlungsauslösedienst in weniger als der Hälfte der Mitgliedstaaten der Europäischen Union an (vgl. Rz. 21). Auch giropay ist unmittelbar lediglich in Deutschland tätig. Ein Grund für die Beschränkung auf einzelnen Mitgliedstaaten ist, dass das System von der Betreiberseite her auf Verträge mit Kreditinstituten ausgelegt ist, die über die von der DK erarbeiteten und betriebenen Schnittstellen angeschlossen werden. Eine Ausweitung der Tätigkeit auf Kreditinstitute in anderen Mitgliedstaaten ist daher derzeit noch nicht realisierbar. Denn ohne den Zugang zu Bankkunden eines Mitgliedstaates kommt die Nutzung von giropay allenfalls für Händler in Frage, die deutsche Kunden im grenzüberschreitenden Handel erreichen wollen. Über eine Kooperation mit dem

---

289 Ständige Rspr.; vgl. BGH, Beschluss vom 19.12.1995, WuW/E BGH 3037 – Raiffeisen.
290 EPSM Market Research Newsletter 03-04/16, S. 3 ff., S. 5.

österreichischen System eps konnte das Bezahlverfahren seine Reichweite lediglich in geringem Umfang ausdehnen. Derzeit ist aber nicht ersichtlich, dass eine europaweite Tätigkeit innerhalb des Prognosezeitraums erreicht werden kann.

339. Weitere Verfahren wie eps und iDEAL werden lediglich in Österreich und den Niederlanden (dort mit 56 % Marktführer) angeboten, nicht jedoch im Rest von Europa. Ihr Tätigkeitsfeld zielt darauf ab, in erster Linie Verbrauchern mit österreichischen bzw. niederländischen Grirokonten Zahlungsmöglichkeiten anzubieten.

340. Auch das Bezahlverfahren Trustly, das bisher lediglich in den skandinavischen Ländern und in Estland, Polen, Spanien und Italien angeboten wurde , erreicht auch nach einer Ausdehnung seiner Tätigkeit auf den Rest von Europa im Jahre 2016 bisher keine signifikante Marktstellung außerhalb seiner angestammten Tätigkeitsgebiete. In Frankreich dominiert das nationale Bezahlbverfahren Cartes Bancaires (CB) auch als Bezahlverfahren im Internethandel (80 %). Händler, die grenzüberschreitende im Internethandel erfolgreich sein wollen, müssen daher jedenfalls (derzeit noch) nationale Bezahlverfahren anbieten können.

341. Ob und wie schnell die Harmonierung des europäischen Zahlungsverkehrsraums (SEPA: Single European Payment Area) sowie die Deckelung der Gebühren für Kreditkartenzahlungen zu einem Zusammenwachsen eines einheitlichen Binnenmarktes führen wird, bei dem auch Bezahlverfahren im Internethandel für domestische Transaktionen europaweit vermarktet werden, ist zum gegenwärtigen Zeitpunkt nicht absehbar, weshalb die Beschlussabteilung nach wie vor von nationalen Märkten für Bezahlverfahren im Internethandel ausgeht.

3. Die Beschlüsse bezwecken eine Beschränkung des Wettbewerbs

342. Die von der DK und den Beteiligten zu 2. - 4. beschlossenen Online-Banking-Bedingungen bezwecken eine Beschränkung des Wettbewerbs im Sinne von Artikel 101 Abs. 1 AEUV sowie § 1 GWB, soweit darin Sorgfaltspflichten zum Umgang mit PIN und TAN enthalten sind, durch die die Nutzung von bankenunabhängigen Zahlungsauslösediensten ausgeschlossen wird.

343. Eine bezweckte Wettbewerbsbeschränkung liegt vor, wenn die Beschränkung ihrem Wesen nach geeignet ist, den Wettbewerb zu beschränken. Hierbei handelt es sich um Beschränkungen, die ein derart großes Potenzial für negative Auswirkungen auf den Wettbewerb haben, dass der Nachweis tatsächlicher Auswirkungen im Markt nicht

erforderlich ist.[291] Bei einer bezweckten Beschränkung des Wettbewerbs ergibt sich die Durchsetzung des Kartellverbots nicht in Abhängigkeit von dem gemeinsamen Marktanteil der an der Beschränkung beteiligten Wettbewerber.[292] Für die Prüfung des Zweckes einer Vereinbarung oder eines Beschlusses kommt es auf den Inhalt der Wettbewerbsbeschränkung (dazu unter a)), die mit ihr verfolgten Ziele (dazu unter b)) sowie auf den wirtschaftlichen und rechtlichen Zusammenhang (dazu unter c)) an, in dem sie steht. Bei letzterem sind die Art der von der Beschränkung betroffenen Waren und Dienstleistungen, die bestehenden tatsächlichen Bedingungen und die Struktur des Marktes zu berücksichtigen. Auch wenn die Absicht der Beteiligten kein notwendiges Element der Beurteilung des Zweckes einer Vereinbarung darstellt, kann diese zur Beurteilung herangezogen werden (dazu unter d)).[293] Im Rahmen dieser Beurteilung ist unschädlich, dass die Parteien neben der Wettbewerbsbeschränkung auch andere, zulässige Zwecke verfolgen.[294]

a) Inhalt der kartellrechtswidrigen Beschlüsse

344. Bereits der Wortlaut der in Rede stehenden Sorgfaltspflichten richtet sich gegen die Nutzung von PIN und TAN auf Seiten von Zahlungsauslösediensten im Internethandel. Hieraus ergibt sich eine Beschränkung des Wettbewerbs von bankenunabhängigen Zahlungsauslösediensten, die keine vertragliche Anbindung an die Online-Banking anbietenden Kreditinstitute haben, gegenüber mit diesen in Wettbewerb stehenden Kreditkarten und bankseitig vermarkteter Zahlungsauslösedienste.

345. Diese AGB Klausel zielt ihrem Wortlaut nach auf eine Einschränkung der Tätigkeit von Zahlungsauslösediensten, indem sie deren Nutzung durch die Kunden faktisch unterbindet. Da Kunden in den Online-Banking-Bedingungen verpflichtet werden, Personalisierte Sicherheitsmerkmale geheim zu halten und zum Zwecke der Auftragserteilung ausschließlich über die von der Bank mitgeteilten Online-Banking-

---

291 Bekanntmachung der Kommission, Leitlinien zur Anwendung von Artikel 81 Absatz 3 EG-Vertrag (2004/C 101/08), ABl vom 27.04.2004, Nr. C 101, S. 97, Rz. 21; auch Bekanntmachung über Vereinbarungen von geringer Bedeutung, die im Sinne des Artikels 101 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union den Wettbewerb nicht spürbar beschränken (De-minimis-Bekanntmachung) 2014/C 291/01,), Rz. 2.

292 Mitteilung der Kommission, Bekanntmachung über Vereinbarungen von geringer Bedeutung, die im Sinne des Artikels 101 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union den Wettbewerb nicht spürbar beschränken (De-minimis-Bekanntmachung), Amtsblatt der Europäischen Union, 2014/C 291/01 vom, 30.08.2014, Rz. 2.

293 Europäischer Gerichtshof, Urteil vom 11.09. 2014 in der Rechtssache C-67/13 P, Groupement des cartes bancaires (CB)/Kommission, zitiert nach curia.europa.eu, Rz.53 f.

294 EuGH, Urteil vom 20.11.2008 in der Rechtssache C-209/07 BIDS, Rz. 21 m.w.N., zitiert nach juris.

Zugangskanäle zu übermitteln, schränken diese Regelungen den Wettbewerb der verschiedenen Zahlungssysteme gegenüber Internet-Händlern ein. Als Beispiel für die durch die Sorgfaltspflichten ausgeschlossene Nutzung von PIN und TAN werden die nicht mit dem kontoführenden Kreditinstitut vereinbarten Internetseiten aufgeführt und ausdrücklich und ausschließlich Online-Händlerseiten als untersagte Nutzungsmöglichkeit genannt.

346. Durch die Bezugnahme auf die „Eingabe auf Online-Händler-Seiten“ in den Sorgfaltspflichten werden gezielt Anbieter von bankenunabhängigen Zahlungsauslösediensten ausgeschlossen. Da die Dienstleistungen von bankenunabhängigen Zahlungsauslösediensten auf vertraglicher Basis mit Händlern angeboten werden und die Dienstleistung in der Auslösung der Zahlung durch eine Verbindung zwischen der Internetseite des Händlers mit der des Zahlungsauslösedienstes erfolgt, zielt diese in den OBB formulierte Sorgfaltspflicht gegen die Nutzung von Zahlungsauslösediensten durch Internethändler und Verbraucher.

347. Dagegen werden bereits nach dem Wortlaut der Sorgfaltspflichten Produkte mit vergleichbaren Risiken, die aus der Perspektive der DK keine potenziellen Konkurrenzprodukte zu den DK-nahen Bezahlverfahren giropay, Paydirekt oder Kreditkarten sind, nicht von dem Verbot erfasst. Da sich die Reichweite von giropay lediglich auf Banken bezieht, mit denen giropay in einem Vertragsverhältnis steht, unterfällt dieser Zahlungsauslösedienst nämlich gerade nicht der Regelung, obwohl der Händler auch hier den Kunden an den Zahlungsdienst weiterleitet.

b) Die mit der Wettbewerbsbeschränkung verfolgten Ziele

348. Der DK geht es bei dem Verbot der Eingabe von Personalisierten Sicherheitsmerkmalen auf Seiten von Online-Händlern weder darum, dass die Eingabe von PIN und TAN ausschließlich über Kanäle erfolgen soll, die von den Kreditinstituten umfänglich selbst kontrolliert werden, noch um eine weitestgehende Minimierung möglicher Gefahren aus der Eingabe von PIN und TAN über Wege, deren technische Sicherheit dritte Dienstleister zu verantworten haben: Durch die Regelung der OBB wird die Verwendung von Verfahren, die auf der Basis von Java-Applikationen betrieben werden, nicht von einer Zustimmung des Kreditinstituts abhängig gemacht. Solche Produkte, die auf der Basis von Java-Applikationen betrieben werden, können von Kreditinstituten hinsichtlich ihrer Sicherheit nicht kontrolliert werden und bergen insoweit potenzielle Sicherheitsrisiken. Auch die Vermeidung der Gewöhnung an die Eingabe von PIN und TAN auf Seiten Dritter wird durch die Regelungen dieser Sorgfaltspflicht nicht hinreichend abgesichert.

349. Die OBB in ihrer Gesamtheit stellen eine standardisierte Form der Ausgestaltung des Online-Banking-Vertragsverhältnisses zwischen Kunde und Bank dar und bilden einen Rahmen, in dem die Vertragsparteien die Dienstleistungen in Anspruch nehmen bzw. erbringen. Wesentliche Inhalte der Regelungen stellen unter anderem Sicherheitsfragen sowie die Verteilung der Haftung zwischen dem Anbieter und dem Nutzer des Online-Bankings dar.

350. Die Ausgestaltung der Sorgfaltspflichten schafft die Grundlage für eine Verteilung der Haftung zwischen Bank und Nutzer u.a. im Falle möglicher finanzieller Schäden durch das Fehlverhalten des Nutzers.

351. Mit den von der DK erarbeiteten Sorgfaltspflichten verfolgt die DK allerdings kein konsequentes und umfassendes Sicherheitskonzept zum Schutz vor Missbrauch. Vielmehr zielt die Regelung, PIN und TAN nicht auf Seiten von Online-Händlern einzugeben, in erster Linie darauf ab, eine klare Unterscheidung zwischen bankenunabhängigen Zahlungsauslösediensten und anderen Intermediären zu erreichen, zu denen bankeigene Produkte wie zum Beispiel Kontoinformations- und Zahlungsauslösedienste gehören, aber auch solche Produkte von Drittanbietern, bei denen Kunden PIN und TAN zur Auslösung von Überweisungsaufträgen eingeben, die allerdings im Rahmen der individuellen Kundennutzung des Online-Banking-Kontos (Software, die auf Geräten des Kunden betrieben wird) ohne Verbindung zu einem Online-Händler erfolgt.

352. Die spezifische Regelung zur Eingabe von PIN und TAN lediglich auf den zwischen Kunden und Bank vereinbarten Internetseiten führt zur Etablierung eines Branchenstandards, den Kunden, unabhängig von der Wahl ihres Kreditinstitutes, nicht umgehen können. Als Branchenstandard können Kunden nicht zwischen Banken mit einer restriktiven Zugangspolitik und solchen mit einer wettbewerbsfördernden Regelung wählen.

353. Die DK und die Beteiligten zu 2. - 4. beziehen sich in den beanstandeten Beschlüssen zu den Sorgfaltspflichten auf eine spezifische Eingabe der PIN und TAN gegenüber Dritten im Internet. So, wie die DK den Begriff Internetseiten verwendet, soll damit keineswegs die Eingabe von PIN und TAN über das Internet generell – außerhalb des Internetauftritts der kontoführenden Bank – unterbunden werden. Angebote wie Starmoney und Starmoney.Web (vgl. Rdnr. 116ff.) sind Beispiele für Kontoinformationsdienste, über die ebenfalls Aufträge an das kontoführende Kreditinstitut auch über das Internet erteilt werden können, die gemäß den Sorgfaltspflichten keiner expliziten Nutzungsbeschränkung unterfallen. Bei Starmoney, einem von der Finanzinformatik

(Sparkassengruppe) entwickelten multibankenfähigen Produkt, handelt es sich zumindest für Kreditinstitute des BdB und des BVR um Produkte Dritter, deren technische Ausgestaltung nicht kontrolliert werden kann. Welche Kontodaten auf Servern der Finanzinformatik oder deren Tochterunternehmen gespeichert und verarbeitet werden, wie die Eingabe von PIN und TAN gegenüber Dritten gesichert wird, ist für kein Kreditinstitut nachvollziehbar. Für die Nutzer ist dabei offensichtlich, dass sie PIN und TAN in der Sphäre eines Dritten eingeben und gerade nicht ausschließlich auf Internetseiten oder im Rahmen der Nutzung von Produkten, die ihr kontoführendes Kreditinstitut eigens hierfür zugelassen hat.

354. Von daher ist auch die Argumentation der DK ist nicht stringent, bei einer Nutzung von Zahlungsauslösediensten „gewöhne“ sich der Kunde an die Weitergabe von Personalisierten Sicherheitsmerkmalen.

355. Dass Kunden PIN und TAN nicht ausschließlich in der Kommunikation mit dem kontoführenden Kreditinstitut verwenden, hat die DK mit der Konzeption des Online-Banking-Systems angelegt und akzeptiert: durch die Sorgfaltspflichten nicht in Frage gestellt werden soll u.a. die Möglichkeit zur Eingabe von PIN und TAN im Rahmen der Nutzung von Finanzverwaltungssoftware wie z.B. Starmoney der Finanzinformatik oder vergleichbarer bankfremder Produkte, wenn diese die Schnittstellen der DK nutzen. Auch dort wird der Kunde daran „gewöhnt“, PIN und TAN nicht ausschließlich im Rahmen der Kommunikation mit seinem Kreditinstitut zu verwenden. Dass auch solche Produkte eine Eingabe von PIN und TAN erfordern und diese dann erst über das Internet an das kontoführende Kreditinstitut weiterleiten (um den Zugang zum Konto zu erstellen und Daten abzufragen bzw. Aufträge zu erteilen), berücksichtigt die DK nicht als Gefahr für die Sicherheit des Online-Bankings durch spezifische Sorgfaltspflichten der Kunden oder Sicherheitsanforderungen an diese Produkte. Die internen Unterlagen der DK belegen vielmehr, dass sie die vereinbarten Sorgfaltspflichten gerade so ausgestalten wollte, dass diese Angebote einzelner Bankengruppen nicht behindert werden.[295] Werden bei der Nutzung solcher Produkte Softwarebestandteile wie JAVA-Applikationen eingesetzt, um eine verschlüsselte Kommunikation mit dem kontoführenden Kreditinstitut aufzubauen, hält die DK dies für eine angemessene technische Lösung, die ihren

---

[295] In der Fußnote zu der Sorgfaltspflicht des Kunden, nach der Legitimationsdaten nicht auf kreditinstitutsfremden Internetseiten (z.B. von Online-Händlern) eigegeben werden dürfen (Entwurf der Online-Banking-Bedingungen vom 16.04.2008) heißt es, dass die Formulierung jetzt nicht mehr den Einsatz von Online-Banking Software (z.B. Starmoney) ausschließt, bei der der Nutzer die Legitimationsdaten offline eingibt.

Sicherheitsansprüchen genügt. Tatsächlich akzeptiert sie damit bei diesen Produkten größere Risiken als bei Zahlungsauslösediensten, weil solche Java-Applikationen nicht von der DK bzw. von ihr beauftragten Einrichtungen geprüft und zugelassen, sondern von den Dienstleistungsanbietern selbst programmiert werden, ohne dass es zu einer Abnahme der Produkte durch die DK kommt.[296] Es wird nicht berücksichtigt, dass es bei der Programmierung einer solchen Java-Applikation oder einer lokal auf dem Kundenrechner installierten Software, welche die Schnittstellen der DK zur Übertragung von PIN und TAN an das Kreditinstitut nutzt, ebenfalls zu einer ungerechtfertigten Weiterleitung der Daten über das Internet an einen Dritten kommen kann.[297] Dass solche Gefahren für den Kunden bei der Nutzung entsprechender Produkte nicht erkennbar sind, da Art und Weise der Programmierung von Finanzverwaltungssoftware und Java-Applikationen für Kunden nicht nachvollziehbar sind, problematisiert die DK ebenfalls nicht. Als praxistaugliche Anwendung bezieht sich die DK vielmehr ausgerechnet auf das Produkt kontoblick.de[298], das, bis zum Marktaustritt des Dienstleisters nach Insolvenz, den Zugang zu den Kontodaten des Kunden über eine Java-Applikation realisiert hat und die Kundendaten dann auf Server des Unternehmens gespeichert, dort für den Kunden grafisch aufbereitet und anschließend in anonymisierter Form zu Marktforschungszwecken verwendet hat.[299] Solche Dienstleistungen stellen aber gerade nicht sicher, dass PIN und TAN bei Nutzung des Produktes vor einer ungewollten missbräuchlichen Verwendung geschützt sind.

356. Die Beteiligten stellen stattdessen einen unzulässigen Zusammenhang zwischen dem Angebot eines am Markt tätigen bankenunabhängigen Bezahlverfahrens im Internethandel und der Gefährdungen des Online-Bankings durch kriminelle Vorgehensweisen her, wenn sie darauf verweisen, die Ausgestaltung der OBB in der hier beanstandeten Form sei als Reaktion auf zunehmende Gefährdungen des Online-Bankings durch kriminelle Angriffe zu betrachten.

357. Die DK konkretisiert das Verbot der Eingabe von PIN und TAN ausdrücklich in Bezug auf Online-Händlerseiten. Im Zusammenhang mit Online-Händlern bezieht sich die Weitergabe von PIN und TAN nur auf Bezahlprozesse und damit auf eine Nutzung von Zahlungsauslösediensten. Neben den bankenunabhängigen Zahlungsauslösediensten ist keine Anwendung im Zusammenhang mit Online-Händlern ersichtlich, bei der die Eingabe

---

296 Schreiben der DK v. 09.08.2011, Bl. 1706 d.A.
297 Vgl. Darstellung des Umgangs der DK mit Produkten der Buhl Data, Rz. 134ff.
298 Vgl. Rz. 161ff.
299 Schreiben der DK v. 09.08.2011, Bl. 1709f. d.A.

von PIN und TAN vorgesehen ist und deren Nutzung durch die Ausgestaltung der Sonderbedingungen ausdrücklich als zustimmungspflichtig geregelt wird.

358. Ein einheitliches und stringentes Sicherheitskonzept würde aber erfordern, dass umfassende Regelungen zum Umgang mit Dienstleistern gefunden werden, die entweder zu einer Zulassung von Dienstleistern nach angemessenen und für alle geltenden Regelungen führen oder die Formulierung geeigneter und abstrakter Sicherheitskriterien zum Ergebnis haben. Das Intermediärskonzept, in dem solche Überlegungen angestellt worden sind, wurde nicht zu einem umfassenden praxistauglichen Sicherheitskonzept ausgearbeitet. Die Arbeit hieran wurde in den Arbeitsgruppen der DK eingestellt, nachdem der Umgang mit bankenunabhängigen Zahlungsauslösediensten erschwert wurde, die Formulierung der OBB ansonsten die Nutzung bankennaher Angebote aber weiter ermöglichte.

c) Der wirtschaftliche und rechtliche Zusammenhang, in dem die Sorgfaltspflichten stehen

359. Bei der Beurteilung der Frage, ob eine Koordinierung zwischen Unternehmen schon ihrer Natur nach schädlich für das Funktionieren des Wettbewerbs ist, sind relevante Anhaltspunkte bezüglich des wirtschaftlichen oder juristischen Zusammenhangs, in den sich diese Koordinierung einfügt, zu berücksichtigen. Hierzu gehören die Art der fraglichen Dienstleistungen sowie die Struktur des betreffenden Marktes und der auf diesem bestehenden tatsächlichen Bedingungen.[300]

360. Neben dem Inhalt der Sorgfaltspflichten belegen auch die tatsächlichen Marktbedingungen, dass die Sorgfaltspflichten die Beschränkung des Wettbewerbs auf dem Markt für Bezahlverfahren im Internethandel bezwecken.

aa) Bestehender rechtlicher Rahmen bei der Ausgestaltung der Sorgfaltspflichten

361. Die Tätigkeit von Zahlungsauslösediensten unterlag bei Erarbeitung und Beschluss der Sorgfaltspflichten im Jahr 2009 keiner rechtlichen Beschränkung. Zahlungsauslösedienste unterfielen zu dieser Zeit keiner staatlichen Aufsicht über Zahlungsdienste. Die Kreditwirtschaft hat die rechtlichen Freiräume zur Ausgestaltung von Sorgfaltspflichten genutzt, um Wettbewerber vom Markt auszuschließen.

---

[300] Europäischer Gerichtshof, Urteil vom 11.09. 2014 in der Rechtssache C-67/13 P, Groupement des cartes bancaires (CB)/Kommission, zitiert nach curia.europa.eu, Rz.53f.

362. Bei der Erarbeitung der Sonderbedingungen bestand keine rechtliche Regelung, der zufolge das Angebot von Zahlungsauslösediensten zum damaligen Zeitpunkt zwingend zu unterbinden war. Die nationalen gesetzlichen Regelungen sahen für die Kreditinstitute Spielräume zur Ausgestaltung ihrer Allgemeinen Geschäftsbedingungen vor, wie die sichere Verwendung von Personalisierten Sicherheitsmerkmalen erfolgen kann. In diesem Zusammenhang sehen gesetzliche Regelungen und deren auszugestaltende Spielräume keine abweichende Behandlung von Diensten vor, je nachdem ob diese von Banken, banknahen oder aber bankfremden Dienstleistern angeboten werden. In jedem Fall dürfen in Folge des Inkrafttretens der PSD2 bestehende Zahlungsauslösedienste ihre Tätigkeit weiterhin am Markt anbieten. Daran werden sie durch die beanstandeten Formulierungen in den OBB aber gehindert.

363. Die beschlossenen Sorgfaltspflichten in den OBB beziehen sich nur auf bankfremde Zahlungsauslösedienste, nicht auf solche, mit denen Banken in einer vertraglichen Verbindung stehen. Soweit sich die DK auf die durch die Umsetzung der PSD verändernden rechtlichen Rahmenbedingungen bezieht,[301] die eine Überarbeitung der Online-Banking-Bedingungen erforderlich machten, boten sich ihr weite Spielräume bei der Ausgestaltung der vom Gesetzgeber nicht abschließend geregelten Sachverhalte.

364. Die gesetzliche Regelung in § 675l Abs. 1 BGB sieht vor, dass Kunden Personalisierte Sicherheitsmerkmale vor unbefugtem Zugriff schützen müssen, lassen aber offen, was als „unbefugt“ gilt. Da sich aber aus dem Umgang mit PIN und TAN Auswirkungen auf die Verteilung der Haftung zwischen Kreditinstitut und Kunde (§ 675v Abs. 1 BGB) ergeben, obliegt den Kreditinstituten die Verpflichtung, mit ihren Kunden eine Vereinbarung zu treffen, wie ein Zahlungsauthentifizierungsinstrument sicher verwahrt wird (Art. 248 § 4 Abs. 1 Nr. 5 a EGBGB als Umsetzung von Art. 42 Nr. 5a PSD). Bei der Ausgestaltung der Pflichten der Kunden hat der Gesetzgeber berücksichtigt, dass die Pflichten des Kunden nicht abschließend gesetzlich geregelt werden können und sich ein Teil der Pflichten aus der vertraglichen Vereinbarung zwischen dem Kunden und dem Kreditinstitut ergibt, da nur das Kreditinstitut die Besonderheiten bei der Verwendung von PIN und TAN gebührend berücksichtigen kann. Es gab insoweit lediglich Vorgaben des Gesetzgebers, dass Kunden Informationen zur Sicherung von Personalisierten Sicherheitsmerkmalen zur Verfügung gestellt werden müssen, inhaltliche Vorgaben für die Kreditwirtschaft waren damit nicht verbunden.

---

[301] Schriftsatz Oppenländer Rechtsanwälte vom 29.07.2014, Bl. 6092f. d.A.

365. Konkretisierungsbedürftige gesetzliche Bestimmungen bzw. Spielräume bei der Umsetzung der rechtlichen Vorgaben in Allgemeine Geschäftsbedingungen sind kartellrechtskonform auszulegen und auszugestalten. Die konkrete Ausgestaltung der Sorgfaltspflichten durch die Beteiligten spiegeln dagegen den Willen der DK und ihrer Mitglieder wider, bankenunabhängige Zahlungsauslösedienste aus dem Markt für Bezahlverfahren im Internethandel zu drängen.

366. Bei der Ausgestaltung dieser Regelungen kann sich die DK nicht darauf berufen, dass durch die kartellrechtlich relevante Vereinbarung die Einhaltung andere Rechtsgüter, wie z.B. Datenschutz oder Urheberrecht sichergestellt wird.[302] Sofern solche und andere Rechtsbereiche für die Tätigkeit eines Zahlungsauslösedienstes Bedeutung erlangen, obliegt die Überwachung der Einhaltung gesetzlicher Vorschriften den Behörden und Gerichten und rechtfertigt keine Kartellabsprache zwischen privaten Unternehmen oder Unternehmensvereinigungen.[303]

367. Der rechtliche Rahmen hat sich während des Verfahrens geändert: Die früher geltenden Richtlinien und Verordnungen über Zahlungsdienste wurden im Jahr 2015 modifiziert und durch eine neue Richtlinie ergänzt. Spätestens nach Umsetzung der vom europäischen Gesetzgeber überarbeiteten PSD2 im Jahre 2018 wird jeglicher Spielraum für die deutsche Kreditwirtschaft zur Einschränkung am Markt tätiger Zahlungsauslösedienste wegfallen.

368. Die PSD2 regelt die Aufsicht über Zahlungsdienste neu. Wesentliche Änderungen ergeben sich hinsichtlich der Erfassung neuer Arten von Zahlungsdiensten, die zukünftig der Aufsicht unterstellt werden. Für die erforderlichen Anpassungen der nationalen Rechtsvorschriften zur Anwendung der neuen Regeln haben die Mitgliedstaaten zwei Jahre Zeit, also bis zum 13.01.2018.

369. Vor Ablauf der Umsetzungsfrist entfalten die Regelungen der PSD2 zwar keine unmittelbare Wirkung gegenüber Kreditinstituten, hierzu bedarf es noch der Umsetzung in nationales Recht durch den deutschen Gesetzgeber. Allerdings geht von der neuen Richtlinie eine Vorfeldwirkung aus, die an den eindeutig formulierten Zielen sowie an der in Erwägungsgrund 33 der PSD2 genannten Handlungsanweisung an mitgliedstaatliche

---

302 Schriftsatz. Oppenländer Rechtsanwälte, 29.07.2014, Bl. 6190ff. d.A.

303 Urteil des EuG in der Rechtssache C-68/12 vom 7.02.2013, Slovenska sporitel, Rz. 20, (zitiert nach: http://curia.europa.eu).

Behörden bei der zukünftig vorzunehmenden Entscheidung über die Zulassung von Zahlungsauslösediensten anknüpft.[304]

370. Erklärtes Ziel der PSD2 ist es, die Kontinuität im Markt bis zur Umsetzung der Richtlinie in nationales Recht sicherzustellen und gleichzeitig bestehenden Dienstleistern unabhängig von ihrem Geschäftsmodell die Möglichkeit zu geben, ihre Dienste in einem klaren und harmonisierten Rechtsrahmen anzubieten. Unbeschadet der Notwendigkeit, die Sicherheit von Zahlungsvorgängen und den Schutz der Verbraucher vor nachweislichen Betrugsrisiken zu gewährleisten, sollen die Mitgliedstaaten, Kommission, Europäische Zentralbank und die Europäische Aufsichtsbehörde (EBA) bis zur Anwendung dieser Regelungen, das heißt, bis zur Umsetzung in nationales Recht, den fairen Wettbewerb im Markt sicherstellen. Dabei soll eine ungerechtfertigte Diskriminierung der vorhandenen Marktteilnehmer vermieden werden.[305]

371. Die aus dem Effektivitätsgebot (effet utile) des Artikel 4 AEUV erwachsende Pflicht der (nationalen) Verwaltungen in Bezug auf das von der Union vorgesehene Regelungsziel[306] gebietet es daher, dass auch die nationalen Kartellbehörden bei der Anwendung der europäischen sowie nationalen Wettbewerbsregeln das Regelungsziel der PSD2 beachten. Das bedeutet, dass das Bundeskartellamt als nationale Wettbewerbshörde keine Entscheidungen trifft bzw. unterlässt, die den Zweck dieser Richtlinie ernstlich gefährden würde, sofern das nationale Recht dies zulässt (keine Vorfeldwirkung contra legem). Jegliche ungerechtfertigte Diskriminierung von Zahlungsauslösediensten durch eine kartellbehördliche Verfügung oder durch ein Unterlassen eines kartellbehördlichen Einschreitens ist demnach zu vermeiden.

372. Eine solche Diskriminierung ergibt sich bereits daraus, dass die von den Bankenverbänden vereinbarten Sorgfaltspflichten für das Online-Banking nach wie vor die Weitergabe von PIN und TAN auf Online-Händlerseiten untersagen. Damit verbleibt durch die bestehenden Regelungen auf Seiten der Nutzer der Dienstleistungen zumindest die Ungewissheit, ob die Nutzung rechtlich unzulässig ist. Auch mit der Tatsache, dass die bestehenden Regelungen als Basis für Klagen gegen Zahlungsauslösedienste genutzt werden können, sind Diskriminierungen von Marktteilnehmern verbunden.

---

304 Vgl. zur Vorffeldwirkung von Richtlinien: Grabitz/Hilf/Nettesheim, Nettesheim, Das Recht der Europäischen Union, Band 3, Art. 288 RN 118.

305 Erwägungsgrund Nr. 33 und Art. 115 Abs. 6 PSD2.

306 Vgl. hierzu: Grabitz/Hilf/Nettesheim, von Bogdandy/Schill, Das Recht der Europäischen Union, Band 3, Art. 4 RN 90.

373. Aus der Reichweite der PSD2 heraus sind diese diskriminierenden Regelungen daher in den Sonderbedingungen durch die deutschen Aufsichtsbehörden abzustellen.

bb) Tatsächliche Bedingungen auf dem Markt und die Struktur des Marktes

374. Auch die tatsächlichen Marktbedingungen belegen, dass die Ausgestaltung der Sorgfaltspflichten eine unmittelbare Einschränkung des Wettbewerbs auf dem Markt für Internetbezahlverfahren bezweckt. Die Regelungen beziehen sich auf innovative, wachsende Wettbewerber auf dem Markt, auf dem Kreditinstitute bisher weitgehend nur durch die Nutzung von Kreditkarten Umsätze erzielen konnten, deren ungeschmälerte Realisierung durch den aufkommenden Wettbewerb in Frage gestellt wird.

375. Den größten Verbreitungsgrad unter den Bezahlverfahren im Internethandel erreichen derzeit PayPal und Kreditkarten, wobei lediglich geringfügige Unterschiede zwischen den Kreditkartensystemen von VISA und Mastercard bestehen. Nur zwei weitere, dem Markt zuzurechnende Verfahren erreichen noch einen Verbreitungsgrad von mehr als 50%, d.h. sie werden von mehr als der Hälfte der Online-Händler angeboten. Hierzu gehören die Zahlung per Nachnahme und der Zahlungsauslösedienst Sofort. Alle anderen Verfahren, insbesondere auch das von der Kreditwirtschaft angebotene Verfahren giropay, ereichten bisher deutlich geringere Marktdurchdringungsraten.[307] Inwieweit das von der Kreditwirtschaft gemeinsam erarbeitete neue Bezahlverfahren Paydirekt eine stärkere Marktdurchdringung erreichen wird, ist wegen des gerade erst angelaufenen Einführungszeitraums zum jetzigen Zeitpunkt noch nicht abzusehen.

376. Das Angebot von Zahlungsauslösediensten ergibt sich aus dem Bedarf der Online-Händler nach günstigen, sicheren und einfachen Bezahlverfahren. Online-Händler bieten jeweils mehrere Bezahlverfahren an. Der Händler, dem für die Inanspruchnahme und Abwicklung eines Kaufvorgangs durch ein Bezahlverfahren Kosten entstehen, hat nur einen geringen Einfluss auf die Wahl des jeweiligen Verfahrens durch den Kunden. Allerdings kann ein Händler zum Beispiel durch eine differenzierte Ausgestaltung der Höhe der Versandkosten Einfluss auf die Wahl des Verfahrens nehmen und wird dies häufig auch tun, um seine Kosten für die Bezahlverfahren entweder zu beschränken oder zumindest teilweise zu refinanzieren.

---

[307] E-Commerce-Markt Deutschland 2014, Marktstudie der 1.000 umsatzstärksten B2C-Onlineshops für physische Güter, EHI Retail Institute, Köln, S. 42.f [\\10.10.200.11\Gruppen\b4\Jakobi\Fälle\1 - B4-71-10 - Sofortueberweisung-de\3 - Ermittlungen - Scans\EHI_2014].

Bezahlverfahren	Angegebene Ø-Gesamt-nutzungskosten in %	Angegebene Ø-Ausfälle in %	Summe der angegebenen Transaktionszahlen
Zahlung bei Abholung	0,39 [0-2,5]	2,9	215.353
Vorauskasse	0,42 [0-3]	0,0	261.758
Rechnung (White Label)	0,83 [0,1-2,5]	1,1	10.634.529
Sofortüberweisung	0,93 [0,5-1,5]	0,0	246.536
Lastschrift	1,24 [0,05-4]	1,1	462.578
giropay	1,37 [0,6-2,2]	0,0	28.668
Nachnahme	1,41 [0,4-5]	0,0	717.946
Bezahlen über Amazon	1,60 [1,5-1,8]	Keine Angabe	Keine Angabe
PayPal	1,87 [1-4]	0,2	1.543.757
Finanzierung	2,19 [0,1-5,9]	1,2	2.675.469
Kreditkarte	2,28 [1-4]	0,4	693.215
Rechnungskauf (Brand/Marke)	2,80 [1,5-5]	0,3	175.270

Hinweis: Gilt nur für Unternehmen mit einem Umsatz von mehr als einer Million Euro

Abb. 8 - Ergebnisse des EHI Retail Institut zu den Durchschnittskosten von Bezahlverfahren im Internethandel, E-Commerce-Markt Deutschland 2014

377. Neben PayPal, der Finanzierung und der Inanspruchnahme von Dienstleistern für die Abwicklung des Rechnungskaufs sind Kreditkarten derzeit das mit Abstand teuerste Bezahlverfahren für Online-Händler. Auch die Akzeptanz von giropay ist für den Händler mit deutlich höheren Kosten verbunden, als die Abwicklung von Zahlungen z.B. über das von der Sofort angebotene Bezahlverfahren.

378. Durch die Nutzung von Kreditkarten, für die das EHI Retail Institute einen umsatzbezogenen Marktanteil von rund 15% ermittelt, realisieren die kartenausgebenden Kreditinstitute Erträge aus der vom Händler zu zahlenden Interchange Fee. Demgegenüber erhalten die Kreditinstitute bei der Nutzung bankenunabhängiger Zahlungsauslösedienste keine Erträge.

379. Mit der Verbreitung eines Zahlungsauslösedienstes und den in Rz. 376 dargestellten Steuerungsmöglichkeiten der Händler drohen der Kreditwirtschaft Ertragsverluste aus ihren originären Produkten.[308] Soweit Leistungen der bankenunabhängigen Zahlungsauslösedienste angeboten werden, profitieren diese von der Bereitschaft des Händlers, im Vergleich zu PayPal oder Kreditkarten für ihn günstigere Produkte anzubieten und seine Kunden im Rahmen ihrer Möglichkeiten in Richtung günstigerer Bezahlverfahren zu lenken.

---

[308] Nach Inkrafttreten der Verordnung über Interbankenentgelte für kartengebundene Zahlungsvorgänge liegt die Obergrenze für Interbankenentgelte bei Kreditkartenzahlungen bei 0,3% des Umsatzes.

380. Das Verbot der Nutzung von Zahlungsauslösediensten ohne die Zustimmung durch das jeweils kontoführende Kreditinstitut schützt daher vor allem die Ertragsinteressen der den Spitzenverbänden angeschlossenen Kreditinstituten gegenüber bankenunabhängigen Dienstleistern. Ein solches Vorgehen über die Ausgestaltung der beanstandeten Sorgfaltspflicht in den OBB war aus Sicht der DK notwendig geworden, um Verfahren, die nicht bereits auf der Grundlage bilateraler „Diskussionen“ zum Marktaustritt gebracht werden konnten (vgl. Rz.289ff.), in ihrer Ausbreitung und ihrem wirtschaftlichen Erfolg einzuschränken.

381. Soweit die DK neben der Ausgestaltung der Online-Banking-Bedingungen konkrete Überlegungen zum Umgang mit Intermediären, die Dienstleistungen im Zusammenhang mit dem Online-Banking anbieten, angestellt hat, zielten diese auch auf die Frage ab, [redacted].[309] Dies verdeutlicht, dass die Generierung bzw. Erhaltung von Ertragsquellen bei der Beurteilung der Tätigkeit von Intermediären eine zentrale Rolle spielte.

382. Die Strategie, die Tätigkeit bankenunabhängiger Zahlungsauslösedienste zu unterbinden, ist daher auch vor dem Hintergrund der Erträge zu beurteilen, die den Kreditinstituten unmittelbar aus der Abwicklung von Zahlungen im Internethandel über bankengestützte Zahlungsverfahren zufließen.

d) Die Absicht der Beteiligten zum Ausschluss bestehender Bezahlverfahren im Internethandel vom Markt

383. Die DK führt mit der Ausgestaltung der Sorgfaltspflichten ihr Vorgehen gegen bankenunabhängige Zahlungsauslösedienste fort, deren System die Nutzung von Kontoinformationen des Kunden und in diesem Zusammenhang die Eingabe von PIN und TAN auf Internetseiten von Online-Händlern vorsieht. Die Erarbeitung der Online-Banking-Bedingungen ist vor dem Hintergrund des Vorgehens der DK gegen Bezahlverfahren im Internethandel auf der Basis der früheren AGB-Regelungen zu sehen. Die oben dargestellten Schriftwechsel mit L’Tur, T-Online und Promido belegen,[310] dass es der DK dabei vor allem darum ging, das Angebot von bankenunabhängigen Zahlungsauslösediensten auf dem Markt für Bezahlverfahren im Internethandel auf der Grundlage der bestehenden AGB-Regelungen branchenweit zu unterbinden. Auch

---

309 [redacted]

310 Vgl. Rz.173ff.

gegenüber der Stiftung Warentest wurde die Tätigkeit der Sofort auf der Basis der 2009 verabschiedeten neuen Online-Banking-Bedingungen als Verstoß gegen die bestehenden Sorgfaltspflichten dargestellt (vgl. Rz. 233ff.).

384. In der Auseinandersetzung mit den Gefahren und einem möglichen Umgang der DK mit Dienstleistern, die Kenntnis von PIN und TAN erlangen (Intermediäre), spricht sich die DK dafür aus, auf geschäftspolitischer und rechtlicher Ebene Lösungen zu finden, z.B. die Einführung eines eigenen kreditwirtschaftlichen Bezahlverfahrens im Internethandel oder entsprechende Sorgfaltspflichten in den Kundenbedingungen. Ziel ist dabei, dass auch zukünftig PIN und TAN auf keinen Fall bei Intermediären eingegeben werden dürfen (vgl. Rz. 194).

385. Mit dem Verbot der Eingabe von PIN und TAN auf anderen als den gesondert vereinbarten Internetseiten schafft die DK eine rechtliche Grundlage für ihre über einen langen Zeitraum verfolgten Anstregungungen, die Tätigkeit von bankenunabhängigen Zahlungsauslösediensten auf dem Markt für Bezahlverfahren im Internethandel zu unterbinden, ohne zugleich die Nutzung der aus dem Bankensektor stammenden Produkte zu verhindern.[311] In der entsprechenden Arbeitsgruppe wurde insbesondere auch auf bereits geführte Diskussionen mit der Sofort verwiesen und auf das Ziel, die Sorgfaltspflichten so zu formulieren, dass sich daraus keine erneuten Diskussionen mit Anbietern von Zahlungsauslösediensten[312] und keine Diskussionen mit dem Bundeskartellamt über Wettbewerbsbeschränkungen ergeben.[313]

---

311 Vgl. Rz. 214 ff.

312 Vgl. Rz.217.

313 [redacted]

4. Die Beschlüsse bewirken eine Beschränkung des Wettbewerbs

386. Die konkrete Ausgestaltung der Sorgfaltspflichten in den OBB bewirkt jedenfalls auch eine Beschränkung des Wettbewerbs.

387. Die Prüfung der Wirkung des Beschlusses erfolgt hilfsweise. Soweit eine Regelung, die dazu führt, die Tätigkeit von Zahlungsauslösediensten am Markt zu unterbinden, eine ihrem Wesen nach bezweckte Wettbewerbsbeschränkung darstellt, ist die Anwendbarkeit von Art. 101 Abs. 1 AEUV und § 1 GWB nicht vom Ergebnis der Prüfung ihrer Wirkung abhängig. Der Zweck und die Wirkung einer Vereinbarung stehen alternativ zueinander und müssen nicht kumulativ erfüllt sein.[314]

388. Bei der Wirkung einer Vereinbarung ist auf die bestehenden wirtschaftlichen, rechtlichen und tatsächlichen Markt- und Wettbewerbsverhältnisse abzustellen, wobei es auf die Art der Vereinbarung, die tatsächliche Umsetzung in der Praxis und die Marktmacht der Beteiligten ankommt.[315]

389. Auswirkungen auf die Wettbewerbsposition Dritter auf dem Markt reichen zur Feststellung der wettbewerbsbeschränkenden Wirkung eines Beschlusses aus, wobei die Wirkung ursächlich auf den Beschluss zurückzuführen sein muss.[316]

390. Die Banken nutzen ihre Stellung als Anbieter von Girokonten gezielt aus, um kollektiv Vorgaben für die Nutzung des Girokontos im Online-Banking-Verfahren zu machen, die bankenunabhängige Anbieter von Zahlungsauslösediensten vom Markt verdrängen. Die wettbewerbsbeschränkende Wirkung auf dem Markt für Bezahlverfahren im Internethandel ergibt sich aus dem branchenweiten einheitlichen Vorgehen zur Ausgestaltung, Umsetzung und Durchsetzung der Regelungen.

391. Die in der DK zusammenarbeitenden Verbände vertreten die Gesamtheit der in Deutschland tätigen Kreditinstitute. Ihre Tätigkeit führt zu bundesweiten Wirkungen auf dem Markt für Bezahlverfahren im Internethandel. Die von der DK und ihren Spitzenverbänden erarbeiteten OBB, die die Tätigkeit der Zahlungsauslösedienste de facto ausschließt, werden von nahezu allen Kreditinstituten verwendet.[317] Insgesamt wurden in Deutschland im Jahr 2014 mehr als 56 Mio. Girokonten mit Onlinezugang bei

---

314 Vgl. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Bd. 2 Europäisches Kartellrecht, 12. Aufl., Artikel 101 AEUV, Rz. 218f.

315 Vgl. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Bd. 2 Europäisches Kartellrecht, 12. Aufl., Artikel 101 AEUV, Rz. 233.

316 Vgl. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Bd. 2 Europäisches Kartellrecht, 12. Aufl., Artikel 101 AEUV, Rz. 234.

317 Vgl. Rz. 219ff.

deutschen Kreditinstituten geführt.[318] In Folge der bestehenden Sorgfaltspflichten in den Online-Banking-Bedingungen wurde dieses Marktpotential dem Wettbewerb durch Zahlungsauslösedienste entzogen bzw. die erfolgreiche Verbreitung und das Wachstum von Zahlungsauslösediensten erheblich erschwert.

392. Die DK konkretisiert in Bezug auf die Nutzung bankenunabhängiger Zahlungsauslösedienste eine gesetzliche Regelung in der Form, dass Kunden diese Dienstleistungen nicht nutzen können, ohne gegen die aus ihrer Sicht geltenden vertraglichen Regelungen zu verstoßen. Die Sorgfaltspflichten zielen darauf ab, das Angebot bankenunabhängiger Zahlungsauslösedienste als rechtswidriges Angebot rechtlich sanktionieren zu können, wie von der Beigeladenen zu 6. in der Begründung der Klage vor dem Landgericht Köln vorgetragen wurde („Verleitung zum Vertragsbruch"). Die Regelungen wirken sich somit unmittelbar nachteilig auf die Geschäftsmöglichkeiten bankenunabhängiger Zahlungsauslösedienste aus.

393. Die Regelungen wirken sich auf die Nutzung von Zahlungsauslösediensten aus, deren Markttätigkeit von der DK seit mehr als 10 Jahren unter Verweis auf die bestehenden Regelungen angegriffen wurde.[319] Die Regelungen beziehen sich auf Zahlungsauslösedienste auf dem Markt für Bezahlverfahren im Internethandel, von denen in den letzten Jahren Preiswettbewerb zu Lasten bankennaher Verfahren ausgegangen ist. Auch wenn die Marktanteile von Zahlungsauslösediensten im Vergleich zu den großen und etablierten Systemen noch verhältnismäßig gering sind, handelt es sich um stetig wachsende Marktanteile. Die kartellrechtswidrige Vereinbarung der Spitzenverbände der DK hat, soweit die Sorgfaltspflichten darauf gerichtet sind, die Nutzung von Zahlungsauslösediensten zu unterbinden, den Wettbewerb nicht vollständig unterbinden können, die Entwicklung des Wettbewerbs über Jahre hinweg aber tatsächlich erheblich beeinträchtigt. Die Marktanteile sind daher insbesondere wegen der Wettbewerbsbeschränkungen noch niedrig.

394. Die Regelungen der DK haben in der Vergangenheit Innovationen im Bereich der Bezahlverfahren im Internethandel unterbunden[320] oder erschwert[321]. Das strategische und koordinierte Vorgehen der DK hat zudem bereits dazu geführt, dass Unternehmen aus dem Markt ausgeschieden sind und somit Innovationen und Wettbewerb durch diese

---

318 https://www.bundesbank.de/Redaktion/DE/Downloads/Statistiken/Geld_Und_Kapitalmaerkte/Zahlungsverkehr/zvs_daten.pdf?__blob=publicationFile, Stand 19.04.2016.

319 Vgl. Rz. 173ff.

320 Vgl. Vorgehen gegen die von L'tur angebotenen Dienstleistungen unter Rz. 289.

321 Vgl. Vorgehen gegen Deutsche Telekom, Rz. 176 und Sofort, Rz. 290.

Dienstleister unterbunden wurden ([redacted]). Die Wirkung der Erarbeitung der Sorgfaltspflichten und des Vorgehens der DK gegen Bezahlverfahren, die trotz der Regelungen in den AGB angeboten worden sind, liegt in der Reduzierung des Wettbewerbsdrucks auf Produkte der Kreditwirtschaft und bankennaher Produkte (giropay, Paydirekt, Kreditkarten)[322] durch Innovationen und in der Beschränkung des Wettbewerbs zumindest auf dem Markt für Bezahlverfahren im Internethandel. Ohne die Regelung hätten Kunden von Online-Händlern keine Sorge haben müssen, gegen vertragliche Bestimmungen zu verstoßen, wenn sie Zahlungsauslösedienste zur Bezahlung auswählen. Eine Steuerungswirkung der Online-Händler auf für sie günstigere Bezahlverfahren wären von Kunden in größerem Umfang angenommen worden. Bezahlverfahren von Zahlungsauslösediensten hätten eine weitere Verbreitung und höhere Akzeptanz erreicht.

395. Die Wirkung der Wettbewerbsbeschränkung ergibt sich schließlich auch daraus, dass die Regelungen dazu führen, dass Zahlungsauslösedienste neben der erfolgreichen Umsetzung ihres Geschäftsmodells Ressourcen aufwenden müssen, um sich gegen Angriffe von Seiten der Bankenverbände, Kreditinstitute und Wettbewerber gegen ihre wettbewerbliche Tätigkeit zur Wehr zu setzen. Exemplarisch steht hierfür die Presseerklärung der DK gegenüber der Stiftung Warentest, in der das Produkt der Sofort mit widerrechtlichen Phishing-Angriffen in Verbindung gebracht wurde.[323] Erst nach Einschaltung eines Rechtsbeistands, der zur Abgabe einer Unterlassungserklärung aufforderte, konnte die Verwendung der Formulierung für die Zukunft unterbunden werden. Gleiches gilt für das Verhalten einzelner Kreditinstitute, die auf die Rechtswidrigkeit der Verwendung von Zahlungsauslösediensten gegenüber eigenen Kunden hinweisen oder der Klage von giropay.[324] Schließlich hat die beanstandete Regelung in den OBB der DK und den Spitzenverbänden der Kreditwirtschaft Zeit verschafft, mit „Paydirekt“ ein eigenes Produkt zu entwickeln und auf dem Markt zu platzieren, das ein direktes Konkurrenzprodukt für bestehende Zahlungsauslösedienste ist. Durch die jahrelange „Diskreditierung“ von bestehenden Zahlungsauslösediensten haben DK und die Spitzenverbände der Kreditwirtschaft erfolgreich ein negatives Image für derartige Produkte geschaffen, das es ihnen jetzt erlaubt, ihr eigenes Produkt „Paydirekt“ als von Banken betriebenes und daher besonders vertrauenswürdiges Konkurrenzprodukt am Markt zu plazieren.

---

322 Vgl. Rz. 378.
323 Vgl. Rz. 235.
324 Vgl. Rz. 238ff.

5. Spürbarkeit

396. Die mit den in den Online-Banking-Bedingungen enthaltenen Sorgfaltspflichten der Kunden bezweckte oder jedenfalls bewirkte Wettbewerbsbeschränkung auf dem Markt für Bezahlverfahren im Internethandel in Deutschland ist spürbar.

397. Eine Vereinbarung, die einen wettbewerbswidrigen Zweck, bankenunabhängige Zahlungsauslösedienste vom bundesweiten Markt für Bezahlverfahren im Internethandel zu drängen, verfolgt, stellt ihrer Natur nach und unabhängig von ihren konkreten Auswirkungen eine spürbare Beschränkung des Wettbewerbs dar.[325] Der Ausschluss von Wettbewerbern hat einen unmittelbaren Effekt auf die Marktstruktur und unterbindet die Fortentwicklung von Märkten durch Innovationen zum Vorteil der Marktgegenseite und der Verbraucher, die durch den Wettbewerb eine größere Auswahl unterschiedlicher Produkte erlangen und sich einem stärkeren Preiswettbewerb der Anbieter von Bezahlverfahren im Internethandel gegenüber sehen.[326]

398. Auch bei einer hilfsweise angenommenen bewirkten Wettbewerbsbeschränkung ist das Kriterium der Spürbarkeit erfüllt. Die Vereinbarung geht über das hinaus, was unter einer lediglich theoretisch denkbaren Beeinflussung des Marktes verstanden werden kann. Die Außenwirkungen der hier zu prüfenden Sorgfaltspflichten sind deshalb spürbar, weil die DK durch deren Beschluss Wettbewerber auf dem bundesweiten Markt für Bezahlverfahren im Internethandel in ihrer Tätigkeit einschränkt und darauf abzielt, diese vom Markt zu verdrängen. Die beanstandete Sorgfaltspflicht nimmt Einfluss auf die bestehende Marktstruktur, indem die Angebotsvielfalt für Händler als Nachfrager von Bezahlverfahren im Internethandel verringert wird.

399. Die Sorgfaltspflichten nehmen Einfluss auf mehr als 50 Mio. Girokontokunden, die als Nutzer von Bezahlverfahren im Internethandel auftreten können. Sie wirken sich auf Zahlungsauslösedienste aus, die, trotz aller Behinderungen durch die DK, eine verhältnismäßig große und stetig steigende Marktdurchdringung in dem dynamisch wachsenden Internethandel in den letzten Jahren erreicht haben.

---

[325] Urteil des Gerichtshofs der Europäischen Union v. 13.12.2012, Expedia Inc./Autorité de la concurrence, Rz. 37, verfügbar über www.curia.eu.

[326] Zahlungsauslösedienste „bieten sowohl Händlern als auch Verbrauchern eine kostengünstige Lösung und ermöglichen es Verbrauchern, auch dann online einzukaufen, wenn sie nicht über Zahlungskarten verfügen," vgl. Erwägungsgrund 29, PSD2.

400. Schließlich werden durch die Sorgfaltspflichten auch Ertragsinteressen der von den Spitzenverbänden der deutschen Kreditwirtschaft vertretenen Kreditinstitute z.B. als Herausgeber von Kreditkarten gesichert.

401. Der Beschluss der in der DK zusammenarbeitenden Spitzenverbände der Kreditwirtschaft bezieht sich insgesamt auf über 50 Mio. Online-Girokonten in Deutschland (vgl. Rz. 42), die als potentielle Nutzer von Bezahlverfahren im Internethandel und von Zahlungsauslösediensten in Frage kommen. Durch die Vorgabe von Sorgfaltspflichten wird der Markt für Bezahlverfahren in einer signifikanten Weise beeinflusst, da für den größten Teil der Kunden damit eine mögliche Bezahlmethode ausgeschlossen wird, was sich auch auf die Wettbewerbsmöglichkeiten von Zahlungsauslösediensten gegenüber anderen Bezahlverfahren auswirkt. Bei der Beurteilung der Frage, ob die Wettbewerbsbeschränkung die Spürbarkeitsanforderungen erfüllt, kann nicht allein auf die derzeitige Marktdurchdringung von Zahlungsauslösediensten und den Umfang abgestellt werden, in dem Kunden solche Verfahren tatsächlich nutzen. Das Verbot zur Eingabe Personalisierter Sicherheitsmerkmale hat sowohl bei Händlern als auch bei Nutzern zu Verunsicherungen hinsichtlich der rechtlichen Zulässigkeit solcher Verfahren geführt. Das Nutzungsverhalten der Kunden ist bisher auch deshalb gering geblieben, weil die Sorge vor einem möglichen Vertragsbruch bestand und die DK und die Kreditinstitute diesen Anschein durch Pressearbeit und Veröffentlichungen in der Vergangenheit gefördert haben.

402. Von Zahlungsauslösediensten geht Wettbewerbsdruck auch auf etablierte Bezahlverfahren wie PayPal und Kreditkartenzahlung aus. Kreditkarten, durch die kartenherausgebende Kreditinstitute Erträge generieren, werden durch die Marktdurchdringung von Zahlungsauslösediensten und deren wettbewerblichen Erfolgen in ihrer Marktstellung angegriffen. Im Jahre 2013 wurden Kreditkarten in mehr als 80% der Online-Shops als Bezahlverfahren angeboten bei steigender Verbreitung im Jahresvergleich zu 2012.[327] Sofortüberweisung.de erreichte im Jahr 2011 eine Verbreitung von 36%[328] und konnte diesen Wert bis 2013 auf annähernd 50%[329] steigern. Insbesondere durch die Preisgestaltung gegenüber dem Händler und die Sicherheit des

---

[327] Online-Payment-Studie 2014 Daten, Fakten, Hintergründe und Entwicklungen, Jahresvergleich der Sichtbarkeit der Zahlungsmittel in den Top-1.000-Onlineshops in den Jahren 2012 und 2013, EHI Retail Institute e.V., Köln, S. 27.

[328] Online-Payment-Studie 2012 Daten, Fakten, Hintergründe und Entwicklungen, Angebotene Zahlungsverfahren in den Top-Online Shops 2011, EHI Retail Institute e.V., Köln, S. 21.

[329] Online-Payment-Studie 2014 Daten, Fakten, Hintergründe und Entwicklungen, Jahresvergleich der Sichtbarkeit der Zahlungsmittel in den Top-1.000-Onlineshops im Jahr 2013, EHI Retail Institute e.V., Köln, S. 26.

Zahlungseingangs geht von Sofortüberweisung.de ein starker Wettbewerbsdruck aus. Das EHI Retail Institute ermittelt für Unternehmen mit mehr als 1 Mio. € Umsatz Kosten für das Bezahlverfahren sofortüberweisung.de von durchschnittlich 0,93% des getätigten Umsatzes. Lediglich Kosten für Zahlung bei Abholung, Vorauskasse und bei Rechnungskauf als White-Label-Lösung waren dabei günstiger. Durchschnittliche Kosten für Kreditkartenzahlungen lagen demgegenüber mit 2,28% des Transaktionsvolumens deutlich darüber, am obersten Ende aller betrachteten Bezahlverfahren.

403. Trotz der mit den OBB bezweckten Beschränkung des Wettbewerbs ist das Bezahlverfahren der Sofort in den vergangenen Jahren relativ stark in der Händlerakzeptanz gewachsen. Es ist davon auszugehen, dass dieses Wachstum in der Kundenakzeptanz ohne die Hindernisse, die sich rechtswidrig aus den OBB ergeben, deutlich stärker ausgefallen wäre.

6. Anwendbarkeit von Artikel 101 Abs. 1 AEUV, § 1 GWB (Nebenabreden)

404. Eine Anwendbarkeit von Artikel 101 Abs. 1 AEUV, § 1 GWB ist auch nicht ausgeschlossen. Auf die Beschlüsse zur einheitlichen Verwendung der Online-Banking-Bedingungen einschließlich des darin enthaltenen Verbots der Eingabe von PIN und TAN außerhalb der mit dem kontoführenden Kreditinstitut vereinbarten Internetseiten sind Art. 101 Abs. 1 AEUV, § 1 GWB anwendbar, da sie nicht als eine vom Tatbestand des Kartellverbots erfasste Nebenabrede zu betrachten sind.

405. Unter dem Begriff der „Nebenabreden“ sind im Rahmen des Art. 101 Abs. 1 AEUV Wettbewerbsbeschränkungen zu verstehen, die mit der Durchführung einer Hauptmaßnahme unmittelbar verbunden und für diese notwendig sind. Unmittelbar verbunden sind nur Einschränkungen, die eine dem Hauptgegenstand dieser Maßnahme untergeordnete Bedeutung haben und untrennbar mit ihm verbunden sind, demnach in einer offensichtlichen Beziehung zu ihm stehen. Notwendig ist eine Beschränkung, sofern sie für die Durchführung der Hauptmaßnahme objektiv notwendig und gegenüber der Hauptmaßnahme verhältnismäßig ist. Zur Feststellung der fehlenden objektiven Notwendigkeit einer Nebenabrede genügt es, wenn dargetan werden kann, dass das mit der Hauptabrede betriebene System auch ohne diese Nebenabrede überhaupt funktionsfähig ist. Dagegen kommt es nicht darauf an, dass sich das Fehlen der Nebenabrede negativ auf die Funktionsweise auswirken kann. Möglicherweise sich aus der Nebenabrede ergebende Vorteile können im Rahmen des Art. 101 Abs. 3 AEUV, § 2

GWB zu berücksichtigen sein.[330] Die Prüfung der objektiven Notwendigkeit einer Wettbewerbsbeschränkung führt nicht zu einer „Rule of reason“, in deren Rahmen wettbewerbsfördernde und wettbewerbswidrige Wirkungen einer Vereinbarung gegeneinander abgewogen werden. Eine solche Prüfung kann nur im Rahmen des Art. 101 Abs. 3 AEUV stattfinden, während im Rahmen des Art. 101 Abs. 1 AEUV nur eine vergleichsweise abstrakte Betrachtung anzustellen ist. Daraus folgt insbesondere, dass nicht zu prüfen ist, ob angesichts der Wettbewerbssituation auf dem relevanten Markt die Beschränkung für den geschäftlichen Erfolg der Hauptmaßnahme unerlässlich ist, sondern dass die Feststellung ausreicht, ob die Beschränkung im besonderen Rahmen der Hauptmaßnahme für die Verwirklichung dieser Maßnahme notwendig ist. Wäre die Hauptmaßnahme ohne die Beschränkung nur schwer oder gar nicht zu verwirklichen, so kann die Beschränkung als objektiv notwendig zu ihrer Verwirklichung betrachtet werden.[331]

a) Die Beteiligten können Verhaltenspflichten für den Online-Banking-Kunden gemeinsam festlegen, um Schadensfälle zu vermeiden

406. Der Hauptzweck der Online-Banking-Bedingung besteht in der Gewährleistung von Sicherheit durch die Definition entsprechender Verhaltensregeln der Kunden. Hierzu wird der Kunde verpflichtet, die Personalisierten Sicherheitsmerkmale geheim zu halten und Authentifizierungsinstrumente sicher aufzubewahren (vgl. Rz. 33). Darüber hinaus enthalten die Online-Banking-Bedingungen Regeln zur Haftungsverteilung zwischen Bank und Kunde in Fällen, in denen aufgrund nicht autorisierter Zahlungsvorgänge finanzielle Schäden entstanden sind.

407. Grundsätzlich können die Beteiligten in kartellrechtlich zulässiger Weise Regeln festlegen, um die Sicherheit des Online-Bankings zu erhöhen und Risiken, die durch die unbefugte Weitergabe und Nutzung Personalisierter Sicherheitsmerkmale bzw. Authentifizierungsinstrumente entstehen, zu begrenzen. Eine solche Ausgestaltung kommt wegen der damit einhergehenden Erhöhung der Sicherheit des Gesamtsystems und der Begrenzung von Schadenskosten allen Nutzern zu Gute und wird auch vom Gesetzgeber vorausgesetzt, etwa wenn er die Anbieter verpflichtet, vorvertragliche

---

330 Entscheidung des Europäischen Gerichts vom 24.05.2012, MasterCard / Kommission, Slg. II-, Rz. 88.

331 Zusammengefasste Darstellung des Konzepts der Nebenabreden in der Entscheidung des Europäischen Gerichts vom 24.05.2012, MasterCard / Kommission, Slg. II-1, Rz. 77 ff. unter Hinweis auf die Entscheidung des Gerichts Erster Instanz vom 18.09.2001, M6, Slg. II-2459, Rz. 105ff.

Informationen zum konkreten Inhalt der Sorgfaltspflichten bereitzustellen (Art. Art. 248 § 4 Abs. 1 Nr. 5 a EGBGB). Die Beteiligten können die Kunden auch dazu verpflichten, nur auf bestimmten Internetseiten die Personalisierten Sicherheitsmerkmale einzugeben, um z.B. die Gefahr des Phishings (vgl. Rz. 52) zu verringern.

b) Ein generelles Verbot, Personalisierte Sicherheitsmerkmale außerhalb gesondert vereinbarter Internetseiten, insbesondere Online-Händlerseiten, einzugeben, ist nicht notwendig

408. Die konkrete Ausgestaltung der Sorgfaltspflichten der Kunden, nach der es unzulässig ist, Personalisierte Sicherheitsmerkmale außerhalb vereinbarter Internetseiten einzugeben, z.B. nicht auf Online-Händlerseiten, ist nicht eine im oben genannten Sinne unmittelbar mit der Hauptmaßnahme verbundene und notwendige Regelung.

409. Um das Ziel, die Sicherheit gegen Phishing und andere Missbräuche zu steigern, zu erreichen, stehen der DK und ihren Verbänden eine Reihe von weniger wettbewerbsbeschränkenden Regelungen zur Verfügung. So ist es etwa möglich, ein Zertifizierungsverfahren für Zahlungsauslösedienste einzuführen und die Eingabe der Personalisierten Sicherheitsmerkmale auf den Seiten zertifizierter Anbieter zuzulassen. Grundzüge für ein solches Verfahren haben die Beteiligten selbst diskutiert und erarbeitet. Im Rahmen eines solchen Zulassungsverfahrens können die Prozesse externer Dienstleistern überprüfbar gemacht werden. Denkbar sind auch technische Lösungen, die eine Verarbeitung der Personalisierten Sicherheitsmerkmale durch den Zahlungsauslösedienst ausschließen.

410. Das generelle Verbot der Eingabe von Personalisierten Sicherheitsmerkmalen außerhalb gesondert vereinbarter Internetseiten, insbesondere Online-Händler-Seiten, ist hingegen überschießend. Entgegen der Ansicht der Beteiligten können die mit dem Beschluss verbundenen wettbewerbsbeschränkenden Wirkungen nicht als notwendig angesehen werden, um die Sicherheit des Online-Bankings zu gewährleisten. Die Beteiligten gehen zu Unrecht davon aus, die Sicherheitsrisiken, die sich aus der Eingabe von Personalisierten Sicherheitsmerkmalen außerhalb der Internetseiten des kontoführenden Kreditinstituts ergeben, ließen sich nicht anders vermeiden als durch eine Qualifizierung als grobe Sorgfaltspflichtverletzung.[332]

411. Allein die Bedrohungslage des Online-Bankings durch kriminelle Aktivitäten rechtfertigt nicht den nahezu vollständigen Ausschluss von Wettbewerb, ohne dass zwischen dem

---

[332] Schriftsatz Oppenländer Rechtsanwälte , vom 29.07.2014, Bl. 6165 d.A.

kriminellen Verhalten durch Phishing und dem Zahlungsauslösedienst ein konkreter Zusammenhang besteht. Soweit die DK Sicherheitsbedenken geltend macht, beziehen sich diese regelmäßig auch nicht auf die Gefahren aus dem Angebot und der Nutzung von dauerhaft am Markt tätigen Zahlungsauslösediensten, bei denen auch die Internethändler die Zuverlässigkeit prüfen, sondern auf kriminelle Vorgehensweisen des Phishing, die ein grundsätzlich mit dem Online-Banking verbundenes Problem darstellen. Eine besondere Gefährdung des Online-Bankings durch die Tätigkeit von bestehenden Zahlungsauslösediensten ist nicht ersichtlich. Dies gilt erst recht vor dem Hintergrund der Vielzahl bestehender Finanzverwaltungssoftwareprodukte und sonstiger Applikationen für mobile Geräte mit nicht durch die DK geregelten Sicherheitsfragestellungen.

III. Eignung zur Beeinträchtigung des zwischenstaatlichen Handels

412. Die Beschlüsse der DK und ihrer Spitzenverbände (Beteiligten zu 2. – 4.) sind schon deswegen geeignet, den Handel zwischen Mitgliedstaaten – hierunter sind nicht nur der traditionelle grenzüberschreitende Austausch von Waren und Dienstleistungen sondern alle grenzüberschreitenden wirtschaftlichen Tätigkeiten zu verstehen[333] – zu beeinträchtigen, weil sie sich auf das gesamte Hoheitsgebiet Deutschlands erstrecken. Derartige Kartelle verfestigen die Abschottung der Märkte auf nationaler Ebene und behindern die vom Vertrag über die Arbeitsweise der Europäischen Union gewollte wirtschaftliche Verflechtung.[334]

IV. Fehlen der Freistellungsvoraussetzungen des Artikel 101 Abs. 3 AEUV, § 2 GWB

413. Die Voraussetzungen der Freistellung der Beschlüsse (Art. 101 Abs. 3 AEUV, § 2 GWB) sind nicht erkennbar und von den Beteiligten auch nicht vorgetragen worden. Es ist nicht ersichtlich, dass die beanstandeten Beschlüsse für die Umsetzung der Ziele der Beteiligten unerlässlich sind. Vielmehr belegt der Vortrag der Beteiligten im Verfahren, dass es den Beteiligten möglich gewesen wäre, durch andere Maßnahmen Regelungen herbeizuführen, durch welche die Sicherheit des Online-Bankings gewährleistet und

---

333 Bekanntmachung der Kommission vom 27.04.2004, Leitlinien über den Begriff der Beeinträchtigung des zwischenstaatlichen Handels in den Artikeln 81 und 82 des Vertrags, 2004/C 101/07, ABl. C 101/81, Rz. 19 ff.

334 Ständige Rechtsprechung, vgl. Urteil des Gerichtshofs der Europäischen Union vom 19.02.2002, Slg. S. I-1577, Rz. 95, „Wouters“ m.w.N. Im Übrigen wären auch die Schwellenwerte der Leitlinien über den Begriff der Beeinträchtigung des zwischenstaatlichen Handels in den Artikeln 81 und 82 des Vertrages, Rz. 52 (Marktanteil von 5%, Marktvolumen von 40 Mio. EUR) überschritten.

gleichzeitig der Wettbewerb auf dem Markt für Bezahlverfahren im Internethandel weniger stark beeinträchtigt worden wäre.

414. Vom Verbot des Art. 101 Abs. 1 AEUV, § 1 GWB freigestellt sind gem. Art. 101 Abs. 3 AEUV, § 2 GWB Beschlüsse von Unternehmensvereinigungen, die unter angemessener Beteiligung der Verbraucher an dem entstehenden Gewinn zur Verbesserung der Warenerzeugung oder -verteilung oder zur Förderung des technischen oder wirtschaftlichen Fortschritts beitragen, ohne dass den beteiligten Unternehmen Beschränkungen auferlegt werden, die für die Verwirklichung dieser Ziele nicht unerlässlich sind, oder Möglichkeiten eröffnet werden, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten.

415. Bei der Beurteilung der Freistellungsvoraussetzungen müssen die vier genannten Voraussetzungen kumulativ erfüllt sein. Sofern nur eine einzige Voraussetzung nicht gegeben ist, liegen die Freistellungsvoraussetzungen insgesamt nicht vor. Bei der Prüfung der Voraussetzungen ist die Einhaltung einer Prüfungsreihenfolge nicht zwingend vorgegeben.[335]

1. Effizienzgewinne: Verbesserung der Warenerzeugung (Förderung des technischen und wirtschaftlichen Fortschritts)

416. Die erste in Art. 101 Abs. 3 AEUV genannte Freistellungsvoraussetzung bezieht sich auf die Verbesserung der Warenerzeugung und -verteilung, die mit dem wettbewerbsbeschränkenden Beschluss einhergeht. Analog gilt die Regelung auch für Dienstleistungen, auch wenn diese nicht explizit im Text benannt werden.[336] Berücksichtigungsfähig sind lediglich objektive Vorteile, die sich unmittelbar aus den unter wettbewerbsrechtlichen Regelungen zu prüfenden Beschlüssen ergeben müssen. Neben Kosteneinsparungen sind auch qualitative Verbesserungen als mögliche Effizienzgewinne anerkannt. Hierunter fallen auch technische Fortentwicklungen von Dienstleistungen, z.B. zur Steigerung der Sicherheit.[337]

417. Derzeit ist nicht ersichtlich und von den Beteiligten nicht vorgetragen, dass mit den zu beurteilenden Beschlüssen Effizienzgewinne realisiert werden. Auch wenn die

---

335 Schneider in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1 Deutsches Kartellrecht, 12. Aufl., § 2 GWB, Rz. 26.

336 Bekanntmachung der Kommission, Leitlinien zur Anwendung von Artikel 81 Absatz 3 EG-Vertrag (2004/C 101/08), ABl vom 27.04.2004, Nr. C 101, S. 97, Rz. 48.

337 Ellger, in: Immenga/Mestmäcker, Kommentar zum Europäischen Kartellecht, 5. Aufl. 2012, Art. 101 Abs. 3, Rz. 157.

Sorgfaltspflichten generell dazu beitragen, die Sicherheit des Online-Bankings durch Vorgaben zur sicheren Handhabung des Systems und zum Umgang mit Personalisierten Sicherheitsmerkmalen zu fördern, gilt dies nicht für das generelle Verbot zur Eingabe von Personalisierten Sicherheitsmerkmalen außerhalb der gesondert vereinbarten Internetseiten, insbesondere auf Seiten von Online-Händlern. Es ist nicht erkennbar, dass, wie von der DK vorgetragen wurde, die Nutzung von Zahlungsauslösediensten, anders als die Nutzung von Finanzsoftwareprodukten mit vergleichbarem Risikopotenzial, zu Gewöhnungseffekten bei Kunden führen wird, die einen sorglosen Umgang mit Personalisierten Sicherheitsmerkmalen bewirken.

418. Soweit die DK in ihren bisherigen Stellungnahmen überhaupt darauf eingegangen ist, führt sie die Notwendigkeit der Ausarbeitung und Präzisierung der Sorgfaltspflichten in den 2009 verabschiedeten Online-Banking-Bedingungen neben dem Anpassungsbedarf aufgrund des geänderten rechtlichen Rahmens im Wesentlichen auf die Notwendigkeit zurück, auf technische Entwicklungen zu reagieren. Insbesondere die Bedrohung des Online-Bankings durch kriminelle Angriffe Dritter (z.B. durch Phishing, Trojaner, Man-in-the-middle-Attacken) stellt die DK als wirtschaftliches Risiko dar, dem mit der Überarbeitung der Online-Banking-Bedingungen begegnet werden sollte.[338]

419. Die Online-Banking-Bedingungen streben mit den Sorgfaltspflichten die Ausgestaltung eines Handlungsrahmens an, der bestehenden Gefahren durch Missbrauch und Manipulationen Dritter begegnen und die Sicherheit des Systems zum Schutz vor finanziellen Schäden erhöhen soll. Standardisierte Regelungen sollen dazu beitragen, einen verlässlichen und sicheren Rahmen zu fördern, in dem die Vertragsparteien tätig werden und Haftungsfragen in Schadensfällen vorhersehbar geregelt werden können. Die Sorgfaltspflichten haben damit grds. das Potenzial zur Steigerung der Sicherheit des Online-Banking-Systems und damit auch zur Erzielung von Effizienzen im Sinne der Prüfung unter Art. 101 Abs. 3 AEUV und § 2 GWB.

420. Ob und in welchem Umfang die Sorgfaltspflichten insgesamt dazu führen, dass hierdurch qualitative Verbesserungen für die Sicherheit des Online-Bankings erzielt werden, die sich in gesteigerter Sicherheit niederschlagen und als Effizienzgewinne berücksichtigt werden können, muss im Rahmen der hier stattfindenden Prüfung der Freistellungsvoraussetzungen nicht abschließend beurteilt werden. Die Prüfung erstreckt sich hier lediglich auf die Frage, welche Effizienzgewinne mit der konkreten Pflicht, nach

---

[338] Schreiben der DK v. 02.11.2010, Bl. 483 d.A.

der Personalisierte Sicherheitsmerkmale nicht außerhalb der gesondert vereinbarten Internetseiten, insbesondere nicht auf Online-Händlerseiten eingegebenen werden dürfen, verbunden sind.

421. Es ist zweifelhaft, inwieweit das implizite Verbot der Nutzung bankenunabhängiger Zahlungsauslösedienste in Ziff. 7.2 Abs. 1 i.V.m. Abs. 2 dritter Spiegelstrich OBB überhaupt geeignet ist, die Sicherheit im Online-Banking zu erhöhen. Die DK stellt insoweit eine Verbindung zwischen den Gefahren aus kriminellen Angriffen (z.B. durch Phishing) und der Tätigkeit von Intermediären her. Die Sorgfaltspflicht richtet sich indessen nur gegen die Tätigkeit von Intermediären, ohne vergleichbare Risiken aus der Nutzung von Finanzsoftware zu berücksichtigen. Dies ergibt sich auch aus der Fußnote in den Arbeitsversionen der Online-Banking-Bedingungen, in der von der „*Verhinderung der Einschaltung von Intermediären aus Sicherheitsgründen*“ die Rede ist, gleichzeitig aber der Einsatz von Produkten mit vergleichbarem Risikopotenzial wie StarMoney ausdrücklich ermöglicht werden soll.[339]

422. Die Abwehr von Gefahren stellt grundsätzlich eine berücksichtigungsfähige Verbesserung dar. Da bisher keine schlüssige Begründung vorgetragen wurde, welche konkreten Gefahren gerade mit Zahlungsauslösediensten verbunden sind, die durch die Sorgfaltspflichten abgewehrt werden sollen, und warum diese Gefahren schwerer wiegen als solche, die im Zusammenhang mit anderen am Markt angebotenen Dienstleistungen rund um das Online-Banking bestehen, bei denen keine vertraglichen Beziehungen zwischen Anbietern und kontoführenden Kreditinstituten geschlossen wurden, sind Effizienzgewinne aus der Sorgfaltspflicht, also Verbesserungen der Sicherheit des Online-Bankings nicht ersichtlich.

423. Auch die Argumentation der Parteien, dass mit der entsprechenden Sorgfaltspflicht eine Dienstleistung unterbunden werde, die datenschutzrechtlichen Bedenken begegnet, vermag einen Effizienzgewinn nicht zu begründen. Soweit die Sorgfaltspflichten Anbieter vom Markt ausschließen sollen, die nach den Maßstäben der DK Datenschutzrecht oder auch andere Rechtsbereiche nicht berücksichtigen, handelt es sich hierbei nicht um Effizienzgewinne im Sinne von Art. 101 Abs. 3 AEUV und § 2 GWB. Die Überprüfung der Einhaltung rechtlicher Vorgaben obliegt den zuständigen Behörden und Gerichten und

339 [redacted]

kann keine kartellrechtliche Vereinbarung mit negativen Auswirkungen für den Wettbewerb rechtfertigen.[340]

424. Aber selbst unter der Annahme, dass die ihrem Zweck nach auf die Unterbindung der Nutzung einer speziellen Dienstleistung ausgerichtete Klausel in den Online-Banking-Bedingungen als effizienzsteigernd angesehen werden könnte, wäre dies für die Freistellung des Beschlusses vom Kartellverbot nicht ausreichend, da eine solche Regelung nicht unerlässlich ist und damit eine der weiteren Freistellungsvoraussetzungen nicht erfüllt.

2. Unerlässlichkeit

425. Die beanstandeten Beschlüsse sind zur Erreichung des Zieles, die Sicherheit des Online-Bankings zu gewährleisten, nicht unerlässlich. Es sind bereits andere, mildere Maßnahmen von der DK selbst erwogen und mit der Beschlussabteilung diskutiert worden, die eine Nutzung von Zahlungsauslösediensten durch Kunden im Internethandel weiter ermöglichen und negativen Auswirkungen auf dem Wettbewerb verhindern würden.

426. Die dritte im Art. 101 Abs. 3 AEUV genannte Voraussetzung verlangt, dass durch den Beschluss keine Wettbewerbsbeschränkungen auferlegt werden, die zur Erzielung der mit dem Beschluss verbundenen Effizienzgewinnen nicht unerlässlich sind. Die Freistellungsvoraussetzung fordert von den Parteien eines Beschlusses den Nachweis, dass die Umsetzung der dargetanen Effizienzgewinne nicht auf andere Weise erreicht werden können. Sofern die Ziele des Beschlusses auch mit Maßnahmen erreicht werden, die den Wettbewerb weniger stark belasten, verstößt ein Beschluss gegen das Gebot, das schonendste Mittel zur Erreichung des angestrebten Zweckes einzusetzen. [341]

427. Bei der Prüfung, ob die angestrebte Maßnahme nur durch die gefassten Beschlüsse oder auch durch wettbewerbskonformere Lösungen erreicht werden kann, ist zu klären, ob der Beschluss insgesamt vernünftigerweise notwendig ist und ob die einzelnen, sich aus dem Beschluss ergebenden Wettbewerbsbeschränkungen hierfür vernünftigerweise notwendig sind. [342]

Soweit Zahlungsauslösedienste Personalisierte Sicherheitsmerkmale entgegennehmen, um über den Zugang zum Online-Banking des Kunden eine Aussage gegenüber dem

---

340 Urteil des EuG in der Rechtssache C-68/12 vom 07.02. 2013, Rz. 20, (zitiert nach: http://curia.europa.eu).

341 Schneider, in: Langen Bunte, Bd. 1, § 2 GWB, Rz. 46.

342 Bekanntmachung der Kommission, Leitlinien zur Anwendung von Artikel 81 Absatz 3 EG-Vertrag (2004/C 101/08), ABl vom 27.04.2004, Nr. C 101, S. 97, Rz. 73 ff.

Internethändler abgeben zu können, ob das Kreditinstitut die Überweisung, mit der der Rechnungsbetrag aus dem Geschäft mit dem Kunden beglichen werden soll, annehmen wird, hat die DK Kriterien entwickelt, nach denen ein solches Geschäftsmodell die Sicherheit und Integrität des Online-Bankings nicht in Frage stellt. Das der Beschlussabteilung vorgestellte Zulassungskonzept hat die DK aus ihrer Sicht relevanten Wirtschaftsteilnehmern zur Kommentierung und Beurteilung zugeleitet. Bereits die schriftlich vorgetragenen Überlegungen der DK, dass sie unter den genannten Sicherheitsaspekten eine Zusammenarbeit als möglich ansieht, belegen, dass mildere Mittel im Umgang mit Zahlungsauslösediensten bestehen, als deren Nutzung pauschal zu untersagen.

428. Das Zulassungsverfahren sieht die Zertifizierung des jeweiligen Anbieters von Zahlungsauslösediensten durch die DK vor. Der Zahlungsauslösedienst muss die Einhaltung von Sicherheitsanforderungen nachweisen. Mit der Eingabe der Personalisierten Sicherheitsmerkmale auf der Seite eines zertifizierten Anbieters verstieße der Online-Banking-Kunde grds. nicht gegen die ihm obliegende Einhaltung von Sorgfaltspflichten.

429. Als Voraussetzung für die Eingabe von PIN und TAN auf der Internetseite eines Zahlungsauslösedienstes fordert die DK eine verlässliche und fehlerfreie Datenverarbeitung durch den Betreiber, bei der Funktionsstörungen und missbräuchliche Eingriffe weitgehend ausgeschlossen sind. Dabei sollen die Sicherheitsanforderungen dem entsprechen, was für Kreditinstitute bei der Verarbeitung sicherheitssensibler Daten in ihren eigenen und in den Systemen der beauftragten Rechenzentren gilt.[343] Die DK und ihre Spitzenverbände haben detaillierte Anforderungen an die Sicherheit von Zahlungsauslösediensten im Internethandel erarbeitet und in diesem Zusammenhang auch Prüfanforderungen an Dienstleister beschrieben, mit denen die Einhaltung der Sicherheitsanforderungen bei den Betreibern solcher Verfahren validiert werden kann.[344]

430. Inhaltlich beziehen sich die Sicherheitsanforderungen auf die zu schützenden Datenelemente. Dabei werden Anforderungen an den Schutz Personalisierter Sicherheitsmerkmale, den Schutz von Kunden- und Transaktionsdaten, die Nutzung vorgegebener Schnittstellen, die Identifizierungspflicht des Zahlungsauslösedienstes gegenüber dem kontoführenden Kreditinstitut sowie die Beschränkung der Tätigkeit auf zugelassene Dienste gestellt. Im Rahmen der Anforderungen an die

---

343 Schreiben der DK v. 09.08.2011, Bl. 1697 d.A.
344 Schreiben der DK v. 29.03.2012, Bl. 2854ff. d.A.

Sicherheitsorganisation werden sowohl Anforderungen an die interne Organisation als auch an externe Parteien formuliert. Neben der personellen Sicherheit, die sich auf Anforderungen an Mitarbeiter und andere Personen in Bezug auf den Umgang mit schützenswerten Datenelementen bezieht, gehören auch Anforderungen an die sichere Umgebung von Rechenzentren zum Schutz vor unbefugten Datenzugriffen zu dem von der DK erarbeiteten konzeptionellen Ansatz. In diesem Zusammenhang werden Zutrittskontrollen und Verschlüsselungstechniken sowie der Betrieb von Hardware-Sicherheitsmodulen gefordert. Das Konzept enthält daneben auch Anforderungen an die Kommunikations- und Betriebsverwaltung, die Betriebsüberwachung, die Planung und Abnahme von IT-Systemen, den Schutz vor Schadsoftware und an das Sicherheitsmanagement von Netzwerken. Auch Anforderungen an die Kontrolle von Zugriffen innerhalb von Rechenzentren, Netzwerken und über mobile Endgeräte sind in den Anforderungen formuliert. Schließlich werden noch allgemeine Anforderungen an den Rechenzentrumsbetrieb unter der Überschrift Beschaffung, Entwicklung und Wartung von IT-Systemen aufgestellt.[345]

431. Die ebenfalls von der DK und ihren Spitzenverbänden erarbeiteten Prüfanforderungen beschreiben, welche Prüfungsschritte eine Einhaltung der Sicherheitsanforderungen sicherstellen würden, welche Nachweise für die Durchführung der Prüfung vom Betreiber des Bezahlverfahrens zu erbringen wären und schließlich, in welcher Form die Durchführung der Prüfschritte zu dokumentieren wäre.[346] Einem solchen Modell stehen allerdings die im SecuRe Pay Forum vertretenen Zentralbanken und insbesondere die EZB kritisch gegenüber, soweit es die Eingabe der Personalisierten Sicherheitsmerkmale auf Seiten dritter Anbieter zulässt. Nach derzeitiger Rechtslage wäre ein solches Modell aber denkbar.

432. Für andere Geschäftsmodelle, die aus Sicht der DK mit weniger strikten Anforderungen tolerierbar wären, da sie ohne die Entgegennahme von PIN und TAN arbeiten könnten, hat die DK ebenfalls Anforderungen vorgelegt. Derzeit sind Dienstleister mit solchen alternativen Geschäftsmodellen nicht am Markt tätig, weshalb es sich bei diesen Überlegungen nur um theoretisch relevante Konstrukte handelt.

433. Die von der DK entworfenen und vorgestellten Konzepte zum Umgang mit Zahlungsauslösediensten sehen neben der Ausarbeitung eines Zulassungsverfahrens auch die vertragliche Vereinbarung zwischen den zugelassenen Dienstleistern und den

---

345 Schreiben der DK v. 29.03.2012, Anlage 1, Bl. 2860 d.A.
346 Schreiben der DK v. 29.03.2012, Anlage 2, Bl. 2888 d.A.

einzelnen Kreditinstituten vor. Diejenigen Dienstleister, die das Zulassungsverfahren erfolgreich abgeschlossen haben, sollen nach der Vorstellung der DK auf einer Positivliste geführt werden, aus der die kontoführenden Kreditinstitute dann diejenigen auswählen sollen, die sie als Zugangskanal für das Online-Banking definieren und damit deren Nutzung durch ihre Kunden ermöglichen wollen. Dabei soll es keine Pflicht zur Zusammenarbeit mit einzelnen Dienstleistern geben.[347]

434. Bei der Beurteilung der Unerlässlichkeit stellt die Beschlussabteilung einzig auf die Frage ab, ob es nach der Vorstellung der Beteiligten sicherheitstechnisch möglich erscheint, Geschäftsmodelle von Zahlungsauslösediensten anders zu behandeln, als ihre Nutzung generell - wie in den Online-Banking-Bedingungen geschehen - zu untersagen. Für die Beurteilung kommt es dabei wesentlich auf die Erfüllung der sicherheitsrelevanten Kriterien an.

435. Soweit die Beteiligten meinen, in jedem Fall sei auch eine vertragliche Vereinbarung zwischen dem Betreiber des Zahlungsauslösedienstes und dem kontoführendem Kreditinstitut erforderlich, trifft dies jedenfalls insoweit nicht zu, als damit das Vorliegen einer einzelvertraglichen Regelung gefordert wird. Im Rahmen der Möglichkeiten von Drittanbietern, Produkte zur Nutzung im Online-Banking anzubieten, hat die DK durch die Definition von Schnittstellen (FinTS, HBCI) Standards geschaffen, welche für eine gewerbliche Tätigkeit einer Reihe von Dienstleistern z.B. im Bereich Home-Banking Software ausreichend sind. Unabhängig davon, ob diese Angebote auf den Geräten der Kunden oder als Webapplikationen angeboten werden, bestehen zwischen kontoführenden Kreditinstituten und den Dienstleistern regelmäßig keine individuellen Verträge. Zum Beispiel werden bei der Nutzung des Produktes „Starmoney.web“ sowohl PIN als auch TAN über das System an das kontoführende Kreditinstitut übertragen und die Kontodaten auf der technischen Infrastruktur des Anbieters gespeichert. Vertragliche Vereinbarungen zwischen Anbieter und kontoführenden Kreditinstituten bestehen nicht und werden von der DK oder einzelnen Verbänden oder Kreditinstituten auch nicht gefordert. Solche Angebote werden allein auf der Basis der Sicherheitsstandards des anbietenden Unternehmens angeboten, ohne dass eine Zulassung oder Prüfung durch die DK oder einzelne Kreditinstitute stattfindet. Daher erscheint es sachgerecht und diskriminierungsfrei, die Zulassung eines Zahlungsauslösedienstes unter Sicherheitsaspekten als hinreichend für die Tätigkeit solcher Dienstleister am Markt anzusehen. Das schließt nicht aus, dass über die Anerkennung von Rahmenbedingungen

---

[347] Schreiben der DK v. 15.04.2011, Bl. 1554 d.A.

und Standards auch vertragliche Beziehungen zwischen dem jeweiligen kontoführenden Institut und dem Anbieter von Zahlungsauslösediensten zu Stande kommen. Ein Beispiel hierfür sind die Händlerbedingungen des electronic cash-Vertragswerks, die eine unmittelbare Vertragsbeziehung zwischen dem kartenausgebenden Institut und dem kartenakzeptierenden Händler begründen. Nicht ausgeschlossen ist auch der Abschluss eines Rahmenvertrages der kreditwirtschaftlichen Spitzenverbände, die in Vertretung für ihre Mitglieder handeln, und dem jeweiligen Anbieter eines Zahlungsauslösedienstes. Eine solche Lösung – mit Anerkennung der entsprechenden Sicherheitsstandards – wird beispielsweise im Verhältnis zu den Netzbetreibern im electronic cash-System praktiziert.

436. Wenn die DK ein solches Zulassungsverfahren etablieren würde, wäre der Abschluss von Verträgen zwischen Zahlungsauslösedienstleistern und Kreditinstituten kein notwendiger Bestandteil eines solchen Konzeptes. Zudem würde eine solche Forderung den Vorgaben der PSD2 widersprechen, die das Erbringen von Zahlungsauslösediensten nicht vom Bestehen einer vertraglichen Beziehung zwischen Zahlungsauslösedienst und kontoführendem Kreditinstitut abhängig macht (Vgl. Art. 115 Abs. 6, Erwägungsgrund 33 PSD2).

V. Verstoß gegen § 19 Abs. 3 Satz 1 i.V.m. Abs. 1, Abs. 2 Nr. 1 GWB

437. Der oben dargestellte Gesamtplan der Beteiligten zu 1. - 4, mit dem Ziel der Behinderung von Zahlungsauslösediensten stellt darüber hinaus auch eine unbillige Behinderung von Zahlungsauslösediensten gemäß § 19 Abs. 3 S. 1 i.V.m. § 19 Abs. 1, Abs. 2 Nr. 1 GWB dar.

438. Das Verbot der unbilligen Behinderung anderer Unternehmen (§ 19 Abs. 1, Abs. 2 Nr. 1 GWB) gilt nach § 19 Abs. 3 Satz 1 GWB auch für Vereinigungen von miteinander im Wettbewerb stehenden Unternehmen im Sinne des § 2 GWB. Der Anwendungsbereich der besonderen Verhaltensaufsicht des § 19 Abs. 1, Abs. 2 Nr. 1 GWB wird insofern auch auf Unternehmensvereinigungen ausgedehnt, die weder marktbeherrschend (§ 18 GWB) noch mit relativer oder überlegener Marktmacht (§ 20 GWB) versehen sind. Die Beteiligten zu 2. – 4. sind als solche Unternehmensvereinigungen anzusehen. Der Begriff der Vereinigung entspricht dem Begriff der Unternehmensvereinigung in § 1 GWB bzw. des Art. 101 AEUV. Dies ergibt sich aus der Bezugnahme der Regelung auf die Freistellungstatbestände in § 2, § 3, § 28 Abs. 1, § 30 Abs. 2a, § 31 Abs. 1 GWB. Insofern kann auf die oben stehenden Ausführungen zum Begriff der Unternehmensvereinigung verwiesen werden (oben unter I.1.).

439. Nach dem Wortlaut des § 19 Abs. 3 Satz 1 GWB werden zwar allein die nach § 2 GWB freigestellten Kartelle von dem Anwendungsbereich der Norm erfasst. Im heutigen System der Legalausnahme vom Kartellverbot ist die Anwendung des § 19 Abs. 3 Satz 1 GWB aber auch ohne explizite Freistellung dann eröffnet, wenn die kartellrechtliche Zulässigkeit der Tätigkeit der jeweiligen „Vereinigung von miteinander im Wettbewerb stehenden Unternehmen“ an sich keinem Zweifel unterliegt. Im System der Legalausnahme ist daher in diesen Fällen nicht weiter aufzuklären, ob die Tätigkeit der Unternehmensvereinigung, im Zuge derer das nach § 19 Abs. 3 Satz 1 GWB zu prüfende Verhalten erfolgt (hier: die Aufstellung der AGB-Banken), schon auf Ebene des § 1 GWB bzw. Art. 101 Abs. 1 AEUV nicht tatbestandsmäßig ist, oder ob sie erst auf Ebene der Freistellungstatbestände von Kartellverbot ausgenommen wird, zumal die Grenze hier gerade bei Konditionenempfehlungen fließend sein kann.[348] Fließend ist diese Grenze insbesondere bei Bank- und Versicherungsbedingungen, angesichts der besonderen Konditionen in diesen Branchen.[349] Ziel der Sonderregelung des § 19 Abs. 3 Satz 1 GWB für Unternehmensvereinigungen ist es, die Ausübung der durch eine prima facie zulässige Kooperation erhöhte Marktmacht der Mitgliedsunternehmen den Einschränkungen des § 19 Abs. 1, Abs. 2 Nr. 1 und 5 GWB zu unterwerfen.[350] Tragend für die Normanwendung ist daher die besondere Marktmacht der prima facie legalen Unternehmensvereinigung. Einer schon prima facie illegalen Unternehmensvereinigung käme eine solche Marktmacht nicht zu, da deren Verhaltensspielraum schon durch die Drohung mit einem Bußgeldverfahren begrenzt würde.[351]

440. Nach diesen Grundsätzen sind die DK und die Spitzenverbände der Kreditwirtschaft Normadressaten nach § 19 Abs. 3 Satz 1 GWB. Die gemeinsame Erstellung Allgemeiner Geschäftsbedingungen für Banken gehört seit Jahrzehnten zu den Aufgaben der entsprechenden Unternehmensvereinigungen. Dass diese Tätigkeit an sich prima facie kartellrechtswidrig wäre, entspricht weder dem Verständnis der Beteiligten, noch hat sich das Bundeskartellamt oder die EU-Kommission in der Vergangenheit veranlasst gesehen, die Aufstellung der AGB-Banken an sich zum Gegenstand eines Verfahrens nach Art. 101 AEUV bzw. § 1 GWB zu machen. Wirtschaftlich setzten die DK und ihre Spitzenverbände

---

348 Vgl. Horizontal-Leitlinien der KOM vom 14.01.2011 (C 11/1), Rn. 270-272, 300-307, 312f., 320, 335.

349 A.a.O., Rn. 259 a.E.. Vgl. auch Braun in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1, Deutsches Kartellrecht, 12. Auflage, nach § 2 Rn. 175.

350 Vgl. Nothdurft in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1, Deutsches Kartellrecht, 12. Aufl., § 19 GWB, Rz. 82.

351 Für eine Normanwendung auch ggü. illegalen Kartellen: Nothdurft in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1, Deutsches Kartellrecht, 12. Aufl., § 19 GWB, Rz. 80.

mit der Erstellung allgemeiner Geschäftsbedingungen einen Branchenstandard, was eine hinreichende Grundlage dafür bietet, die Ausübung des entsprechenden Gestaltungsermessens auch am besonderen Maßstab des § 19 Abs. 3 Satz 1 GWB zu messen.

441. Soweit eine Identität oder zumindest eine Wechselbeziehung zwischen dem Markt, auf den sich die Freistellung (oder bereits die fehlende Tatbestandsmäßigkeit) des Handelns der Unternehmensvereinigung bezieht, und dem Markt, auf dem die Behinderung stattfindet, vorliegen muss[352], so ist auch diese Voraussetzung hier erfüllt. Die in den OBB erfolgte Koordinierung der Online-Banking-Bedingungen bezieht sich auf dem Markt für Privatgirokonten. Die hier festgestellen Auswirkungen, insbesondere die unbillige Behinderung von Wettbewerbern, wirken sich auf den Wettbewerb auf dem bundesweiten Markt für Bezahlverfahren im Internethandel aus. Zwischen diesen Märkten besteht eine Wechselwirkung: Die Regelungen der Kreditwirtschaft beziehen sich auf die Nutzung des Online-Bankings und damit auf die Situation auf dem Markt für Privatgirokonten. Da Zahlungsauslösedienste darauf basieren, dass Kunden eines Online-Shops ihren Online-Banking-Zugang für die Bezahlung von Waren und Dienstleistungen im Internethandel nutzen können, sind durch die Regelungen der Kreditwirtschaft auch die Dienstleistungen der Anbieter von Bezahlverfahren im Internethandel betroffen. Sofern Bankkunden die OBB einhalten, findet das Angebot von bankenunabhängigen Zahlungsauslösediensten keine Nutzer. Die OBB errichten im Hinblick auf den Zugang zu diesem Markt eine rechtliche Markzutrittsschranke. Lediglich Zahlungsauslösedienste der Kreditwirtschaft selbst sind auf der Grundlage der Regelungen nicht betroffen. Die OBB führen zu einer Gestaltung des Marktes durch Ausschluss bzw. Förderung bestimmter Wettbewerber im Bereich der Bezahlverfahren im Internethandel.

442. Das Verbot dieses Verhaltens liegt im intendierten Anwendungsbereich des § 19 Abs. 3 Satz 1 GWB, so dass der Tenor dieser Verfügung auch auf diese Rechtsgrundlage gestützt werden kann: Durch die kartellrechtlich im Grundsatz zulässige Aufstellung der AGB-Banken durch die DK und ihre Spitzenverbände unterliegen diese einer besonderen Rücksichtnahmepflicht im Hinblick auf die Marktwirkungen der von ihnen aufgestellten Standard-Bedingungen, und zwar *unabhängig* von deren Zulässigkeit unter dem Aspekt der Koordinierung des Marktverhaltens ihrer Mitglieder (§ 1 GWB oder Art. 101 AEUV). Selbst wenn die von der DK aufgestellten Standard-Bedingungen unter dem Aspekt einer

---

[352] Vgl. Nothdurft, in: Langen/Bunte, Kartellrecht, Kommentar, Bd. 1, Detusches Kartellrecht, 12. Aufl. § 19 Rz 81.

Koordinierung zwischen den in ihr zusammengeschlossenen Banken nicht zu beanstanden wären, hätte sie nach § 19 Abs. 3 Satz 1 GWB dafür Sorge zu tragen, dass von den Bedingungen keine negativen Wirkungen auf einzelne Marktteilnehmer ausgehen, insbesondere wenn diese an der Aufstellung der Bedingungen nicht beteiligt waren. Insofern ist es einer Unternehmensvereinigung verboten, eine unter dem Aspekt der Koordinierung ggf. noch zulässige Aufstellung von Geschäftsbedingungen dazu zu nutzen, Dritte im Wettbewerb mit ihren Mitgliedsunternehmen zu behindern und eigene Angebote der Unternehmensvereinigung (bzw. der in ihr zusammengeschlossenen Unternehmen) zu Lasten von Außenseitern zu fördern. Dass dies hier der Fall ist und bezweckt wurde, ist bereits dargelegt worden (hierzu oben, insb. unter II. 3. d.). Insofern wäre das Verhalten der DK und der Spitzenverbände auch dann im Sinne des Tenors dieser Verfügung rechtswidrig und verboten, wenn die OBB entgegen der hier vertretenen Auffassung unter dem Aspekt der Koordinierung (§ 1 GWB, Art. 101 AEUV) noch als zulässig zu betrachten wären. Die Rechtswidrigkeit ergäbe sich dann aus der Behinderungswirkung i.S.v. § 19 Abs. 1, Abs. 2 Nr. 1 GWB zu Lasten von bankenunabhängigen Zahlungsdiensteanbietern.

443. Die übrigen Tatbestandsvoraussetzungen dieser Norm liegen vor. Eine Behinderung liegt in der nachteiligen Wirkung der OBB auf den Geschäftsbetrieb der Anbieter von bankenunabhängigen Zahlungsauslösediensten, da die Inanspruchnahme ihrer Leistungen für die Endkunden mit Rechtsrisiken im Hinblick auf die Geschäftsbeziehungen mit ihrem Kreditinstitut belastet wird. Diese Behinderung ist auch unbillig, da eine Abwägung der Interessen der DK und ihrer Spitzenverbände einerseits mit den Interessen der Anbieter von Zahlungsauslösediensten andererseits unter Berücksichtigung der auf die Freiheit des Wettbewerbs gerichteten Zielsetzung des Gesetzes[353] zu deren Gunsten ausfällt: Ausschlaggebend ist dabei zum einen die Erwägung, dass sich die OBB gegen den Marktzugang der Anbieter von bankenunabhängigen Zahlungsauslösediensten insgesamt richten. Die durch die OBB errichtete Marktzutrittsschranke betrifft nicht nur einen Teilbereich der Geschäftstätigkeit der Anbieter von Zahlungsauslösediensten, sondern deren Geschäftsmodell an sich. Das Gesetzesziel, die Märkte offen zu halten[354], erfordert deswegen in besonderem Maße das Eingreifen der Missbrauchsverbote. Zum anderen ist zu berücksichtigen, dass es sich

---

[353] St. Rspr., zuletzt BGH, Urteil vom 06.10.2015, KZR 87/13, NZKart 2015, 535 Rn. 59 – Porsche-Tuning.

[354] St. Rspr., zuletzt BGH, Urteil vom 24.10.2011, KZR 7/10, WuW/E DE-R 3446, Rn. 37, 50 – Grossistenkündigung.

beim Angebot der Sofort und anderer bankenunabhängiger Zahlungsauslösedienste um eine neuartige und innovative Leistung handelte, an der auf Seiten der Betreiber von Websites und deren Kunden ein Bedarf stand, der durch die Angebote der Mitgliedsunternehmen der Spitzenverbände nicht befriedigt wurde. Insofern ging es speziell im Verhältlnis zur Sofort um deren Verbleib auf einem von ihr wesentlich mit geschaffenen Markt, was ebenfalls das Eingreifen der Missbrauchsaufsicht in besonderem Maße erfordert. Die mit der Einführung der OBB von der DK und ihren Spitzenverbänden verfolgten Interessen vermögen diese Belange nicht aufzuwiegen. Insofern kann auf die vorstehenden Ausführungen verwiesen werden (vorstehend unter IV. 1. und 2.).

E. Angebotene Zusagen

444. Die von der DK aufgezeigten Alternativen, wie die Tätigkeit von Zahlungsauslösediensten aus ihrer Sicht kompatibel mit den kreditwirtschaftlichen Anforderungen ausgestaltet werden könnten, wurden gegenüber dem Bundeskartellamt nicht als Verpflichtungszusage übersandt. Sie wurden unverbindlich diskutiert und nicht weiter auf ihre Eignung zur Lösung der kartellrechtlichen Probleme beurteilt.

445. Soweit die Beteiligten beabsichtigen, Verpflichtungszusagen (§ 32 b GWB) anzubieten, müssen diese geeignet sein, die Wettbewerbsprozesse auf dem Markt für Bezahlverfahren im Internethandel strukturell abzusichern. Wesentlich ist insofern, dass die am Markt entwickelten Geschäftsmodelle bankenunabhängiger Anbieter von Zahlungsauslösediensten nicht auf Grund technischer Anforderungen von vornherein ausgeschlossen oder grundsätzlich zu modifizieren sind. Kritisch zu bewerten ist daher insbesondere, wenn diese Anbieter künftig auf Vorleistungen der kontoführenden Institute angewiesen wären.

446. Sofern Zahlungsauslösedienste in Folge technischer Änderungen nicht mehr in der Lage wären, die für den Händler im Internethandel essentielle Rückmeldung, dass die Überweisung im Online-Banking des Kunden eingestellt wurde und mit einer hohen Wahrscheinlichkeit auch durchgeführt wird, eigenständig abzugeben, bestünden auch in Folge solcher technischer Lösungen möglicherweise Beschränkungen des Wettbewerbs fort. Dies gilt vor allem dann, wenn die Zahlungsauslösedienste im Rahmen der Umsetzung solcher Konzepte von Kreditinstituten Bestätigungen über ausreichende verfügbare Mittel auf dem Kundenkonto zur Überweisung des Rechnungsbetrages oder eine unwiderrufliche Bankgarantie einkaufen müssen oder an der Bestätigung zu der Ausführung der Zahlung durch das kontoführende Kreditinstitut nicht mehr beteiligt sind.

447. Mit Schreiben vom 02.12.2015 hat die DK den Entwurf eines öffentlich-rechtlichen Vertrags sowie den Entwurf einer geänderten Fassung der Sonderbedingungen für das Online-Banking zur Beendigung des Verfahrens übersandt.

448. In den geänderten Sonderbedingungen sollte der Hinweis darauf, dass die Eingabe personalisierter Sicherheitsmerkmale „z.B. nicht auf Online-Händlerseiten“ erfolgen darf, ersatzlos gestrichen werden. Desweiteren hatte die DK darin vorgeschlagen, als neue Sorgfaltspflicht aufzunehmen, dass Kunden zur Bezahlung von Waren und Dienstleistungen im Internet einen zum Zeitpunkt des Inkrafttretens der PSD2 auf dem Markt tätigen Zahlungsauslösedienst nutzendürfen, soweit dieser einen Sitz im Europäischen Wirtschaftsraum hat. Ohne dass die Nutzung von dem jeweiligen Kreditinstitut vorab gestattet würde, sollte der Kunde danach verpflichtet sein, den Zahlungsauslösedienst sorgfältig auszuwählen.[355]

449. Von der Umsetzung dieser Änderungen in Form einer Zusage, welche die Beschlussabteilung nach § 32 B GWB für bindend hätte erklären können, haben die Beteiligten Abstand genommen und den Vorschlag, der inhaltlich geeignet gewesen wäre, die Beschränkung zu beseitigen, zurückgenommen.

F. Ermessen

450. Diese Verfügung ergeht auf der Grundlage des § 32 GWB. Gemäß § 32 Abs. 1 GWB entscheidet die Kartellbehörde nach pflichtgemäßem Ermessen, ob sie bei Verdacht Verstöße gegen deutsches oder europäisches Kartellrecht aufgreift.[356] Dies gilt auch für die Frage, ob das Bundeskartellamt lediglich eine Zuwiderhandlung feststellt und auf die Tenorierung von Maßnahmen zur Abstellung des Kartellvorwurfs verzichtet. Soweit der Wortlaut des § 32 Abs. 3 GWB ein berechtigtes Interesse fordert, damit das Bundeskartellamt eine Zuwiderhandlung auch nach deren Beendigung feststellen kann, gilt diese Einschränkung nicht für die Feststellung einer noch andauernden kartellrechtlichen Zuwiderhandlung. Bei der rechtlichen Würdigung eines noch andauernden Verhaltens ist im Umkehrschluss zu § 32 Abs. 3 GWB und nach allgemeinen Grundsätzen ein besonderes Feststellungsinteresse nicht erforderlich. Im Rahmen des Verhältnismäßigkeitsgrundsatzes kann sich der Tenor der Entscheidung auf eine bloße Feststellung beschränken, wenn dies nach den Umständen des Einzelfalls als

---

355 Vgl. Schreiben vom 02.12.2015, Anlage Öffentlich-rechtlicher Vertrag, S. 3.
356 Vgl. Bornkamm, Langen Bunte, § 32, Rz. 9.

ausreichend erscheint, weil davon auszugehen ist, dass der rechtmäßige Zustand in Zukunft auf anderem Wege wieder hergestellt wird.[357]

451. In Ausübung ihres Ermessens hat die Beschlussabteilung entschieden, die Entscheidung auf die Feststellung der Rechtswidrigkeit der Beschlüsse der DK und der Spitzenverbände der Kreditwirtschaft zu beschränken. Bei der Entscheidung hat die Beschlussabteilung dabei insbesondere berücksichtigt, dass eine Vielzahl von Maßnahmen möglich erscheint, wie der Kartellverstoß unter Wahrung der berechtigten Sicherheitsinteressen der Kreditwirtschaft abgestellt werden kann. Unter anderem hat die DK hierzu zwei verschiedene Konzepte vorgestellt. Um einerseits den Handlungsspielraum der Beteiligten zu 1. – 4. ausreichend zu erhalten, andererseits auch die klaren kartellrechtlichen Grenzen dieses Handlungspielraums aufzuzeigen, reicht eine Festellung wie im Tenor getroffen aus.

Eine solche Feststellung der Rechtswidrigkeit der Koordinierung und Umsetzung der beanstandeten Klauseln der Online-Banking-Bedingungen ist auch zu diesem Zeitpunkt noch sinnvoll und erforderlich. Zwar hat hat der europäische Gesetzgeber europäische Institutionen im Zuge der Umsetzung der PSD2 damit beauftragt, technische Standards zu erarbeiten, wie die aufeinander abgestimmte Tätigkeit von Zahlungsauslösediensten und Kreditinstituten zu erarbeiten. Die Beschlussabteilung geht davon aus, dass derartige kartellrechtswidrige Verhaltensweisen wie das in diesem Verfahren beanstandete durch solche zukünfigen Standards sowie auch durch die Umsetzung der PSD2 in nationales Recht in Zukunft abgestellt werden. Allerdings ist es den vom Kartellrechtsverstoß betroffenen Unternehmen nicht zuzumuten, bis zum Ende der Umstetzungsfrist der PSD2 in nationales Recht die unbillige Behinderung sowie die derzeit rechtliche Unsicherheit, die sich auch auf die anhängigen Zivilverfahren auswirkt, nocht länger hinzunehmen.

Im öffentlichen Interesse liegt eine feststellende Entscheidung des Amtes gerade im Hinblick auf diese anhängigen Zivilverfahren, die mit Blick auf das vorliegende Verfahren ausgesetzt wurden. Die vorliegende Entscheidung befördert diese Verfahren durch die ausführliche Begründung der Rechstauffassung des Amtes auf der Grundlage eines im Wege der Amtsermittlung vollständig aufgeklärten Sachverhalts. Angesichts der z.T. bereits langandauernden Aussetzung der Zivilverfahren spricht damit auch das Interesse an einer wirkungsvollen Verzahnung von öffentlicher und privater Kartellrechtsdurchsetzung für den Erlass einer Feststellungsentscheidung.

---

[357] Vgl. Emmerich, Immenga/Mestmecker, § 32 Rn. 48f.

452. Entsprechend den Anträgen der Beteiigten zu 1. bis 4. (s.o., Rn. 262, 264) wird gemäß § 65 Abs, 3 Satz 2 GWB die sofortige Vollziehung dieser Entscheidung ausgesetzt. Die Aussetzung des Sofortvollzugs kommt auch bei einer rein feststellenden Entscheidung in Betracht (vgl. § 80 Abs. 1 Satz 2 VwGO). Die Aussetzung verhindert nicht, dass die Verfügung im Hinblick auf die anhängigen Zivilverfahren ihre Zwecke erfüllt, da sie und die in ihr niedergelegten Ermittlungsergebnisse auch ohne Vollziehbarkeit in diesen Verfahren verwertet werden können. Zudem würde eine weitergehende Bindungswirkung nach § 33 Abs. 4 GWB ohnehin erst von bestands- bzw. rechtskräftigen Behörden- oder Gerichtsentscheidungen ausgehen. Für die Aussetzung spricht der Umstand, dass die Beteiligten zu 1. bis 4. – sofern sie sich durch die feststellende Amtsentscheidung zu Abstellungsmaßnahmen veranlasst sehen – diese nicht zunächst auf Grundlage der Rechtsauffassung des Amtes treffen müssern, um sie dann ggf. bei Korrekturen des Senats erneut abändern müssen.

G. Gebühren

453. Amtshandlungen aufgrund von § 32 GWB sind gem. § 80 Abs. 1 Satz 2 Nr. 2 GWB gebührenpflichtig. Dabei darf die Gebühr nach § 80 Abs. 2 Satz 2 Nr.2 GWB 25.000 EUR nicht übersteigen. Ist der personelle oder sachliche Aufwand unter Berücksichtigung der wirtschaftlichen Bedeutung besonders hoch, kann diese Gebühr auf das Doppelte erhöht werden (§ 80 Abs. 2 Satz 3 GWB).

454. Die Höhe der Gebühren richtet sich nach dem personellen und sachlichen Aufwand der Kartellbehörde unter Berücksichtigung der wirtschaftlichen Bedeutung, die der Gegenstand der gebührenpflichtigen Handlung hat (§ 80 Abs. 2 Satz 1 GWB). Von den genannten Bestimmungsmerkmalen kommt der wirtschaftlichen Bedeutung das größte Gewicht zu. Entspricht die nach diesen Bestimmungsmerkmalen festgestellte wirtschaftliche Bedeutung dem Durchschnitt, ist grundsätzlich eine mittlere Gebühr angemessen. Dies beträgt nach dem derzeit geltenden Gebührenrahmen 12.500 EUR. Von diesem Mittelwert sind, abhängig von der jeweiligen wirtschaftlichen Bedeutung und dem Arbeitsaufwand, Zu- oder Abschläge vorzunehmen, deren Höhe im pflichtgemäßen Ermessen der Kartellbehörde liegt.[358] Zur Bemessung der wirtschaftlichen Bedeutung sind

---

[358] Vgl. OG Düsseldorf, WuW 2000, 894 „Tequila“; KG WuW/E OLG 5259 „Kleinhammer“; KG WuW/E OLG 5287 „Finanzbeteiligung Gebühr“.

die Wettbewerbsbeschränkung und deren Intensität sowie die Marktbedeutung der Verfahrensbeteiligten zu berücksichtigen.[359]

455. [redacted]

456. [redacted]

457. [redacted]

458. [redacted]

459. [redacted]

[359] Stockmann, in: Immenga / Mestmäcker, GWB, 4. Auflage, § 80 Rn. 15.

[redacted]

[redacted]

460. [redacted]

461. [redacted]

H. Rechtsmittelbelehrung

462. Gegen diesen Beschluss ist die Beschwerde eröffnet. Sie ist schriftlich binnen einer mit Zustellung des Beschlusses beginnenden Frist von einem Monat beim Bundeskartellamt, Kaiser-Friedrich-Straße 16, 53113 Bonn, einzureichen. Es genügt jedoch, wenn sie innerhalb dieser Frist bei dem Beschwerdegericht, dem Oberlandesgericht Düsseldorf, eingeht

463. Die Beschwerde ist durch einen beim Bundeskartellamt oder beim Beschwerdegericht einzureichenden Schriftsatz zu begründen. Die Frist für die Beschwerdebegründung beträgt zwei Monate. Sie beginnt mit der Zustellung der angefochtenen Verfügung und kann auf Antrag vom Vorsitzenden des Beschwerdegerichts verlängert werden. Die Beschwerdebegründung muss die Erklärung enthalten, inwieweit der Beschluss angefochten und seine Abänderung oder Aufhebung beantragt wird, und die – gegebenenfalls auch neuen – Tatsachen und Beweismittel angeben, auf die sich die Beschwerde stützt.

464. Beschwerdeschrift und Beschwerdebegründung müssen durch einen Rechtsanwalt unterzeichnet sein. Die Beschwerde hat aufschiebende Wirkung.

E.-M. Schulze | Holin | Jakobi

H. Jakobi ist wegen Abwesenheit an der Unterschrift gehindert

INHALTSVERZEICHNIS