CONVENIENCE TRANSLATION
provided by an external translation service; no official document

4. Decision Division

B 4 – 71/10

ADMINISTRATIVE PROCEDURES DECISION PURSUANT TO SECTION 32 OF THE ACT AGAINST RESTRAINTS OF COMPETITION (GWB)

Decision

In the administrative procedure

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

   – Party One –

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

   – Party Two –

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

   – Party Three –

Counsel of Parties One to Three:
Oppenländer Rechtsanwälte
Börsenplatz 1
70174 Stuttgart
Fax: 0711 / 601 87 – 222

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

– Party Four –

Counsel of Party Four:
Denton Europe LLP
Markgrafenstrasse 33
10117 Berlin
Fax: 030 / 264 73-133

5. Sofort GmbH
   Fußbergstraße 1
   82131 Gauting

– Summoned Party Five -

Counsel of Summoned Party Five:

Kapellmann und Partner Rechtsanwälte
Viersener Straße 16
41061 Mönchengladbach
Fax: 02161 / 811-777

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

– Summoned Party Six -

Counsel of Summoned Party Six:

Osborne Clarke
Innere Kanalstraße 15

50823
Cologne
Fax: 0221 / 5108 - 4111

to examine an infringement of Article 101 para. 1 of the Treaty on the Functioning of the European Union[1] (TFEU) and Section 1 of the Act against Restraints of Competition[2] (GWB) and Section 19 para. 3 sentence 1 in conjunction with Section 19 para. 1, para. 2 no. 1 GWB, the 4th Decision Division of the Federal Cartel Office made the following decision on 29.06.2016:

1. It is noted that the decision of Party One regarding the acceptance of the Special Conditions for Online Banking, as reported to the Office in the correspondence of 05.08.2009, is unlawful with regard to Section 7.2 para. 1 in conjunction with para. 2, third bullet point, Section 10.2.1 para. 5, fourth bullet point.

2. It is noted that the decision of Party Two, which confirmed acceptance of the Special Conditions for Online Banking and their disclosure and recommendation in the correspondence of 07.07.2009 sent to the regional associations and in the association newsletters of 05.08.2009 with regard to Section 7.2. para. 1 in conjunction with para. 2, third bullet point, Section 10.2.1. para. 5, fourth bullet point of the Special Conditions for Online Banking decided by Party 1 is unlawful.

3. It is noted that the decision of Party Three regarding the acceptance of the Special Conditions for Online Banking and their disclosure and recommendation in the newsletter sent to the banking group on 13.08.2009 is unlawful with regard to Section 7.2. para. 1 in conjunction with para. 2, third bullet point, Section 10.2.1. para. 5, fourth bullet point of the Special Conditions for Online Banking decided by Party One.

4. It is noted that the decision of Party Four is unlawful regarding the acceptance of the Special Conditions for Online Banking

---

1 Treaty on the Functioning of the European Union in the version published on 09.05.2008 (Official Journal of the European Union 2008 / C 115/01).

2 Act against Restraints of Competition in the version published on 26.06.2013 (BGBl. I p. 1750), last amended by Art. 258 version of 31.08.2015 (BGBl. I 1474).

and their disclosure and recommendation in the newsletter sent to the members on 22.07.2009 is unlawful with regard to Section 7.2. para. 1 in conjunction with para. 2, third bullet point, Section 10.2.1. para. 5, fourth bullet point of the Special Conditions for Online Banking decided by Party One.

5. The enforcement of this ruling shall be suspended.

Grounds

A. Introductory Summary

1. The Special Conditions for Online Banking (in the following referred to as "OBC" or "Online-Banking-Conditions") are an integral part of the General Terms and Conditions of banks. They were jointly developed by the German Banking Industry Committee (in German: Deutsche Kreditwirtschaft) (in the following referred to as: GBIC)[3] and central associations of the German banking industry represented by the GBIC and are applied nationwide by the respective member institutes when dealing with their customers. They regulate, among other things, due diligence requirements of the online banking customers when handling the personalised security credentials PIN (Personal Identification No.) and TAN (Transaction No.). According to the provisions of the Online-Banking-Conditions, PIN and TAN must not be entered on the online websites of retailers, apart from on specially agreed internet sites.

2. Section 7.2. para. 1 in conjunction with para. 2, third bullet point of the OBC[4] states:

"The participant must treat his/her personalised security credentials (see No. 2.1) with strict confidence and only use and transmit them to the Bank via the online banking channels notified to him/her separately by the Bank, and safely store his/her authentication medium (see No. 2.2) in a place where it cannot be accessed by third parties

---

3 Until August 2011, GBIC referred to itself as the Central Credit Committee ("CCC"). The name GBIC will be used consistently in the following, also in connection with matters which occurred before August 2011, apart from in the case of quotes and descriptions of committees, e.g. working groups.

4 The detailed levels of OBC of the savings banks and private banks deviate from the decision by the GBIC in places, while the text of the duties of care is identical for the various banking groups.

. This is due to the fact that anyone who is in possession of the authentication medium and also has the relevant personalised security feature can misuse the online banking service. Particular note should be taken of the following information on the protection of the personalised security feature and the authentication medium: [...] The personalised security feature must not be entered on internet pages other than the ones agreed upon separately (e.g. on online retailer websites)."

The liability provision corresponding with the duty of care under Section 10 .2.1 paragraph 5, fourth bullet point reads as follows:

"*In cases where unauthorised payment transactions are made prior to the blocking notification and the Participant has intentionally or in gross negligence breached their duties of care under these conditions or has acted with fraudulent intent, the account holder shall be fully liable in respect of any losses incurred as a consequence thereof. Gross negligence on the part of the Participant can be deemed to have occurred, in particular, if he/she [...] has identifiably entered the personalised security feature on Internet pages other than the ones agreed upon separately (cf. No. 7.2 paragraph 2, third bullet point, […].*"

3. The resolutions passed by the GBIC and the central associations of the German banking industry represented by the GBIC for the approval and implementation of this provision breach Article 101 TFEU and Section 1 GWB, as they aim to achieve a restraint of competition, or at least result in such a restraint. Even the wording of the contested clauses indicates that their aim is solely to prohibit the activities of payment initiation services such as, for example, those provided by Sofort GmbH, which offers payment processes for online retailers and customers on the internet with the help of these personalised security credentials. The contested Online-Banking-Conditions are also objectively capable of making it more difficult for online retainers and bank customers to use payment initiation services or prevent this entirely.

4. The contested Online-Banking-Conditions only seemingly addresses security problems. As is clear from the history of these Online-Banking-Conditions, the true reason for introducing the contested Online-Banking-Conditions is to prevent payment initiation services. These provisions cannot be categorised as a necessary part of a consistent security concept of the banks. In fact, their real purpose is to protect the revenue interests of those credit institutions working together in the member associations of the GBIC.

5. The contested provisions have a negative effect on innovative payment service providers who have developed a range of services required by online retailers, as it covers their need for an inexpensive and quick payment option while also covering the identical interests of online customers. Such innovative processes are becoming increasingly important on the market for internet payment processes with their constantly increasing market penetration and encourage competition in this market, to which established payment method providers must react.

6. The adopted Special Conditions for Online Banking allow credit institutions to exclude competitors from the market or make their market presence significantly more difficult by establishing a legal barrier to entry, as customers deciding which payment initiation services to use would be breaching the applicable general terms and conditions of their account-holding bank and would need to take legal liability consequences into account. In connection with the media policies of the GBIC, which aims to "ostracise" payment service providers which are independent of banks, the Online-Banking-Conditions and liability consequences have significantly restricted the market development of payment service providers.

7. The fact that the contested clauses have not resulted in a complete elimination of the competition from payment initiation services is mainly due to the fact that a few providers, such as Sofort GmbH, have not distanced themselves from the marketing of their services, despite all the measures initiated or supported by the banking industry in connection with the duties of care. The GBIC has encouraged companies which offer services in connection with online banking access to cease their activities with reference to the AGB provisions passed by the GBIC. For the most part, it has been successful with this strategy. Furthermore, the GBIC has developed a framework for action called the "intermediary concept", which specified how the banking industry can position itself against the activities of payment initiation services: proposed measures, such as warnings directed at customers not to use such service providers, have been published on the websites of the credit institutions and were highlighted towards retailers. The attention of the press has also been drawn to alleged risks and problems associated with the use of payment initiation services. Finally, due to its business model, Sofort GmbH was confronted with the provisions of the OBC in several civil proceedings which are currently pending. One of the reasons why in some of these cases no judgement has been delivered so far is that the contested

provisions are still under legal scrutiny in the present antitrust proceedings and that the courts have suspended their pending cases until a decision is made by the Federal Cartel Office. The provisions do not constitute an ancillary provision not covered by the cartel prohibition. They also do not qualify for exemption in accordance with Article 101 para. 3 TFEU and Section 2 GWB. Even if the provisions would achieve efficiencies – which has neither been pleaded, nor has there been put up evidence in that regard – they are in any event not indispensable to achieve that objective.

8. The joint agreement of duties of care and their collective recommendation to the affiliated credit institutions constitute resolutions by associations of undertakings which violate antitrust law. In conjunction with further measures taken by the GBIC and the central associations of the banking industry, they aim to restrict competition from payment initiation services emerging in the market. Given its stated objective, its history and the various actions taken against payment initiation services, the actions of the GBIC and the central associations of the banking industry must be considered as constituting part of an overall plan to eliminate competition from payment initiation services. The underlying resolutions and their recommendation breach Article 101 TFEU and Section 1 GWB as they constitute illegal coordination, both at the level of the GBIC and at the level of the central associations. The implementation of this overall plan, which also includes the collusion between Parties One - Four regarding the Online-Banking-Conditions in relation to the duties of care when dealing with the personalised security credentials, also represents - even if one were to consider the coordination of the Parties as permissible - an unfair disadvantage for other companies and therefore constitutes abuse behaviour within the meaning of Section 19 paragraph 3 sentence 1 in conjunction with Section 1, para. 2 no. 1 GWB.

9. This violation of Art. 101 para. 1 TFEU and Section 1 GWB, Section 19 para. 3 sentence 1 in conjunction with Section 1, para. 2 no. 1 GWB is still on-going. The recommendations still apply, and they are the basis for the general terms and conditions of the individual credit institutions, who have practically all implemented these recommendations.

10. European legislation stipulates in the revised Payment Services Directive 2 (hereinafter PSD2)[5] that, in the period leading to its incorporation into national law, the

---

5 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25.11.2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/26/EU and Regulation (EU) No. 1093/2010 and repealing Council Directive 2007/64/EC, OJ. of the European Union of 23.12.2015. In practice,

continuity of competition has to be ensured and that existing service providers can offer their services irrespective of their business model. In doing so, unjustified discrimination against existing market participants should be avoided. All government agencies have the obligation to ensure these aims, including the Federal Cartel Office. On these grounds, it was legally required to adopt the present decision.

B. Facts

I. The participants

1. The German Banking Industry

11. The German Banking Industry and cooperating central associations of the German banking industry are participants in the cartel administrative procedure. They include the Association of German Banks (Bundesverband deutscher Banken e.V.) (hereinafter: BdB), the National Association of German Cooperative Banks (Deutschen Volksbanken und Raiffeisenbanken e.V.) (hereinafter: BVR) and the German Savings Banks Association (Deutsche Sparkassen- und Giroverband e.V.) (hereinafter: DSGV). The lead management within the GBIC rotates annually between the BdB, BVR and DSGV. BdB is the current central coordinator of the GBIC.

12. The GBIC does not have its own infrastructure and instead draws upon the resources of its members and in particular the respective central coordinator. The GBIC acts as a united association in public and in particular when dealing with legal institutions and administrative authorities when dealing with issues relevant to the association but, in contrast to its members, does not have the status of a registered association.

2. National Association of German Cooperative Banks

13. The BVR is the central association for the cooperative banking industry in Germany. Members are all cooperative banks. The BVR represents the interests of the cooperative financial network nationally and internationally. For this purpose, the BVR coordinates and develops a common strategic orientation within the group. At the same time, the association advises and supports the members in legal, tax and business matters.[6] The purpose of the association according to its articles of association is to promote, support and represent professional and

---

the use of the abbreviation of the term English term Payment Service Directive 2 = PSD2 is also common in German-speaking regions.

6 cf. https://www.bvr.de/Wer_wir_sind/Unsere_Aufgaben,Version 07.06.2016.

specific economic policy and economic interests of its members and of associated institutions within the cooperative banking sector.[7]

3. German Savings Banks Association (DSGV)

14. The DSGV is the umbrella organisation of the savings bank financial group. Its members are the regional associations of the savings bank group, 409 savings banks (as of January 2016), seven state bank groups, DekaBank, nine state building societies, eleven primary insurance groups of the savings banks and various other financial service companies.

15. The DSGV represents the interests of the savings bank financial group and organises the decision-making process within the group. It also defines the strategic direction of the savings bank financial group. For this purpose, its members and related companies work with the DSGV to develop concepts for successful marketing. This relates to strategic market and operational topics ranging from product development and processing, risk management and overall bank management, card and payment transactions to a holistic advisory approach for all customer segments.[8]

4. Association of German Banks (BdB)

16. The BdB is the central association for private banks. It consists of approximately 200 banks and 11 member associations. The BdB supports its member institutions with the implementation of legal requirements and offers assistance with matters relating to banking law and practical and political aspects of banking. The BdB supplies publications and forms for everyday business through its subsidiary Bank-Verlag. In close cooperation between the association headquarters and members, further activities are also carried out in various bodies such as committees, working groups, task forces and communication forums. [9]

---

7 cf. Section 3 para. 1 Articles of Association Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., https://www.bvr.de/p.nsf/0/E9CB768B7DE38656C1257CE1004F68F6/$file/BVR-Satzung2015.pdf,Version 07.06.2016.

8 cf. http://www.dsgv.de/de/ueber-uns/aufgaben_und_ziele.html,Version 07.06.2016.

9 cf. https://bankenverband.de/ueber-uns/unser-selbstverstaendnis/,Version 07.06.2016.

II. Members of GBIC not (no longer) involved in the process

1. Bundesverband Öffentlicher Banken Deutschlands e.V.

17. The Association of German Public Banks (Bundesverband Öffentlicher Banken Deutschlands) (hereinafter: VÖB) is another central association of the German banking industry. It represents more than 60 member institutions, including the regional banks and the federal and state development banks. The VÖB is part of the GBIC and has been involved in the working groups of the GBIC for drafting the Terms and Conditions contractual works and, to this extent, also participated in the unlawful agreement. The credit institutions represented by the VÖB in the area of payment transactions, however, offer online banking either only to a limited extent or no longer use the clauses which are the subject of the decision by the GBIC and by the associations working with the GBIC. In a letter dated 27.06.2016, the Decision Division therefore informed the VÖB, which was initially listed as a participant in the proceedings, that it was no longer a participant in the proceedings and that no rights would be granted to it on the basis of the decision.

2. Association of German Pfandbrief Banks

18. The Association of German Pfandbrief Banks did not participate in the cartel violation at all. The Association of German Pfandbrief Banks is also organised in the GBIC, but did not participate in the working groups on issues of payment transactions. The institutes organised in this association do not offer any payment transaction services and do not apply the Special Conditions for Online Banking in the contested form.

3. Individual credit institutions of the central associations

19. The individual credit institutions represented by the central associations are not involved in the proceedings; formally, they decide independently on whether or not to adopt the recommended Terms and Conditions developed by the GBIC. The central associations have a mandate to revise the Terms and Conditions for directly or indirectly affiliated credit institutions, so that the specification of the content – as intended by the credit institutions – and also the decision-making within the scope of the GBIC were performed by the associations organised within the GBIC. Due to the complexity of the legal issues regulated in the Terms and Conditions, individual credit institutions do not, however, have much leeway to deviate from the rules agreed for online banking, and rarely make use of this option in practice.

III. The Summoned Parties

1. Sofort GmbH

20. Sofort GmbH, Gauting (hereinafter: Sofort or Summoned Party 5) is a service company and has been operating a bank-independent payment system for e-commerce under the brand name "sofortueberweisung.de" since 2005. This is a payment initiation service[10] which activates payments for e-commerce through the customer's online bank account. Customers use their personalised security credentials (PIN and TAN)[11] for online banking by granting Sofort access to the bank at which the account is held so that Sofort can verify that the funds are available in the account and activate the payment to be made to the online merchant. The online merchant is a contractual partner of Sofort and pays a fee to Sofort for the use of the payment process; the fee is usually calculated based on turnover and is significantly less expensive for online retailers than, for example, payment via PayPal or credit card. The payment method has been developed to meet the demand for a fast, safe and uncomplicated payment method for online retailers and customers.

21. Sofort has been offering this payment method on the market for more than ten years. In addition to Germany, Sofort is currently active in a further 12 European countries, including Austria and Switzerland. Particularly in Austria, Sofort's market share is significantly higher than in Germany.[12] In Germany, Sofort is offered by a growing number of retailers as a payment option and is also growing in terms of transactions actually performed. According to Sofort, it is currently

---

[10] Payment initiation services were defined as payment services with entry into force of the revised Payments Services Directives in 2016. They enable access to a payment account managed by another payment service provider. The term includes services provided using a software bridge between the website of the Internet retailer and the website of the institute managing the account. Using this software bridge, the payer can either authorise the payment transaction themselves or pass personalised security credentials, such as their PIN and/or TAN to the third-party payment service provider so that it can arrange the payment with the Institute managing the account on behalf of the payer. cf. http://wirtschaftslexikon.gabler.de/Archiv/-2046338290/zahlungsausloesedienst-v1.html,Version 14.05.2016.

[11] The personalised security credentials include, among other things, the personal identification number (PIN) and the single-use transaction numbers (TAN) for authorisation of transactions with the credit institution managing the account (personalised security credentials are referred to as PIN and TAN in the decision for the sake of clarity).

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

offered by more than 35,000 merchants.[13] More than 3 million transactions are executed each month using the payment process. The company employs more than 150 employees.[14]

22. Since the introduction of the payment method, no security issues have been reported. Sofort operates servers that ensure a secure procedure by which customer data are forwarded to the respective credit institution (and not to the internet retailer). Sofort received the "Tested Payment System" and "Certified Privacy" TÜV certifications from TÜV Saarland. The company's systems are operated on servers which are located within a bank data centre.[15]

23. Since 2013, Sofort has been a part of the Swedish company Klarna AB through a 100% holding of Klarna Germany Holding GmbH.[16] The Klarna Group is one of the leading European payment solution providers for online retailers. Klarna's central product is purchase on account (Rechnungskauf), whereby the company takes over all invoicing services, including the collection of funds. . Klarna works with around 50,000 online merchants and provides its solutions in 15 European countries. Klarna employs more than 1200 people. In total, 35 million customers use Klarna's services. 17 Klarna had a turnover of more than € 200 million in 2013, according to publicly available information.

24. Sofort offers a payment initiation service that complies with the provisions of the PSD2 for the transfer phase between entering into force of the directive and its implementation into national law and therefore enjoys grandfathering protection. The transitional rules state that payment initiation services already active on the market must not be unjustifiably prevented from offering their services until the provisions of the PSD2 have been implemented into national law (cf. fn. 69).

---

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

14 In addition to the payment initiation services, Sofort also offers "Paycode", a service where the purchase of goods or services in Internet retail are processed on account, but where the payment is also triggered via the customer's online banking, for which Sofort Provides a transfer form. Sofort also offers the "Sofort Ident" procedure, which customers can use to verify their age using online banking.

15 Although these specific applications are not directly subject to banking supervision, a comparable security approach to that of the German banking industry applies here (see. paragraph 119).

16 Email, Kapellmann Rechtsanwälte, 30.01.2015, Bl. 6490 of the file, this most likely refers to Klarna Germany Holding GmbH, Berlin, Amtsgericht Charlottenburg, HRB 153963 B.

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

2. giropay GmbH

25. giropay GmbH, Frankfurt am Main, (hereinafter: giropay or Summoned Party Six) grew out of the project of the central associations of the German banking industry, which aimed to introduce a payment method for internet trading provided by the banks as an alternative to Sofort. The payment method offered by giropay is also a payment initiation service. Deutsche Postbank AG, Bonn, the cooperative data centre Rechenzentrum Fiducia & GAD IT AG, Karlsruhe, (Fiducia & GAD) and Star Finanz- Softwareentwicklung und Vertrieb GmbH, Hamburg, a subsidiary of Finanz Informatik GmbH & Co. KG, Frankfurt, (FI), the technical service provider and datacentre of the banking group, are shareholders of giropay.

26. giropay has been offering the payment method since of 2006. It can currently be used by around 35 million online banking customers. This does not include all customers; in fact, only around 70% of online banking customers can use giropay due to the organisation of the payment procedure. Only customers of those credit institutions which have entered into an agreement with giropay can take part.

27. As giropay is orientated towards German credit institutions, the area of distribution of the procedure is essentially limited to the territory of the Federal Republic of Germany. giropay also operates in Austria via a cooperation with the "eps" payment procedure operated by banks in Austria. Both procedures work together via a joint interface, so that internet merchants can reach both customers in Austria and those in Germany and execute payments from both countries using this procedure.

28. giropay also charges the fee only to online merchants, based on the sales price paid during the payment procedure. Customers are not charged any direct fees for the use of giropay. In connection with the use of giropay, GBIC developed a special text key for irrevocable transfers.[18] As transactions initiated using giropay cannot be revoked, merchants have a particularly high protection with regard to the anticipated receipt of payment (payment guarantee).

---

[18] [redacted]

29. In the same way as Sofort, giropay also offers online banking-based invoicing and age verification of the customer through the system. According to a study by the German central bank, around 3% of customers who generally use internet payment methods use the procedure offered by giropay. Sofortüberweisung was, in contrast, used by 23%, and PayPal by 88% of this customer group.[19]

IV. Duties of care of the customer with regard to the use of payment initiation services in internet trade

30. By making the Online-Banking-Conditions part of the general terms and conditions, credit institutions create standardised contracts with their customers as users of online banking[20].

31. The credit institutes operating in Germany have – to the extent that they offer online banking to their customers – made the OBC prepared by the German Banking Industry Committee part of the general terms and conditions (hereinafter: “AGB”) that become the contractual basis for the business relationships with customers. The AGB have been developed by the GBIC as an industry standard, and the affiliated credit institutions in the central associations and those involved in the preparation of the rules are recommended to use them.

1. Duty of care

32. The Online-Banking-Conditions decided upon in 2009 by the parties included a series of duties of care in connection with the personalised security credentials that are used for the authentication of the user and the authorisation of credit transfers via the online-banking. These duties of care include provisions regarding the security arrangements to protect PIN and TAN, in addition to provisions regarding the manner in which these are to be used, and which types of use are prohibited, respectively.

33. Specifically, the online banking user must observe the following: He or she must keep the personalised security credentials strictly confidential and only transfer them within the scope of

---

19 Deutsche Bundesbank, payment behaviour in Germany in 2014. Third study of the utilisation of cash and cashless payment instruments, Frankfurt a.M. 2015, p. 73, multiple mentions of the use of payment methods in internet trade were possible.

20 The concept of "online banking" refers to the banking transactions electronically conducted on the internet. Within the text, users of various applications are always referred to as customers, as the applications are being used within the context of the online banking customer relationship.

the online banking access channels separately specified by the bank when issuing instructions; and he has to keep his/her authentication medium secure from being accessed by third parties (paragraph 7.1 OBC). In particular, the personalised security credentials must not be entered outside of the separately specified internet websites, especially not on online merchant websites (paragraph 7.2 3rd bullet point OBC).

34. The OBC agreed 2009 are associated with a material tightening up of the duties of care, which relates to the technical development of the potential use of online banking (see in this regard the following bullet point IV. 5.) and to the market introduction of payment initiation services in e-commerce (see in this regard the following bullet point V.)

35. Provisions regarding the confidentiality of the PIN and TAN had already been included in the previous versions of the OBC. The BTX[21] conditions of 1984 contain provisions that are based on the risks perceived by the GBIC at the time:

"*BTX Pin and transaction numbers are to be kept confidential to avoid misuse. They must not be made accessible to third parties, as every person who knows this authorisation feature can use the BTX service*".[22]

36. GBIC reacted to changes in online banking in its formulation of the duties of care in the "Conditions for the account/deposit-related use of online banking with PIN and TAN" in 2000. As access was also possible outside the BTX system, namely via the internet provider, steps needed to be taken to ensure – according to the GBIC – that customers were prevented from using fraudulent server operators to access their account. For this purpose, the conditions included a provision relating to the risk perceived by the GBIC and the use of secure access channels:

"The user is required to only make a technical connection to the online banking services

---

21 Screen text is considered to be the forerunner of online banking. This procedure was offered by the Federal Post Office. Customers could use this to send payment orders to their bank within a limited scope and obtain account information.

22 Letter from the GBIC dated 02.11.2010, p.3, Bl. 434 of the file

of the bank using the online banking access channels separately specified by the bank."

2. Liability issues

37. Compliance with the duties of care is associated with an allocation of liability between bank and customer in the event of damage. The user is liable regardless of fault up to an amount of € 150, if the unauthorised payment transactions are the result of a lost, stolen or otherwise mislaid authentication medium before a request to block the account (Sperranzeige) has been submitted.[23] In other cases of improper use of the authentication medium, the user is also liable up to an amount of € 150, if he/she has culpably breached his/her duty to safely store the personalised security credentials.[24] The user must cover the full damages resulting from unauthorised transactions, if he/she has breached his/her duties of care with intent or due to gross negligence or if he/she has acted fraudulently.[25] An example of gross negligence is the recognisable entry of the personalised security credentials outside of the separately agreed websites[26]; this in particular includes their entry on online merchant websites.[27]

38. In contrast, credit institutions are liable for damages in full in the case of unauthorised online banking orders and/or incorrectly executed online banking orders and after the authentication medium has been blocked, according to the OBC.

3. Consequences for the use of payment initiation services on the market for online payments in e-commerce

39. The rules with respect to the duties of care of the user exclude the use of bank-independent products (e.g. payment initiation services) if their websites are not specifically enlisted by the individual credit institutions as websites where customers can enter their personalised security credentials.

---

23 Section 10.2.1 para. 1 Online-Banking-Conditions.
24 Section 10.2.1 para. 2 Online-Banking-Conditions
25 Section 10.2.1 para. 5 Online-Banking-Conditions.
26 Section 10.2.1 para. 5 sentence 2 4. Bullet point Online-Banking-Conditions.
27 Section 7.2 para. 2 3. Bullet point Online-Banking-Conditions.

40. The provisions only apply to payment initiation services offered on the market for online payments in e-commerce. The duties of care do not relate to other products for which customers also enter personalised security credentials for the use of locally installed software products or on websites, e.g. in the case of online banking software products.[28]

V. Development and framework conditions of online banking in Germany

1. Increasing significance of online banking in the processing of banking transactions

41. Traditionally, banking services were provided in bank branches. In addition to the branch network, various other possibilities have been established over the past 30 years for the use of banking services. Online banking is now a significant access channel.[29] This is used to access accounts on PCs, smartphones or similar mobile devices with an internet connection. Alternatively, special software products which provide access to online banking via an internet connection and interfaces specially designed by the banking industry for this purpose (HBCI/FinTS) are also used, in addition to online banking via an internet browser.

42. Online banking has become widespread in recent years. While the number of current accounts in Germany has increased by around 14% from 84 million to 96.1 million from 2003-2012, the number of "online accounts"[30] increased from 30.8 million to 50.3 million over the same period. This represents an increase of more than 63%. By 2012, more than half of current accounts were held as online accounts.

---

[28] Other products are used either as an application on the internet, or installed and operated as software on the customer's device. The risks associated with the processing, use and storage of personalised security credentials when using these systems is not addressed in the Online-Banking-Conditions.

[29] Another option is phone banking, which customers can use to access their credit institution by phone, either through a call centre or a voice computer.

[30] Settlement accounts which can be accessed on the internet.

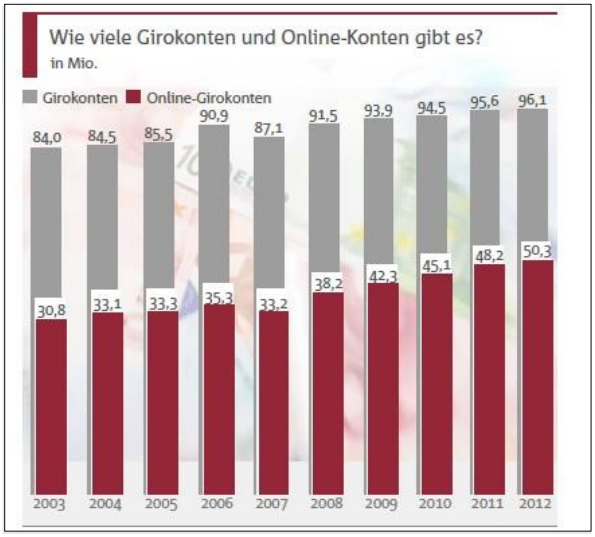

Fig. 1 - Online current accounts at German banks [31]

Kommentar [A1]: How many current accounts and online accounts are there?
Current accounts
Online accounts

43. The usage patterns of account holders have changed over time with the provision of the infrastructure. The proportion of online banking customers in Germany increased from 26% to 45% between 2003 and 2013.

[31] Facts and Figures of the Banking Industry, issued by the Association of German Banks, Berlin November 2013, p. 12, (http://bankenverband.de/publikationen/shopitem/dd247802306c4f789dd44b15417ed8de;Version 21.02.2014), Bl. 4598 of the file

Fig. 2 - Proportion of online banking customers in Germany [32]

Kommentar [A2]: How many people use online banking? Proportion of users in Germany in percent

44. Online banking allows customers to access different types of accounts and services depending on the scope of products offered by the credit institution managing the account. In the field of payment transactions, customers gain access to current accounts and the option, for instance, to view account balances and transactions, arrange the transfer of funds and set up and process Versioning orders. Customers can also gain this type of access by applying for credit facilities. However, online banking may also include access to other types of accounts, such as deposit accounts, credit accounts and securities accounts. In general, all of the customer's accounts held with the corresponding credit institution can be accessed simultaneously using online banking.

45. Online banking-enabled current accounts can also be used by the account holder for the settlement of payment processes in e-commerce, including those associated with the provision of payment initiation services.

46. Customers holding current accounts with online banking are able to use third-party products that can be used to retrieve account information through means of access other than those

---

[32] Facts and Figures of the Banking Industry, issued by the Association of German Banks, Berlin November 2013, p. 13, (http://bankenverband.de/publikationen/shopitem/dd247802306c4f789dd44b15417ed8de;Version 21.02.2014), Bl. 4599 of the file

provided by the credit institution (e.g. web page of the credit institution in charge of the account). Such **account information services** provided by third parties are operated as software applications on customer devices, e.g. PCs, mobile devices, or as internet applications. Customers can use these services to gather, view and analyse information about different accounts at different banks.

a) Access to online banking and initiating transactions

47. A prerequisite for the use of online banking is the availability of internet access via a PC or a similar mobile device and an internet connection.

48. Access to the online banking services of the respective credit institution is established either using software installed on the customer's end device, which communicates with the customer's credit institution through the use of a shared GBIC interface (FinTS), or through the use of an internet browser which creates a connection with the bank's online banking website.

49. If the customer uses special software on his/her device, he/she enters his/her login data for online banking on the device before the software sends it to the credit institution.

50. On the credit institution's web page, the online banking customer enters his/her login data directly into the infrastructure provided by the credit institution, so that the credit institution can check the authenticity of the customer and ensure that only the authorised individual gains access to the account.[33] This is usually the account number or a special access number[34] for online banking which, when used together with the PIN, allows access to the account and the associated applications.[35]

---

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

[34] For example, in comdirect's online banking.

[35] In some cases, the credit institution also requires, in addition to the PIN, the entry of another number or letter combination or parts thereof, which can only be entered by clicking with the mouse rather than using a keyboard, in order to provide a higher level of security (https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniertDasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst=true&docId=3589572), Version 11.06.2014.

51. In order to submit an order to the credit institution after authentication in online banking, the customer – irrespective of whether software is used or whether a connection has been made to the internet browser - enters a TAN, which the bank uses as evidence for the declaration of intent (Willenserklärung) by the online banking customer. Customers can be provided with a TAN in various ways.[36] The TAN procedures are continuously being jointly developed by the banking industry, in particular to ensure that existing procedures continue to provide a sufficient level of security.

b) Risks of online banking

52. The act of entering the PIN and TAN for authentication and confirmation of the declaration of intent is associated with a risk of abuse. Criminals who manage to obtain the relevant data can use it to access account information and misuse the accounts. Obtaining the PIN and TAN electronically in order to carry out criminal acts is referred to as **'phishing'**[37]. Online banking customers are prompted to unintentionally disclose their PIN and TAN to third parties. This can be achieved by sending fake emails or on web pages that mislead customers into believing that it is a message from their bank or their bank's web page. In both cases, customers are asked to enter their PIN and TAN in a reply or on the website.[38]

53. The entry of orders can also be manipulated using malicious software. For example in the case of the so-called "man-in-the-middle attacks"[39], the risk emanates from

---

[36] With regard to the procedures used in practice to transfer the TAN, cf. under paragraph 54f et seq.

[37] The word is a combination of "password" and "fishing" (https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html,Version 12.06.2014).

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

[39] The aim of a man-in-the-middle attack is to spy on the communication between two or more partners without being noticed, for example, in order to gain access to or manipulate information. The attacker moves "into the middle" of the communication by appearing as a recipient to the sender and as a sender by the recipient. The attacker starts by sending a connection request to themselves from the sender. Next, the attacker creates a connection with the actual recipient of the message. If this is successful, the attacker can view or manipulate all information sent by the sender to the intended recipient for passing it on to the correct recipient. The attacker can in turn also access the responses sent by the recipient if there are no corresponding protection mechanisms. (cf. Federal Office for Information Security,

malicious software that is located on the end device of the customer being used to access the online banking service. Using the malicious software, the data traffic between the customer and his/her credit institution can be manipulated by, for example, amending and forwarding recipient account numbers and transfer amounts.

c) Security procedures in online banking

54. In order to be able to react to the evolving risk scenarios, the banking industry has been continuously improving the procedures used to release orders to the bank using online banking over the past few years. While simple TAN lists were sent to customers in the early days,[40] additional standards have been implemented by using further media to generate and transfer TANs and[41] in order to prevent abuse in particular via malicious software.[42]

55. In reaction to the man-in-the-middle attacks, the so-called **iTANplus procedure** was introduced, which allows the online banking customer to check the transaction data on the screen before entering the TAN, which makes it more difficult to manipulate the data by using malicious software.[43]

---

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

[40] In the classic TAN procedure from the early days of online banking, customers received a list with a large number of TANs by post, which were successively used to authorise orders. The single-use TAN were selected by the customer in any order and deleted from the list after use. This method was particularly vulnerable to phishing attacks, as the attacker was able to authorise orders from the customer account using the PIN and each stolen TAN. The iTAN procedure (indexed TAN method) was developed to reduce the potential for abuse. The customer receives a numbered TAN list for this purpose. When a transaction is initiated, the customer is prompted to enter a specific TAN. Even if the attacker is able to steal an online banking customer's TAN, the attacker will not be able to use it to initiate a transaction if they do not know the corresponding index. This TAN procedure therefore provides an additional safety threshold.

[41] However, as early as 2009, the German Federal Office of Criminal Investigation indicated that the iTAN procedure should not be regarded as secure, due to the fact that the distribution of malicious software was steadily increasing (https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/SoFunktioniert/DasOnlineBanking/Sicherheit/PIN-TAN-Schutzverfahren.html?notFirst= true&docId=3600852, Version 12.06. 2014).

[42] The following presentation will provide an exemplary overview of the process and its development by the GBIC, although the presentation of the process variants cannot provide a complete overview.

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

56. The so-called **mTAN or SMS-TAN** procedure, in which an independent transmission channel is offered or even demanded in order to communicate the TAN, was a further improvement of online banking security. For this purpose, customers register a mobile phone number, which is used to provide them with the corresponding TAN for the authorisation of an order sent to the credit institution, and are no longer sent TAN lists. Together with the TAN, customers receive information about order details (e.g. specification of the transfer amount and/or the recipient's account number), with the help of which manipulation using malicious software is made even more difficult.

57. Another method used to increase security and prevent phishing and malicious software is the use of a **TAN generator**, which produces a TAN by pushing a button or entering a control number provided by the bank for the specific order. GBIC continued to develop the existing TAN procedure using a TAN generator. In the **chip TAN procedure** (also referred to as a **smart TAB** procedure), the TAN is produced through the use of a TAN generator. Initially, the bank or current account card is inserted into the TAN generator and is used by the device to create the TAN. The order details required for this purpose are either entered manually or are transferred as a flicker code from the screen of the device used to gain access to the online banking service as light signals via an optical interface to the TAN generator. The order details are displayed on the TAN generator and can be checked by the customer.

58. In addition to the TAN procedure, GBIC has jointly developed further security procedures to protect online banking. These include the **FinTS (HBCI) card**, which is used with a signature card reader that sends the encrypted order to the bank before the transfer and adds a signature. The signature is sent with the order to the bank, where it is decrypted. As the order data is linked to the signature, it is no longer possible to change the order after it has been sent.[44]

59. GBIC has developed Standards for its own signature card reader. The so-called **Secoder** displays the transaction data on the built-in screen and sends the encrypted and signed order data to the credit institution in charge of the account.[45]

---

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

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

GBIC performs an approval and certification procedure to guarantee the security of the Secoder products available on the market.[46] GBIC tests the function and security of the devices available on the market and issues a certification that documents the approval by banks and savings banks.[47]

2. Legal framework for the concept of duties of care for online banking in 2009

60. Due to the risk of unauthorised access to accounts and illegal disposal of customers' funds associated with the use of online banking, special duties of care are imposed on online banking customers in relation to their use of the access data. These arise in part from legal regulations and - to the extent they are not exhaustive - also from the obligations stipulated by the banking industry in their Terms and Conditions (AGB).

61. The legal regulations regarding the use of access data issued by credit institutions are based on European law. The first European Payment Services Directive (the abbreviation PSD for the English name of the directive is also used in the following)[48] was implemented into national law with regard to the sections of the Civil Code (Bürgerliches Gesetzbuch (BGB))[49] relevant to the duties of care of the payment service providers (online banking customers). The civil law rules mainly focus on the rights of the payment service users, with special consideration of the consumer protection in Sections 675 c ff. BGB.[50]However, the provisions included in the BGB also establish obligations of payment service users which, in those places where they remain general ,

---

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

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

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

48 Directive 2007/64/EC of the European Parliament and of the Council of 13.11.2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC text with EEA relevance, OJ. L 319 v. 05.12.2007, p. 1-36.

49 German Civil Code in the version published on 02.01.2002 (I, p. 42, 2909;. 2003 I, p. 738), last amended by Article 16 of the Act of 06.29.2015 (BGBl. I p. 1042).

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

are specified in more detail by the credit institutions as payment service providers and operators of payment services within the scope of their general terms and conditions.

a) Payment Services Directive (old)

62. Credit institutions, that offer both, deposit and lending services, and that give their customers the opportunity to access the accounts at their bank online to initiate transfer orders using payment instruments via the online banking, are effectively providing, as payment service providers[51], a payment service[52] to payment service users (e.g. bank customers). The obligations of the payment service user and the payment service provider relating to the protection of payment instruments and, in particular, the personalised security credentials had previously been specified in the PSD.

63. The Directive, which came into force in 2007, aimed to create a legal framework for non-cash payments in the European single market. [53]

64. In Art. 56[54], the PSD specified the obligations of the payment service users in relation to the use of payment instruments. According to Article 56 para. 1 lit. a) PSD, a payment service user authorised to use a payment instrument is required to adhere to the conditions for its provision and, for this purpose, has to take all reasonable precautionary measures immediately after receiving a payment instrument to protect the personalised security credentials from unauthorised access in accordance with paragraph 2.

65. Service providers such as payment initiation services (e.g. Sofort or giropay), which pass transfers on to the credit institution in charge of the account and which provide the merchant with a notification stating whether the receipt of a payment is to be expected, are not payment service providers within the meaning of the PSD. Furthermore, the PSD did not cover providers of account information services.

---

[51] The credit institutions represented by the GBIC in the preparation of the AGB contractual works are payment service providers within the meaning of the PSD. According to Art. 1 para. 1 lit. a) PSD, credit institutions within the meaning of Art. 4 no. 1 lit. a) of Directive 2006/48/EC or Section 1 para. 1 no. 1 ZAG are payment service providers.

[52] Payment services include, in accordance with Art. 4 no. 3 PSD, any commercial activity listed in the Annex to the Directive. This includes the execution of payment transactions, including the transfer of funds to a payment account by a payment service provider through the execution of credit transfers as mentioned in No. 3 of the Annex.

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

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

At the time, these service providers were not subject to any specific financial supervision. This was also the case if the services offered by the providers originated from the banking sector. The financial supervision of these banks did not extend to these services.

66. The PSD was also amended against the background of the existing activities of payment initiation services, with the aim of integrating these services into the legal framework and ensuring that they are subject to supervision. This took place when the PSD2 came into force (see Rd. 83 ff.).

b) Civil law implementation of the Payment Services Directive (old) into national law

67. The legislator implemented the provisions of the PSD into national law through the law for the implementation of the supervisory regulations of the Payment Services Directive (Payment Services Implementation Act) [55]. The regulatory supervision was regulated in the law regarding the supervision of payment services (ZAG)[56] and via amendments to the law on banking (Banking Act - Kreditwesengesetz)[57]. The civil (private) law elements for payment service providers were implemented in a separate piece of legislation, namely the law for implementation of the Consumer Credit Directive, for the civil law elements of the Payment Services Directive and the reorganisation of the provisions on the right to cancellation and refund of 29.07.2009. [58] The corresponding provisions were added to the German BGB.[59]

68. The provisions under civil law for the implementation of the Payment Services Directive in the BGB stipulate, among other things, issues concerning access to online banking systems in the banking industry and the

---

[55] Payment Services Implementation Act of 29.06.2009 (BGBl. I 1505).

[56] Payment Services Supervision Act of 25.06.2009 (BGBl, p. 1506), amended by Article 342 of the Decree of 31.08.2015 (BGBl, p. 1474).

[57] German Banking Act in the version published on 09.09.1998 (BGBl, p. 2776), amended by Article 339 of the Decree of 31.08.2015 (BGBl, p. 1474).

[58] Law for the implementation of the Consumer Credit Directive, the civil elements of the Payment Services Directive and the reorganisation of the provisions on the right to cancellation and refund of 29.07.2009 (BGBl I 2355).

[59] The specific facts presented here refer to the relationship between banks and those of their customers who use online banking services. In accordance with Section 675 c para. 3 BGB, the definitions of the German Banking Act (KWG) and the Payment Services Supervision Act (ZAG) apply correspondingly to the provisions of the Civil Code. Consequently, to the extent that payment service providers (Section 1 para. 1 ZAG) and payment services (Section 1 para. 2 ZAG) are mentioned in the legal text, the term ‘credit institution’ will be used in the following. The term 'payment service user' is defined as a person who uses a payment service, for instance as a payer, in Section 675 f para. 1 BGB. In the following, the term 'online banking user' (or 'customer') will be used in this regard. cf. Palandt (74th edition), section 675 c BGB, paragraph 10.

authorisation of payment orders within the scope of online banking usage in Chapter 3, "Provision and use of payment services", in particular the authorisation of payment transactions and payment authentication tools in sub-chapter 1.[60]

69. The actual regulations regarding the obligations of online banking customers when using online banking are laid out in Section 675 para. 1 sentence 1 BGB, which stipulates the duties of care in relation to the payment authentication tools[61]. According to this, the online banking customer is required to take all reasonable security precautions immediately after receiving a payment authentication tool in connection with the personalized security credentials in order to prevent unauthorised access and abuse. The provision implements Article 56 para. 1 lit. a) and para. 2 of the Payment Services Directive. The provision applies to current account agreements which include the use of online banking services, as these are payment service framework agreements in accordance with Section 675f para. 2 BGB.

70. The concept of personalised security credentials is not defined in any more detail in the Payment Services Directive, in Sections 675c et seq. BGB, the ZAG or the KWG. The personalised security credential is to be regarded as part of the payment authentication tool and represents a knowledge component which is allocated to the payer by the payment service provider, is known only to the payer and is used for the purpose of authenticating payment orders. [62] Within the scope of online banking, personalised security credentials can comprise PINs, TANs, electronic signatures or passwords.

---

60 According to 675j para. 1 sentence 1 BGB, an effective payment transaction requires the consent of the payer (authorisation). Corresponding agreements need to be made between the payer and his payment service provider regarding the nature and manner of consent. The wording of the legal regulation stipulates that this consent can be granted using a specific payment authentication tool. The law does not specify whether only the payer can authorise a payment or if this can also be performed by a third party. According to Section 675k BGB, the Bank can be authorised in an agreement to block the payment authentication tool if they suspect non-authorised or fraudulent use of the payment authentication tool. Non-authorised use includes the use of the payment authentication tool against the wishes of or without the permission of the payer (e.g. in relation to the use of PINs and TANs in online banking). cf. Frey in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, Section 675k BGB, paragraph 10.

61 According to Section 1 para. 5 ZAG, a payment authentication tool is any personalised tool which is agreed between the payment service user and the payment service provider for issuing payment orders and which is used by the payment service user in order to initiate a payment order.

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

71. In addition to the lack of a definition of personalised security credentials, the legal provisions also fail to define the scope of the "reasonable security precautions" and what is meant by "unauthorised access". In the commentary, unauthorised access is understood as any access not covered by a contractual agreement.[63] In this respect, the statutory provisions require that the details and specifics need to be contractually defined. The banking industry does not use any individual agreements in this regard and instead defaults back to the Special Conditions for Online Banking as part of the general terms and conditions contractual works.

c) Terms and conditions to standardise the contractual relationships and to define legal concepts

72. GBIC revised the terms and conditions and the Online-Banking-Conditions (OBC) in 2009. Since then, the member institutions of the individual central associations use these when dealing with their customers. The OBC are an integral part of the agreement between the bank and the customer and stipulate the rights and obligations when using online banking.

73. The OBC prepared by GBIC regulate fundamental issues regarding the contractual relationship between the credit institution and the customer when using the online banking services. The OBC define the range of services (No. 1). On that basis, customers can perform banking transactions and obtain information from the bank. in contrast, the scope of the banking transactions to be performed via online banking is specified individually by each credit institution.

74. The OBC also include provisions regarding the conditions for the use of online banking (No. 2), access to online banking (No. 3) and granting and revoking instructions (Nos. 4.1 and 4.2). According to this, the agreed personalised security credentials are required for authentication and authorisation when performing banking transactions using online banking so that the payer is identified as an authorised participant for the bank and the instructions are authorised (cf. below under paragraph 69). The way in which participants receive the TAN or an electronic signature to issue instructions within the scope of online banking

---

[63] Sprau in: Palandt (74th edition), Section 675l, paragraph 2; cf. Frey in: Ellenberger, Findeisen, Nobbe (Hrsg.), 2010, Kommentar zum Zahlungsverkehrsrecht, Section 675l BGB, paragraph 9.

[64] The term 'subscriber' is defined under Section 1 para. 2 of the OBC. This includes both the account or deposit holder and authorised persons who use the credit institution's online banking service.

is defined in the OBC as authentication instruments. These can be a list of single-use TANs, a TAN generator which creates chip TANs or a mobile device which is used to send TANs via SMS ("SMS TANs") to the participants of online banking.

75. In addition to the rules for processing online banking orders by the credit institution (No. 5) and for the account holder's information via online banking orders (No. 6), the OBC also include rules regarding the duties of care of the participant (No. 7). The duties of care include the creation of the technical connection to the online banking services using the online banking access channels separately specified by the credit institution. One example of such channels is an internet address. Another obligation of the participant relates to the handling of personalised security credentials and the authentication mediums.

76. With regard to the personalised security credentials, the provisions specify a duty of confidentiality. According to these provisions, instructions must only be issued to the credit institution using the online banking channels separately specified by the credit institution. The reason given for these obligations is the risk that people who are in possession of authentication mediums could use the online banking abusively in connection with the personalised security credentials.

77. For the special protection of personalised security credentials and authentication mediums, the OBC contains a catalogue of special protection requirements which online banking customers are required to observe. These include:

---

65 Online-Banking-Conditions Section 7.2 para. 1 S. 2.

- The personalised security credentials must not be saved electronically (e.g. in the customer's system).
- When entering the personalised security credentials, it must be ensured that other individuals are unable to view them.
- The personalised security credentials must not be entered outside of the separately agreed websites (e.g. not on online merchant websites).
- The personalised security credentials must not be disclosed outside of the online banking procedure, e.g. not by email.
- The PIN and usage codes for the electronic signature must not be stored together with the authentication instrument.
- The participant must use no more than one TAN for authorisation purposes e.g. an instruction, the removal of a block or to release a new TAN list.
- When using the mobile TAN procedure, the device used to receive the TAN (e.g. mobile phone) must not be used for online banking.

Fig. 3 - OBC No. 7.2 para. 2[66]

78. Furthermore, the customer must guarantee the security of the hardware used and must follow the security instructions of the credit institution (No. 7.3) or check the order data - to the extent that this is displayed on a device other than the one used to enter the instructions. The OBC requires customers to check whether the order data displayed by the credit institution corresponds with the data provided for the transaction before confirming the order (No. 7.5).

79. Additionally, the OBC details the reporting and instruction obligations of the customer under No. 8, and the obligation or right of the credit institution to block the use of the online banking service at the request of the customer or on its own initiative under No. 9. Finally, the OBC regulates the liability of the bank in the event of an unauthorised, failed or incorrect online banking order under No. 10 (No. 10.1) and the liability of the account holder in the event of the improper use of his or her authentication medium (No. 10.2).

[66] Letter of the GBIC dated 05.08.2009, Changes to the terms and conditions and special conditions with payment relevance, Annex 19, Special Conditions for Online Banking, p. 6470 ff.. of the file

3. Development of the legal framework following the resolution regarding the duties of care in 2009

a) Recommendations for the security of internet payments by the European Central Bank and the regulatory authorities for the relevant payment service providers

80. A joint working group of the European central banks and banking supervisory authorities (European Forum on the Security of Retail Payments, “SecuRe Pay” Forum for short) released recommendations for internet payment procedure security in 2013. The recommendations of the Pay SecuRe Forum aim to promote harmonised Europe-wide safety Standards for internet payments. They are addressed to payment service providers within the meaning of the Payment Services Directive.[67] Payment initiation services are not currently included in the recommendations' group of addressees.

81. The recommendations are based on four principles:

- First, payment service providers and payment systems should regularly review the risks associated with internet payments, taking into account any current security threats and fraud mechanisms on the internet.

- Second, the initiation of internet payments and access to sensitive payment data - i.e. data that can be accessed and misused for fraud purposes - should be protected through strong customer authentication.

- The third principle aims to ensure the effectiveness of processes established by payment service providers to authorise transactions and monitor transactions and systems. The aim is to detect unusual payment patterns and effectively prevent fraud.

- Finally, payment service providers - as a fourth principle - should make customers aware and provide training in the secure and efficient use of the services to perform internet payments.

82. On the basis of these recommendations, the European Banking Authority (EBA) added recommendations to its guidelines on security in 2014 that were almost identical. The Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin) implemented the EBA guidelines in its own administrative practice to help protect against cybercrime

---

[67] The recommendations therefore have no current direct effect on the activities of payment initiation services, as they are not payment service providers within the meaning of the applicable Payment Services Directive.

in May 2015 by providing the German translation of the text as a circular specifying the minimum security requirements for internet payments (MaSi).[68]

b) Amendment of the Payment Services Directive in 2015

83. The Payment Services Directive PSD was amended in 2015. Upon entry into force of the (new) PSD2, the definition of the types of payment services covered by the Directive and subject to supervision was expanded. It now also applies to payment initiation services and account information services (cf. para no. 46).

84. The PSD2 defines payment initiation services as payment services which initiate a payment order relating to a payment account managed by another payment service provider upon request by the payment service user (Art. 4 No. 15 PSD2). The approval of payment transactions is submitted in the form agreed between the payer and the payment service provider (customer and bank) (Art. 64 para. 2 PSD2). Art. 66 PSD2 specifies the access to the account in the event of the activation of payment initiation services. If the payer uses a payment initiation service and gives its express approval for the execution of a payment in accordance with Art. 64 PSD2, the payment service provider in charge of the account must take action in order to guarantee that the payment initiation services can be used by the payer (Art. 66 para. 2 PSD2). Specific duties of the account-servicing payment service provider (ASPSP) are stipulated in 66 para. 4 PSD2. According to this, the account-servicing payment service provider must communicate with the payment initiation service in a secure way and provide or make accessible all information about the execution of the payment transaction and all information accessible to the payment service provider regarding the payment transaction immediately after receipt of the payment order. The account-servicing payment service provider must deal with payment orders transferred via a payment initiation service in the same way as directly submitted orders in terms of processing times, priorities and fees, unless there are objective reasons to change the way these are treated.

---

[68] Payments on the internet - new circular: Minimum security requirements, BaFin Journal, May 2015, p. 12.

85. The provision of payment initiation services does not depend on the existence of a contractual relationship between the payment initiation service provider and the service provider in charge of the account (Art. 66 para. 5 PSD2).

86. Under European law, customers therefore have the right, once the revised PSD2 came into force in 2015, to use existing payment initiation services and submit payment instructions in the way specified by the bank in this way. In their role as account-servicing payment service providers, banks are required to perform instructions issued via payment initiation services and provide all required information to the payment initiation services, without the existence of a contractual basis. In accordance with PSD2, payment initiation services are permitted to accept PINs and TANs from customers and are not to be treated as third parties from whom the personalised security credentials are to be kept confidential.

87. It was not until the amendment of PSD2 that there was a legal framework within which payment initiation services as payment services (Art. 4 no. 3 in conjunction with Annex I PSD2) require and are granted authorisation for EU-wide activities and are subject to ongoing supervision by government agencies (Article 11, paragraph 1, Article 1 (d) PSD2).

88. Sofort's services fall within the scope of the PSD2. The rules governing the distribution of roles between payment initiation services, payers and payment service providers in charge of the account correspond to those between Sofort, payers and the bank in charge of the account. The PSD2 sets out the rights and obligations of the participating companies and requires member states to ensure, during the implementation of the Directive into national law, that payers have the right to use payment release and account information services as long as the corresponding account is managed online.

89. The relevant public bodies are in the process of developing “Regulatory Technical Standards” for the communication between payment initiation services and account-servicing payment service providers (Art. 66 para. 4 lit. a) PSD2) in accordance with Art. 98 para. 1 lit. d) PSD2, which specify the requirements for unified and secure open standards for the communications between account-servicing payment service providers, payment initiation service providers, account information service providers, payers, payment recipients and other payment service providers - for the purpose of identifying, authenticating, reporting and passing on information and using security measures. In addition to, for instance, guaranteeing a reasonable level of security for payment service providers, these regulatory standards are also aimed at ensuring the establishment and maintenance

of fair competition between all payment service providers and thereby guarantee neutrality in terms of the technology and business model (Art. 98 para. 2 lit. c) and d) PSD2).

90. One of the objectives of the PSD2 is to ensure continuity in the market until the directive is implemented into national law while at the same time providing existing service providers with the option of offering their services within a clear and harmonised legal framework, irrespective of their business model (see recital 33 PSD2[69]). To the extent that PSD2 establishes the form of and the conditions under which payment initiation services can be used in the future, regulations regarding the obligations of payment service providers in relation to payment instruments and personalised security credentials according to Art. 69 PSD2 - for the time until the development of the Regulatory Technical Standards and the implementation of the provisions in national law - do not per se contradict the aim of ensuring of the continued existence of payment initiation services. Where the payment service user is required to adhere to the conditions for the issue and use of a payment instrument, he must take all reasonable steps to protect thee personalised security credentials from third-party access after receiving them.

91. Based on the stated objective of PSD2 in recital 33 to maintain the existing business models of payment initiation services, the provisions of Art. 69 PSD2 specifically refrain from prohibiting the passing on of personalised security credentials to payment initiation services in principle. Doing so would result in discrimination against existing providers on the market, which the European legislator explicitly wishes to avoid through the transitional arrangements to maintain competition in the market.

---

[69] Recital 33 of the PSD2 reads: "This Directive should aim to ensure continuity in the market, enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework. Pending the application of those rules, without prejudice to the need to ensure the security of payment transactions and customer protection against demonstrable risk of fraud, Member States, the Commission, the European Central Bank (ECB) and the European Supervisory Authority (European Banking Authority), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council (11) (EBA), should guarantee fair competition in that market avoiding unjustifiable discrimination against any existing player on the market. Any payment service provider, including the account servicing payment service provider of the payment service user, should be able to offer payment initiation services."

92. In cooperation with the European Central Bank, the EBA plans to develop Regulatory Technical Standards for payment service providers within the meaning of PSD2 and transfer this to the European Commission, which will adopted these Standards. This will, among other things, define the requirements for procedures for strong customer authentication by payment service providers and the requirements for security measures to protect personalised security credentials of the payment service providers if, for instance, payment are initiated via payment initiation services, for instance (Art. 98 para. 1 lit. c) in conjunction with Article 97 paras. 2 and 3 PSD2). The Regulatory Technical Standards will specify the requirements for the security of open Standards for communication. The regulatory technical standard will therefore apply to all parties involved in a payment initiated using payment initiation services. The EBA will orientate the development of the Regulatory Technical Standards in accordance with the objective of Article 98 para. 2 PSD2 and, in addition to ensuring an adequate level of security, will also aim to maintain fair competition between payment service providers (Article 98 para. 2 lit c) PSD2), ensure that the standards are neutral in terms of technology and business models (Article 98 para. 2 lit d) PSD2) and enable the development of user-friendly, generally accessible and innovative means of payment (Article 98 para. 2 lit e) PSD2).

4. Organisation of online banking by the German banking industry

The GBIC takes over central tasks for the organisation and creation of a standardised and secure framework for the execution of payment transactions for the affiliated credit institutions. In doing so, the associations in the GBIC develop shared payment systems, agree standards for the same and procedures for compliance with such standards by certifying technical products (cf. a) below). The associations organised within the GBIC also organise industry-wide security standards and provide standardised interfaces for communication with other players on the market (cf. b) below) in the context of online banking. In addition, the activities of the savings and cooperative banks' data processing centres also contribute to the standardisation of the technical implementation of online banking (cf. c) below). The GBIC therefore plays a key organisational role in the operation of online banking.

a) Exercising of functions by the GBIC regarding banking-related and technical issues within the scope of payment transactions

93. The central associations in the banking industry work together within the GBIC and are responsible for a range of fundamental tasks which are performed on behalf of the entire banking industry.

94. The GBIC identifies itself as an advocate of common opinion and decision-making with regard to technical banking, banking policy and practical banking issues, focusing its activities in the areas of regulatory, securities and tax law. According to its own description, a further focus of its activities is the development of "Standards for payment transactions, including card payment systems".[70]

95. The exercising of functions by the GBIC in the area of payment transactions plays a central role for the affiliated credit institutions. Within this context, the GBIC not only takes over the classic tasks of advocacy, but also acts as a central coordinating body in matters which affect all affiliated credit institutions and which are of central importance for the development of joint projects. These often involve projects that require uniform technical solutions for the large numbers of credit institutions active in Germany [redacted] In the area of payment transactions, the GBIC has extensive experience in coordinating joint projects. These include, for instance, a system for cashless payments (debit card system)[71] and a payment system for

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

[71] Working together, the central associations of the banking industry organised in the GBIC are responsible for the nationwide introduction of the electronic cash process. The contractual basis of the electronic cash method is the "agreement on an institution-wide system for cashless payments at automated cashpoints (electronic cash system)".

withdrawing cash at ATMs.[72] GBIC operates a central registration office for the admission of service providers and products. [73]

b) Performance of tasks by GBIC within the scope of online banking organisation

96. Within the scope of online banking, GBIC has taken over fundamental tasks to realise the technical feasibility and security of the system for the affiliated member institutions. The technical interface developed by the GBIC for communication between banking customers and credit institutions using financial management software and other products is used by almost all German credit institutions. The development of industry-wide standards by the GBIC represents the (on-going) development of safety procedures for the use of online banking services. The preparation of shared terms and conditions for the affiliated central associations represents a task which the GBIC has jointly implemented for several decades.

aa) Interface definition

97. In order to allow bank customers to continue to use online banking, including after the expansion of the screen text (BTX) offered by Deutsche Bundespost in the 1990s through their own applications during the expansion of the internet (e.g. internet browsers

---

[72] The GBIC operates another payment system for the withdrawal of cash at ATMs. For this purpose, the GBIC entered into an agreement regarding the German ATM system, on the basis of which all ATMS operated in Germany are included in a shared system for mutual use. The GBIC also entered into a series of contractual agreements to expand available opportunities to use the ATMs operated by German credit institutions. The German ATM system, for instance, is part of the global Maestro and Cirrus ATM system of MasterCard Worldwide, whereby debit and credit cards with this logo can be used at ATMs worldwide. (agreement on the "German ATM system" of 15.01.2011, No. 1 c.), in: Payment transactions, policy, agreements, conditions, ed. by the Association of German Banks, Berlin).

[73] The GBIC grants the approvals for ATMs for operation in the German ATM system via the VÖB central registration office. For the purpose of communication between those participating in the ATM system, the GBIC has defined a standardised interface in the technical attachments and annexes of the regulations for the German ATM system. In order to demonstrate compliance with the requirements, VÖB performs an authorisation procedure on behalf of the GBIC. This includes proof of conformity, which is associated with a functional test and a safety evaluation. ATMs in the German ATM system can only operate after passing through the type approval. The authorisation also includes the requirements of the international card schemes, such as MasterCard and JCB for use at ATMs in Germany, whereby a specific accreditation of the equipment is not required. (http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/geldautomaten.html, Version 21.07.2014.

and financial management software), GBIC developed an interface called the **H**ome **B**anking **C**ommon **I**nterface (HBCI).[74]

98. GBIC entered into the home banking agreement for the introduction and industry-wide use of HBCI for banking transactions through electronic dialogue (home banking) with all credit institutions. The central associations of the GBIC as contractors thereby ensure that this is recognised by each credit institution, which allow their customers to exchange data within the scope of home banking. The declared aim of the agreement was to add further business transactions to the interface specifications. To this end, the plan was to create a working group in the GBIC, which was to be responsible for all matters arising in connection with the Agreement.[75]

99. HBCI was developed further in 2002 and replaced by the **Fin**ancial **T**ransaction **S**ervices standard (FinTS). FinTS also currently represents the central multi-bank interface used by users and third party service providers for communication within the framework of online banking.[76]

100. GBIC developed FinTS as an industry-wide interface standard supported by more than 2,000 banks and used by the manufacturers of online banking software products, with the result that customers have a variety of products to choose from.[77] The development of this single standard enabled the creation of industry-wide solutions through a variety of private sector deals. Through FinTS, GBIC has expanded communication, which only related to the communications between the customer and their credit institution within the scope of the HBCI interface, to include cases where customers involve so-called intermediaries.

---

74 The development of HBCI was intended to offer a secure and powerful communication interface for online banking credit institutions. The GBIC's objective was to provide online banking with security credentials which would also allow the service to be used in unsecured networks. The central approach was to create a unified industry standard so that account relationships could be managed with identical mechanisms and operate independently of the devices used. The uniform standard was expanded the scope of online banking at the time (issuing transfer orders and access to account information) with the aim of making online banking more attractive. Online banking customers benefitted from the same functionality, regardless of the devices they used. For credit institutions, the uniform standard made it simpler to create applications and maintain the systems. The GBIC also took the advantages for manufacturers into consideration when developing the HBCI in order to achieve planning security when designing customer-friendly home banking programmes http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf. p. 2f.

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

76 B4-71/10, Bl. 1677.

77 www.hbci-zka.de,Version 23.02.2011.

The FinTS standard is also designed for cases where intermediaries forward transaction data of the customer, including the PIN and TAN, to the credit institution in charge of the account within the scope of a FinTS message.[78]

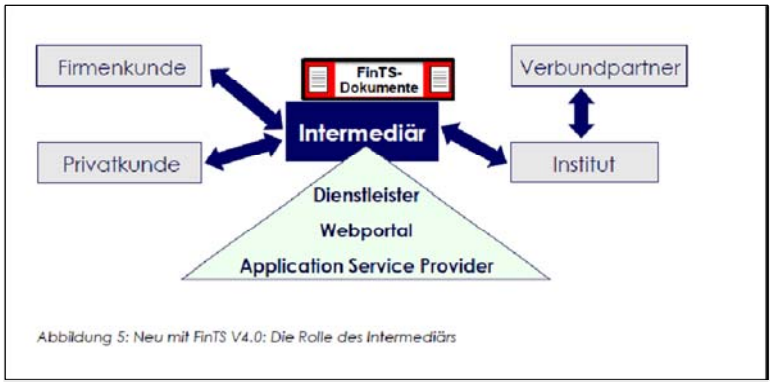

Fig. 4: FinTS V4.0 Compendium, p. 15, the role of the intermediary.

Kommentar [A3]: Corporate clients
Network partner
Private customer
Institute
Service provider
Web portal

bb) Definition of security Standards

101. GBIC has contributed significantly in the field of security standards in the further development of online banking by, for example, jointly creating new methods for the transfer of TANs.

102. Standards for the SMS-TAN procedure (cf. para 56) were jointly developed by the central associations within GBIC.[79] GBIC formulated common minimum security requirements for the use of the mobile TAN procedure and published these on its website.[80] In doing so, GBIC reacted to the vulnerability of other TAN procedures, so that credit institutions could continue to provide safe procedures to their customers when using online banking services. The fact that GBIC

78 FinTS V4.0 Compendium, Financial Transaction Services, the entry into the new world of online banking, http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf. 20.9.2015, p. 16.

79 Press release from the GBIC, Continuing to approach online banking with caution when using mobile TAN - the German Banking Industry give some security tips, 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,Version 25.06.2015.

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

cooperating associations have a central organisational role in the operation of online banking and determine the conditions of use is also evidenced by the fact that, on their website, they explicitly draw attention to the fact that the use of the SMS TAN procedure is not, for instance, permitted using one end device for both communication paths and is therefore explicitly ruled out in the customer conditions for online banking. [81]

cc) Development of common terms and conditions

103. The central associations of the banking industry jointly develop terms and conditions for the affiliated credit institutions.

104. Since the introduction of online banking, GBIC initially created the BTX services offered by Deutsche Post and later also the standardised customer conditions for the additional services being launched on the internet and as software products, which were adopted by the credit institutions.

105. GBIC jointly performed the revision of the (special) conditions originating from 1984 for the use of on-screen text[82] in 2000 and recommended them to its affiliated credit institutions for use. The "conditions for the account and deposit-related use of online banking with PIN and TAN" was filed with the Federal Cartel Office on 03.03.2000 as a joint agreement of the banking industry and was exempted from the cartel ban on 06.06.2000.[83] GBIC justified the central revision by comparing it to the specifications of comparable sets of conditions and mentioned the "Conditions of EC cards" as an example, which are issued by all German credit institutions to their customers for the use of account services and to perform payment transactions.[84]

c) Performance of tasks by data processing centres and credit institutions

106. In addition to the central associations, which perform a series of central tasks for all credit institutions operating in the area of retail banking,

---

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

82 Letter from the GBIC 02.11.2010, Annex 1.

83 B4-167/04.

84 Recommendations by the European Commission of 30.07.1997 on electronic payment instruments and changes to procedures and the improvement of transparency through the clear design and linguistic revision are mentioned as the main reasons for the joint revision.

the savings banks' data processing centres also perform central roles which the affiliated institutes of these banking groups cannot perform themselves due to their size and resources. This in particular includes the operation of a core banking system[85], but also the development and technical implementation of new applications such as software applications for use in connection with online banking.[86]

107. The “FI” operates data processing centres and systems in the savings bank organisation which are used by the savings banks in Germany. In the field of the cooperative sector, Fiducia&GAD is a service provider for the affiliated credit institutions.

108. FI and Fiducia&GAD also operate core banking systems for affiliated credit institutions and, in this context, provide banking applications that are imperative for the technical implementation of online banking and hence for handling the customer business of a credit institution. [redacted] [87]

109. FI operates a core banking system under the name "One System Plus" (Plus OS), while Fiducia&GAD currently operates two core banking systems called "agree" and "Bank21"[88]. These core banking systems are related to the use of the particular data centre services.

---

85 The concept of the core banking system, which was used by the Parties in various merger control proceedings before the Federal Cartel Office, but which is, however, not a fixed term, is understood in the following as the totality of applications for retail banks that allow the institutes to process and implement transactions in an electronic data map. The scope of services offered depends on the needs of the affiliated credit institutions.

86 Although the situation is different for some member institutes of the BdB due to their size, as companies such as [redacted] realise many services themselves, several smaller credit institutions in this banking group also use services of the cooperative data processing centres.

87 [redacted]

88 Fiducia&GAD was the result of a merger of two cooperative data centres, Fiducia IT AG, Karlsruhe and GAD eG, Münster and operated different core banking applications under the brands "agree" and "Bank 21". In the future, the two core banking systems of the merged Fiducia&GAD will be replaced by the product "agree 21" (https://www.fiduciagad.de/ueber-uns.html).

110. A series of the two providers' services are used by all affiliated credit institutions. The FI provides more than of its services to all savings banks. The online banking websites of the savings banks are also implemented by an application used by all savings banks. The same applies to Fiducia&GAD, which is responsible for the full technical implementation of online banking for the cooperative banking group.

5. Further development of online banking via additional applications

111. Online banking is a service of the banking industry with high development dynamics resulting from technical innovations, which relates to both the hardware used and the applications. Over the past few years, further services have been added to the original uses of online banking via the web pages of the account –servicing credit institutions , which customers can use as part of the online banking services. In many cases, these services operate on mobile devices (e.g. smartphones). In addition to the products offered and operated by banks, products are also available from bank-independent providers. These products usually provide access to online banking via the shared FinTS interface of the GBIC and the entry of personalised security credentials. To the extent that these products retrieve and process information such as PIN and TAN, different approaches are available. This can be achieved through the hardware used by the customer or through the provider's infrastructure. In contrast, payment initiation services provide access to online banking via the online banking website of the credit institution, which the customer also uses for its own access to account.

a) Examples of activities of the savings banks group

112. Star Finanz GmbH ("Star Finanz"), a subsidiary of Finanzinformatik ("FI"), develops and markets a variety of software products under the name Star Money for customers' personal financial management. The software is marketed in a version to be stored on the customer's end device (StarMoney) and as an online version (Starmoney.web). When using these products, which are compatible with multiple banks and can be used for accounts with all banks in Germany, the customer also needs to enter his personalised security credentials.

aa) StarMoney

113. StarMoney is a software which is installed by customers on their device. It can be used to view different accounts and actively manage them. The customer can manage accounts held both online and offline. While the customers themselves perform the entry of bookings and entries in the case of offline accounts, the information is read from the systems of the account-servicing companies i in the case of online accounts. This is not limited to the accounts of GBIC member institutions, but also applies to accounts with companies such as eBay and PayPal. StarMoney gains access to credit institution accounts through the FinTS interface provided by the banking industry, which in turn enables access to the data processing centre of the account-servicing credit institution. StarMoney obtains the account data on the internet through the respective interfaces. The data can then be evaluated on the customer's device. In addition to the retrieval of account information, StarMoney can also be used to issue payment orders (transfers).[89]

114. The customers need to enter their authentication information into the system to gain access to the accounts and transfer data or issue instructions. This is the data which also needs to be entered when gaining direct access to the account via the internet browser (account number, PIN and possibly additional access data). When issuing orders to the account-holding bank, the customer enters the corresponding authorisation information through the StarMoney software - this usually includes a TAN, which is provided to the customer by the account-holding credit institution. The communication between the user's computer and the account-holding institution is encrypted without the intervention of a third party, which means that Star Finanz does not gain any access or knowledge of the personalised security credentials of the account holder through the software.

115. To secure the software, Star Finanz has developed a series of additional measures and mechanisms in order to prevent the misuse of the personalised security credentials for identification and authorisation in online banking. Among other things, this includes the independent development of all components which StarMoney

---

89 Product description at www.starmoney.de.

uses to communicate with the data processing centre interfaces of the account-holding credit institutions (so-called kernel, see also explanations about DATEV services under para 166).

bb) StarMoney Web

116. Star Finanz also offers StarMoney as a browser-based program as a free basic version and a paid full version called StarMoney Web. The user is required to register in a portal operated by Star Finanz in order to use both versions. The software, which can be accessed using an internet application, can be used to manage accounts, i.e. access and evaluate account data. It is also possible to issue payment orders using this software.

117. StarMoney Web is not run on the customer's hardware, but in Finanzinformatik's data processing centres. The user communicates with Finanzinformatik's data processing centre via Star Finanz's software integrated into the internet browser (Java applications[90]), which creates an encrypted direct link to the data processing centre of the respective account-holding credit institution without sending the PIN and TAN to Star Finanz. This communication is only possible with banks with a FinTS interface for their online banking services. The customer enters their access data for the account via this link, including the personalised security credentials. These include both the PIN for identification and the TAN to authorise instructions sent to the credit institution in charge of the account. Apart from the personalised security credentials, the retrieved account data is transferred to and stored on the Star Finanz servers. The user can delete the data stored on the servers at any time.

118. Different types of account can be used and managed at the same time with StarMoney Web. These include current, deposit, credit card, building society and loan accounts.

119. The account information is stored on Star Finanz's servers, which are not banking servers. As Star Finanz does not offer banking services, the servers are not subject to supervision by BaFin.

---

90 A program written in the Java programming language which is executed via a web browser in a standardised runtime environment without the need to provide data from the user's terminal or from the server (Finanzinformatik in this case).

120. The personalised security data entered into the software provided by Star Finanz (Java applications) and the customer data saved on Star Finanz's servers is not entered through the website of the respective credit institution in charge of the account as stipulated in the Special Conditions for Online Banking. Star Finanz has no contractual relationship with the account-holding credit institutions whose data it stores on its own servers. There are no separate agreements.

b) Examples of activities of the cooperative banking group

121. Fiducia&GAD serves all cooperative banks. Previously, Fiducia IT AG and GAD eG respectively offered independent technical services for some of the institutes (cf. footnote 88). To this end, the two companies have developed their own technological products for their customers which complement the respective network-wide products of the cooperative banking group.

aa) "ELAXY Finanzmanager"

122. GAD distributes "ELAXY Finanzmanager" as a personal finance management system. The product is developed and operated by a subsidiary of GAD, which distributes the product to financial service providers inside and outside the cooperative banking group. The product has multi-bank capability. The product is currently only available within the cooperative banking sector for credit institutions to use with their own accounts. [redacted] Outside the cooperative banking sector, however, the product is sold with full multi-bank capability.

123. "ELAXY Finanzmanager" is a system which can be used, for example, for the analysis and categorisation of account transactions or to obtain an asset development statement. The product is used as a web application and is available for use on all common end devices. Account information is retrieved through the FinTS interface by "ELAXY Finanzmanager". It is not possible to issue instructions to the credit institution in charge of the account, so there is no entry of TANs to authorise instructions.

124. [redacted]

bb) "Online-Filiale+"

125. GAD also sells a software application (app) called"Online-Filiale+" for use on mobile devices (e.g. smartphones). The app is distributed through online stores such as those for the iOS and Android operating systems, installed on the respective devices of the customers and used on these devices. To access the program, the customer chooses a password that needs to be entered before using the app.

126. The software enables customers to access account information and issue a variety of instructions, such as bank transfers, transfers and standing orders. Basic security settings for online banking can also be changed using this software. This includes, among other things, PIN changes. [91]

127. Due to the multi-bank capability of the app, customers can use all accounts of different credit institutions at the same time, as long as the respective credit institutions in charge of the accounts support the FinTS interface.

128. Independently of the bank in charge of the account, the account is accessed using the standard access data for online banking with the respective credit institution and by entering the PIN. The software can store the encrypted PIN on the respective end device as an alternative. The customer is informed within the app that saving the HBCI-PIN is prohibited by most banks in their security conditions. The customer can confirm that they wish to save their PIN at their own risk by clicking on a control field. This applies both to cooperative accounts and accounts held with other banks.

---

[91] p. 6719 et seq. of the file

Fig. 4, **Screenshot** of the app "Online-Filiale+"

129. In order to issue the instruction, the customer requires a TAN, whereby the software only supports the smart TAN procedure, i.e. the customer can only use those types of TAN which they have created themselves using their chip card and TAN generator. Communication between the app and the credit institution in charge of the account takes place via the web interface. The encrypted data is only transmitted from the user terminal to the credit institution in charge of the account.

c) Examples of payment initiation services in e-commerce

aa) Sofortüberweisung.de as a bank-independent payment initiation service

130. Among other services, Sofort operates a payment initiation service for e-commerce under the brand sofortueberweisung.de. The service is used to pay for goods and services in online shops and to replenish digital wallets, which in turn are used for payment in e-commerce.

131. Sofort markets the payment procedure to merchants and alternatively uses the services provided by Payment Service Providers (PSP). PSPs are companies which allow merchants to accept electronic payments. PSPs are responsible for contractually and technically connecting the merchant usually to different payment methods. For this purpose, the PSPs provide technical

interfaces for the payment methods, which are linked to the merchants.[92] To the extent that Sofort markets its own payment procedures, it enters into an agreement with the merchant and also realises the technical connection of the merchant to the payment system.

132. If the payment method sofortueberweisung.de is shown to the customer as an option when buying goods, they will be forwarded to Sofort's technical system once they have selected the option and can then enter the required data to initiate the payment process. At the beginning of the transaction, the customer receives information in the data protection notification about how the sofortueweweisung.de procedure will be performed, which tests take place and what personal data is collected. The customer will also be informed about the personal data which is passed on, when this occurs and who receives the data. The privacy policy also contains information about the nature and duration of the storage of personal data and the actions which will be taken by Sofort if there is a subsequent message stating that the transfer to be performed by sofortueberweisung.de using online banking has failed, in addition to a contact email address for the customer to ask Sofort any further questions.

133. When using sofortueberweisung.de, the customer selects their credit institution and provides the corresponding account number and enters the personalised security credentials for authentication by the credit institution. The payment system provides access to the online banking services of the respective credit institution via interfaces defined by the GBIC for communication with third party providers(FinTS or HBCI) or by using screen scraping[93], if individual banks do not use the interface standards of the GBIC. sofortueberweisung.de passes on the encrypted account information and personalised security credentials directly to its own data processing centre, which in turn sends it on to the credit institution in encrypted form. The data processing centre used by Sofort is a bank computer centre (data centre of Deutsche Kontor Bank AG), whose security standards are subject to the supervision of BaFin,

---

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

93 "Screen scraping" is a technology for extracting data from websites. See Federal High Court of Justice, Flugvermittlung the Internet (I ZR 224/12), 30. 04. 2014 principle, quoted from juris.

even though these special serves are not currently integrated into the supervision.[94]

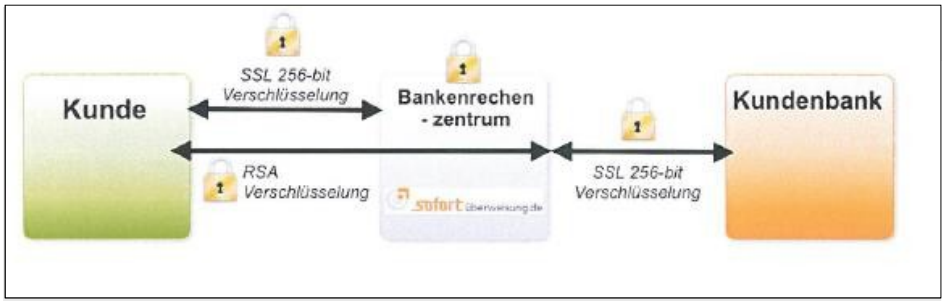

Figure 5: Encryption when using sofortüberweisung.de[95]

Kommentar [A4]: Customer
Encryption
Bank data centre
Customer's bank

134. [redacted]

135. [redacted]

94 [redacted]

95 [redacted]

136. [redacted]

137. [redacted]

138. [redacted]

139. [redacted]

140. [redacted]

bb) Payment initiation services of credit institutions

(1) giropay

141. The payment initiation service giropay[97] also provides merchants with the opportunity to allow customers to pay for goods and services through their credit institution's online banking service.

---

96 Credit institutions booking in real time are those whose systems directly execute and book payment transactions and therefore always allot new transactions on the basis of an up to date account balance.

97 The following description of the payment procedure giropay is based on the responses by giropay GmbH to the Federal Cartel Office's request for information on 05.10.2010 in the cartel administration proceedings B4-72/10, unless other sources have been used.

142. The shareholders of the companies Star Finanz and Fiducia&GAD are the current operators of giropay. Their systems are both operated in the secure environment of a bank data centre, although the security of these centres is not subject to review by the banking authorities.[98] The technical operation includes the technical connection to the respective credit institutions who have decided to participate in the payment initiation services, in addition to the acquirers and Payment Service Provider[99] that realise the contractual and technical connection to the merchant.

143. To the extent that the payment initiation service operators use different technical systems, these are connected to each other via interfaces in order to perform transactions, whereby the credit institutions of the customers and the merchants have concluded agreements with different operators in each case.

144. The customer decides to pay for goods or services with giropay. After selecting the payment initiation service as a payment method, the customer gains access to the giropay website of its credit institution in the operator's system, where they can enter their online banking access details. After entering their PIN, the system will display a pre-filled transfer template and asks the customer to authorise the transfer by entering a TAN. The bank schedules the transfer following the entry of this TAN and accepts it after a positive check has been performed.

145. If the invoice amount is successfully processed, the customer's credit institution sends a payment guarantee to the internet merchant or its acquirer.[100] For this purpose, the GBIC has defined and introduced a special text key for irrevocable internet transfers, which is used by giropay.

(2) Paydirekt

146. Paydirekt is a payment system provided by German private banks, cooperative banks and savings banks. It is a payment initiation service for merchants in e-commerce. The system has been available on the market since the end of 2015.

147. When using the service, the merchant transfers the customer to the Paydirekt system in order to initiate the payment through the customer's current account.

---

98 Letter from BaFin of 08.08.2012, p. 3336 ff.. of the file

99 The giropay Rules and Regulations define a PSP as a technical/operational service provider commissioned by the acquirer, Rules and Regulations, p. 4, Version 25.02.2009.

100 Letter from the GBIC 02.11.2010, p. 456 of the file

The customer needs to log into this system to initiate the payment from their current account. Following successful completion of the payment, the merchant receives a payment guarantee.[101]

d) Examples of other services provided by bank-independent service providers in connection with online banking

148. Products relating to online banking are also developed and distributed by bank-independent providers. Their range of functions includes account balance requests and issuing payment orders. The products can also be differentiated on the basis of whether they are operated on the end device of the respective user or on the server of the respective provider. These services use banks' infrastructures in different ways. Customers also usually enter the personalised security credentials required for access to online banking for these offers. The customer is unable to regularly check how the corresponding service provider processes this data. The following services are to be understood as examples and do not provide a complete overview of the market.

aa) WISO Mein Geld

149. The company Buhl Data Service GmbH, Neunkirchen, has provided different software products related to the use of online banking since 1993. The company's top-selling product is the software sold under the name "WISO Mein Geld". [102]

150. The WISO Mein Geld software is a Personal Finance Management Software which is used to request, display and analyse account transactions, portfolios and account statements from different credit institutions. The software accesses accounts via the FinTS interface as long as the credit institution in charge of the account uses this interface provided by the GBIC, otherwise by

---

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

102 In addition to "WISO Mein Geld", the company also sells software with specific functions for certain commercial applications ("Wiso Mein Büro", "WISO Kaufmann"), although they do not support administrative account functions or relate to specific areas of application, such as the creation of income tax returns ("Wiso Steuer Sparbuch T@x") or property management ("WISO Hausverwalter"), but do provide access to account transaction data.

reading out the website of the respective credit institution (screen scraping[103]). In this case, the software connects to the bank through the internet and receives the required account data, which is then read before being imported and processed in the software.

151. In addition to retrieving account transactions, all standard business transactions can be conducted using the software. These include, for example, issuing transfers and standing orders and the submission of direct debits. The software can also be used to manage administrative orders relating to personalised security credentials. Users can block and change their PIN and request and block new TAN lists via the software.

152. The various software products do not transfer the account details through the Buhl Data server. All communication takes place between the customer's computer and the credit institution's computer via the FinTS interface, or an internet browser if the software reads out the account details. The software asks for account information as soon as the customer initiates this manually or at the time intervals specified by the customer. The software encrypts the access data for online banking and saves it in a database on the customer's computer. The PIN is only stored if the customer explicitly selects this option.

153. There has been no contact or exchange regarding the software products, neither with regard to the functionalities, security issues or other topics between Buhl Data and the German banking industry - at least not in the past ten years since the introduction of the program and until 2012.

bb) Finanzblick

154. In addition to its range of software installed and operated on the customer's computer, Buhl Data also offers a product called Finanzblick. The program can be operated on smartphones (iOS and Android) or as a web application. The web application provides the customer with access to the technical infrastructure of Buhl Data where the program is operated, via an

---

103 Use of an automated system or software to extract data from a website so that it can be displayed on another website ("screen scraping"), cf. Federal High Court of Justice, decision of 30.04.2014, file ref. I ZR 224/12,paragraph 3.

104 Letter from Buhl Data of 13.07.2012, p. 3305of the filehttps://play.google.com/store/apps/details?id=subsembly.banking.

internet connection. The communications of the applications for smartphones are at least partially passed through the company's servers.

155. The storage of access data in connection with the use of products takes place on the customer's device in the case of the smartphone application and on the Buhl Data servers when using the web application. To gain access to the data, the customer needs to register and create a password, which prevents access to the web application by unauthorised third parties.

156. Finanzblick uses the so-called screen parsing to transfer the data. To do this, for example when issuing a transfer instruction, the required data (account access data and PIN, potentially also a TAN, account number of the recipient and purpose) initially needs to be sent to the Finanzblick server in an encrypted form, where it is stored as temporarily encrypted data according to technical requirements, before being encrypted once again and sent to the customer's bank. The booking data is then sent back from the bank in encrypted form. It is also stored as temporarily encrypted data on the Finanzblick server on the way back. Company employees have no access to this data at any time.[105]

157. Essentially, the Finanzblick product provides functionality which is comparable to that of the WISO products. Customers can check account transactions and issue payment orders, including standing orders. Only administrative transactions are not covered by the program.

158. Buhl Data operates separate servers in Germany to save customers' account data, where the data for each customer is saved separately in encrypted form.

cc) Other applications

159. Bank customers with an online banking account have access to the account information of credit institutions and the ability to issue payment orders, but can also do so using other apps that run on mobile devices. Such services are offered by both the banks[106] and bank-independent providers[107]. The services on offer

---

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

107 Letter from Buhl Data of 13.07.2012, p. 3305 of the file

differ in scope. Some only allow customers to view transactions[108], while others allow them to manage various banking transactions, such as issuing transfer instructions or purchase and sale orders for securities transactions. The products available on the market are also designed differently in terms of the multi-bank capability, i.e. simultaneous use for accounts with different credit institutions. While, for example, Commerzbank products can only be used for the company's own accounts, the Commerzbank subsidiary comdirect offers an app which can be used to access the accounts and deposits of different banks. Non-banking products are usually designed to aggregate customers' various bank accounts using the HBCI / FinTS interface of the banking industry.[109]

160. The customer can use the software installed on the mobile end device to enter online banking access data and thereby gain access to the account data of various credit institutions and issue instructions according to the scope of the services. The instructions are authorised using the TAN procedure offered by the corresponding credit institution. Where necessary, the account information is stored on the mobile device used to operate the software.

(1) Kontoblick

161. Kontoblick is another example of a product offered exclusively for use on the internet, which Kontoblick GmbH launched at the end of 2014. The company, which was later liquidated following the initiation of insolvency proceedings on 06.09.2012[110], continued to offer the services described below until the end of 2014.[111] GBIC listed this service as an example of how business models can be implemented without violating the duties of care.

---

107 https://play.google.com/store/apps/details?id=subsembly.banking,Version 20.09.2015.
108 KontoVersion-App der Commerzbank, https://www.commerzbank.de/portal/de/privatkunden/service-und-hilfe/ihre-wege-zu-uns/mobile-banking-apps/apps.html,Version 01.10.2014
109 http://www.pc-magazin.de/vergleichstest/apps-online-banking-test-android-iphone-starmoney-outbank-1944244.html, Version 01.10.2014.
110 Except from the commercial register of Kontoblick GmbH, District Court of Charlottenburg, HRB 133711 B, downloaded on 09.24.2014.
111 The description of how the program works is based solely on the description of the company on its own web page.

162. Kontoblick offered users the option of summarising and evaluating sales in online bank accounts. This included categorising sales and showing overall balances indicating the customer's asset situation in the corresponding accounts.[112] In addition to the online accounts with different credit institutions, the integration of credit card accounts, instant access accounts and savings accounts were also available.

163. The service was available in two different versions. A maximum of two accounts could be managed in the free version. In the paid version, the user was able to manage an unlimited number of accounts and benefit from a more elaborate categorisation of cash flows.[114]

164. Kontoblick gained access to the online banking systems of various credit institutions via GBIC's FinTS interface.[115] Access to the account and account data retrieval was performed via FinTS and a Java application integrated into the website by Kontoblick. It was not possible to conduct transactions that would change the account balance in any other way or initiate other online banking transactions using Kontoblick. The accounts were accessed via Java applications in an encrypted connection that only involved the customer and credit institution. Account transactions were routed through the customer's computer to Kontoblick, used there to display and categorise the account balance, after which they were saved in encrypted form, without the employees of Kontoblick gaining access to the personal data.[116] Kontoblick allowed users to save their personalised security credentials required for online banking, which made it easier to view the account information when logging back into Kontoblick.

165. Kontoblick combined the information gained from the online banking system with its use for market research purposes. The customers implicitly agreed, within the scope of the "Privacy policy statement and consent to the collection, storage and processing of personal data", that Kontoblick is entitled to use and pass the transferred data on to third parties in an anonymised form, only linked to the user's post code, for market research purposes.[117]

---

112 Printout from Kontoblick website p. 6300 of the file
113 Printout from Kontoblick website p. 6200 of the file
114 Printout from Kontoblick website p. 6292 of the file
115 Letter from the GBIC 09.08.2011, p. 1709 et seq. of the file, Printout from Kontoblick website p. 6288 of the file
116 Printout from Kontoblick website p. 6290 of the file
117 Printout from Kontoblick website p. 6286 of the file

(2) Datev

166. Another product with a number of special features is offered by Datev eG, Nuremberg. Datev is a company with the legal form of a cooperative, whose members primarily comprise tax consultants, lawyers and accountants.[118]

167. DATEV distributes enterprise software and IT services, in particular to its members and their clients. Its range of services includes payment solutions[119] which provide the opportunity to access online banking accounts and send payment orders to banks. The connection to the bank data centre is not created between the customer and the credit institution in charge of the account, but through Datev's own data processing centre. The payment solutions are used by DATEV to connect the company's other applications (such as financial accounting and payroll records) with the banking systems and, for example, to import and register account transactions and issue payment orders.

168. Datev uses a so-called HBCI kernel, a software component hosted and licensed by institutions in the banking industry, to access the bank data centre. The HBCI kernel provides a link between the participating data centres and provides Datev with the opportunity to gain access to the online banking services of all German credit institutions, thus ensuring that their own products have multi-bank compatibility. The HBCI Kernel accepts transactions and associated data in an XML syntax used by the Datev applications, converts them to the required HBCI-compatible syntax and executes the transaction by establishing the connection to the data centre of the relevant credit institution and passing on the data.

169. Datev also accepts PINs and TANs through its systems in order to initiate payment orders. These are encrypted through the applications and sent to Datev's data centre, where they are decrypted before being passed on to the data centre of the respective credit institution. They are stored in Datev's data centre before transfer to the HBCI kernel in plain text. Immediately after transfer to the appropriate credit institutions, the sensitive data is deleted in an automated process.

---

118 Credit institutions do not belong to Datev's member group.

119 Datev-Zahlungsverkehr (Windows PC solution) since 2004 and Datev-Zahlungsverkehr online (Internet Solution) since 2007.

170. Datev has not entered into any contractual agreements with the banking industry regarding the acceptance and transmission of PIN and TAN, nor have any joint security concepts been developed, and the service has not been reviewed and approved by the banking industry.

VI. Reaction of the GBIC to the services offered by providers in connection with online banking

171. In recent years, the GBIC has been intensively involved in the security of its system in the light of misuse and has discussed security issues.

172. Within the context of online banking services, the GBIC has spent years taking action against systems which acted as payment procedures in e-commerce and used PIN and TAN for the initiation of payments. The GBIC has explicitly dealt with such service providers when developing an intermediary concept, in which the GBIC has established its position towards the different service providers in connection with online banking (see 2). After the completion of its work on the intermediary concept, GBIC formulated the regulations for dealing with payment initiation services as payment procedures in e-commerce within the scope of the development of the general terms and conditions (duties of care of customers when using online banking) (see 3). Risks posed by intermediaries other than payment initiation services were not discussed during this period. Following the completion of the work on the Online-Banking-Conditions, GBIC also specified how to deal with payment initiation services within the scope of its own public relations work (see 4).

1. Payment methods in e-commerce relating to online banking

173. Along with the development, expansion and use of the internet, various services were developed from 2000 onwards, which also included online banking services offered by the credit institutions. To the extent that these services involved the payment of invoices through access to the credit institutions' online banking systems or internet-based account aggregation services which are associated with the entry of personalised security credentials, GBIC jointly tackled such services. The GBIC regularly refers to the duties of care in the existing Online-Banking-Conditions, which prohibit customers from entering personalised security credentials on non-bank websites.

a) L'TUR Tourismus AG

174. The company L'TUR Tourismus AG (L'Tur) launched a service in 2000 which allowed customers to pay for travel bookings using online banking. GBIC instructed L'Tur to stop offering the service with reference to the existing Online-Banking-Conditions. With reference to the regulations of the "*conditions for account/deposit-related use of online banking with PIN and TAN applicable in the German banking sector*", L'TUR was informed that PIN and TAN, as media which is to be kept confidential, can only be used when dealing with the issuing credit institution within the scope of the use of online banking, which is why the general terms and conditions have standardised the obligation of the customer to ensure that no other individuals gain access to the PIN and TAN. Drawing attention to the fact that the request to enter a PIN and TAN is an inducement to breach contractual obligations, the GBIC demanded that L'TUR cease the provision of its service.[120] L'TUR stopped offering its service at this point in time, as corresponding press reports indicated that customers were breaching their contractual obligations in the existing general terms and conditions of the credit institutions by entering their PIN and TAN on L'TUR's website.[121] L'TUR did not begin to offer the same services following the discussion with the GBIC and instead modified them technically in such a way that the PIN or TAN needed to be entered directly on the credit institution's website. The service no longer had multi-bank compatibility and was now only available for Postbank customers.[122]

b) "moneyshelf.com"

175. GBIC also took action against Deutsche Bank's product sold under the name of "moneyshelf.com", once again with reference to the existing provisions of the online banking conditions. Moneyshelf was a financial portal of Deutsche Bank where customers could view a summarised version of their financial status at different credit institutions on a web page and could also manage the acquisition of funds, stocks and insurance products. In this case, GBIC once again contacted the company to draw its attention to the provisions of the online banking conditions and the obligation of the customer to keep their PIN and TAN

---

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

confidential and not make it accessible to third parties.[123] Discussions were held with Deutsche Bank in the GBIC working group Homebanking in order to develop a joint solution.[124] Deutsche Bank removed the product from the market following the discussion with the GBIC.

c) "Online transfers" by T-Online International AG

176. In 2001, , GBIC attempted to shut down the internet portal for online banking operated by T-Online International AG, a subsidiary of Deutsche Telekom AG by the way of discussions and correspondence. GBIC raised concerns with the company in 2003 in various letters regarding the offer of a payment initiation services with the name "Online-Überweisung" (online transfers) and referred to the fact that it considered this to be a breach of applicable law. In this regard, GBIC referred to an inducement to breach contractual obligations by instructing the customer to enter the personalised security credentials which were to be kept confidential from third parties in accordance with the online banking agreement. T-Online did not comply with GBIC's request to cease this conduct, despite being threatened that the affiliated credit institutions would be informed and supported in pursuing their legal rights.[125] Deutsche Telekom still offers the product today.[126]

d) "sofortueberweisung.de"

177. Finally, GBIC also asked Promido GmbH, which operated the payment initiation services sofortueberweisung.de at the time, to stop this service within the scope of a lengthy exchange of correspondence, as its use was claimed to breach the legal stipulations of the customer conditions and encouraged customers to breach their contractual obligations. Again, reference was made to the regulations in the Special Conditions for Online Banking, according to which customers are obliged to ensure that third parties have no knowledge of their PIN and TAN for online banking.

---

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

2. Preparation of the " concept for intermediaries "

178. The substantive involvement of GBIC in particular with regard to bank-independent payment initiation services as part of the the so-called "intermediaries concept" highlights the strategic concept pursued by GBIC and its affiliated central associations; this strategic concept is reflected neatly in the contested version of the OBC at hand. The "intermediaries concept" and the OBC have been discussed within the same working group (on online banking) of the GBIC with an identical purpose.

179. [redacted][127]

180. [redacted][128]

181. [redacted]

---

127 [redacted]

128 [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 this context footnote 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. Revision of the Online-Banking-Conditions as part of the general terms and conditions

197. Another reaction of GBIC to the services offered by providers in connection with online banking was the revision of the Online-Banking-Conditions as part of the general terms and conditions. The associations in the banking industry working together within GBIC adopted the revision of the general terms and conditions, either as an explicit mandate or within the scope of the statutory tasks performed for the credit institutions affiliated with GBIC. They worked in various working groups while developing the online banking conditions. The Online-Banking-Conditions, which include the duties of care of the customers when using the online banking services, include provisions which prevent the use of bank-independent payment initiation services.

a) Mandating the central associations for the development of model terms and conditions for credit institutions affiliated with GBIC

aa) DSGV

198. The DSGV was involved in the revision of the Online-Banking-Conditions on the basis of its statutory tasks. There was no explicit mandate to revise the General Terms and Conditions of its member institutes or of its regional associations.

199. The statutory mandate resulted from the task of promoting the common interests of its members (regional associations) and their affiliated credit institutions by providing advice, exchanging experience and providing support with regard to legal provisions and other provisions.[143] In this context, the promotion of cashless payment transactions is explicitly mentioned.[144]

---

141 [redacted]

142 [redacted]

143 [redacted]

144 [redacted]

200. The DSGV decided, along with its regional associations, to participate in the drafting of the Special Conditions for Online Banking within GBIC,[145] discussed drafts of the Special Conditions for Online Banking with the regional associations [146] and, in turn, made their feedback the subject of discussion in the GBIC.[147]

bb) BVR

201. The participation of the BVR in the revision of the Online-Banking-Conditions resulted from the statutory tasks of the association which, among other things, include advising members on legal matters. [148]

202. The BVR was granted a contractual mandate for the coordination of the work required for the revision of the Online-Banking-Conditions within GBIC for the entire group

[redacted]

The aim of the project is formulated as the implementation for the entire cooperative banking group. [151]

203. The network-wide coordination of the revision of the Online-Banking-Conditions was discussed with the online banking project team, which was set up within the scope of a

[redacted]

working group of the cooperative data processing centres. [152]

[redacted]

cc) BdB

204. The representation of its members by the BdB as part of the cooperation with the central associations of the banking industry originates from a statutory provision for issues that are not confined to the area of the individual regional associations. [153] The BdB has contributed to the working groups organised within GBIC during the revision of the Online-Banking-Conditions without an additional mandate of its members. [154]

[redacted].[155]

205. On 25.06.2009, the legal committee of the BdB passed a resolution to approve the OBC in the form determined by the GBIC. [redacted].[156] The final version of the OBC is dated 13.07.2009. [157] In a circular dated 22.07.2009, the BdB recommended to its members to use the OBC that had been decided. [158]

b) Implementation of the Online-Banking-Conditions in the relevant bodies of GBIC between 2006 and 2009

206. The GBIC revised the Online-Banking-Conditions in the two working groups - ”Online Banking” and ”Online Banking Contracts” from 2006 to 2009. [159]

207. Representatives of the banking associations BdB, BVR and DSGV and representatives of the IT service providers of the savings bank group (SIZ) and of the cooperative banking group (GAD)

---

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

as well as of the private commercial banks (BV-payment systems GmbH) were represented in the online banking working group (hereinafter: AK-OB). External consultants were also involved in the AK-OB. [160] The online banking agreement working group (hereinafter: AK-OBV), on the other hand, did not include representatives of external consultants. Each association was also represented in the AK-OBV via their respective legal departments. [161]

208. At this time, the AK OB addressed a variety of issues relating to online banking. In addition to the Online-Banking-Conditions this included, for instance, the development of the "intermediaries concept" described above, the further development of the FinTS specifications and the problems associated with phishing.

209. The GBIC's revision of the special conditions began in 2006 in the AK-OB. [162] The first meeting, in which the topic "customer conditions" was discussed, took place on 30.03.2006. [163] To prepare for the meeting, the DSGV distributed a presentation to the participants which addressed the current problems associated with the existing online banking agreement. [164] Specific problems raised included the complexity of the existing rules and the lack of short-term adaptability to technological developments, such as newly-introduced TAN methods or giropay. The DSGV did not consider the existing duties of care of customers to be sufficient and proposed the establishment of additional individual duties of care. The disclosure of PINs and TANs to third parties was discussed both in connection with the "phishing and intermediary issues" and along with the resulting aim to find more precise formulations for the dutiesn of care in relation to the "disclosure of PINs and TANs to third parties". [165] As a recommendation, the DSGV's presentation proposed moving certain technical details into the procedural manual or into the security instructions, respectively, which are separate from the customer terms and conditions,

---

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

whereby, in addition to the general parts to be regulated by the GBIC, there was also an opportunity to enable supplements of individual credit institutions or associations. The DSGV also recommended an update of the necessary rights and obligations in the Online-Banking-Conditions and mentioned the duties of care of customers as an example. [166] At the meeting, the participants of the AK-OB agreed to initially discuss how to proceed within the individual associations. [167]

210. Further discussions were held in 2006, which were attended by representatives of the associations BdB, BVR and DSGV the AK-OB. During these meetings, the main point of discussions was preparatory measures for the development of new joint customer conditions. As of yet, no specific formulations of the customer conditions were made. In a meeting on 22.08.2006, the BVR spoke in favour of centrally proposing or recommending the customer conditions. The BVR emphasised that these rules were under close scrutiny of the competition authorities. The participants of the AK meeting considered it to be the responsibility of the legal practitioners to formulate joint customer conditions with the support of the working group. [168] At a meeting on 14.12.2006, the members explicitly agreed to the development of joint customer conditions in 2007. [169]

211. A first draft of the customer conditions was sent by mail to the members of the AK-OB in 2007 by the DSGV central coordinator in preparation for the special session on 27.04.2007. [170] This draft already included additional duties of care of the customer when dealing with PINs and TANs, which went beyond the existing provisions. Further duties of care for the use of PINs and TANs and when gaining access to online banking services were included in the draft sent for the meeting. For one thing, participants were required to use only the online banking access channels separately specified by the credit institution when creating a technical connection with the online banking services of the credit institution. With regard to the confidentiality of the PIN and TAN, the duties of care contain the requirement that

166 [redacted]

167 [redacted]

168 [redacted]

169 [redacted]

170 [redacted]

queries submitted outside the online banking access channels specified by the credit institution must not be answered.[171]

212. Based on the draft customer conditions of 27.04.2007, work continued on the Online-Banking-Conditions with the involvement of the legal departments of the associations. Given the requirements when dealing with PINs and TANs, the working groups discussed the introduction of a standard generic term, such as "identification data" or "security data". [172] The May 2007 version of the duty of care included the following formulation for the security of the identification data: "*Queries, in particular those relating to confidential identification data, which are submitted outside the online banking access routes separately specified by the credit institutions must not be answered.*" [173] In the version of June 2007, this term was temporarily replaced by separate duties of care for the use of PINs and TANs.[174]

213. Work continued on the Online-Banking-Conditions in 2008. The discussions also dealt with the effects of the EU Payment Services Directive on the Online-Banking-Conditions and in particular the duties of care of customers. [175]

214. The AK-OBV discussed customers' duties of care against the background of dealings with intermediaries at the meeting on 11.03.2008. This included making an explicit link between the issue of dealing with intermediaries and the duties of care associated with online banking access.

[redacted]

---

171 [redacted]

172 [redacted]

173 [redacted]

174 [redacted]

175 [redacted]

176 [redacted]

[redacted]

215. This formulation also reflects the status of customers' duties of care in the draft special conditions following the meeting of 11.03.2008. [177]

216. The relationship between the duties of care and the handling of intermediaries was highlighted even further in the draft special conditions of 16.04.2008. The outcome of this meeting was a newly amended formulation, according to which the authentication information cannot be entered on web pages that are external to the credit institutions (e.g. merchant web pages).[178] For this purpose, the draft includes a commentary as a footnote, which clarifies the connection between the formulation and handling of intermediaries. This envisaged that the use of intermediary services was to be defined as a breach of the special conditions. The formulation was intended to ensure that the ability to use online-banking software provided by companies that are affiliated with the banking industry in particular was not to be questioned. Footnote 14 states:

"Comment: Prevention of the involvement of intermediaries for security reasons. The formulation no longer precludes the use of online banking software (e.g. StarMoney) if the user enters authentication information while using this software "offline". The term "externally to the bank" in principle allows the user to enter their authentication information on intermediary web pages approved by the bank (option when using FinTS 4.0). However, a separate agreement or notification is required for this purpose." [179]

217. In contrast, the link between the prevention of simple phishing attacks and the subsequent duties of care in the draft special conditions was established through the corresponding comments in footnote 15. The duties of care specify that customers are not permitted to pass on authentication information outside of the online banking procedure. As an example, reference is made to

---

177 [redacted]

178 [redacted]

179 [redacted]

disclosure by email, a classic approach used by phishing fraudsters. The comment in the footnote reads: *"Prevention of "simple" phishing."* [180]

The limitation of intermediary activities and the distinction between the activities of software vendors and providers of payment initiation services were also discussed.

[redacted] proposed wording of the duties of care and handling of PINs and TANs. According to this draft, customers should also be able to enter their PIN and TAN on a locally operated - on the customer's PC - software which uses the interfaces of the German banking industry. .[181] This proposal was [redacted]

The proposal was adopted.

[redacted]

[…] pointed out that the definition of "software" needed to be changed insofar as the reference to the use of the IT systems of the banking industry lying behind the use of software products as well as direct contact with the cu[redacted]vant. For this reason, […] was in favour of a more abstract formulation instead of a reference to software. In its response, it in particular referred to the new discussions subsequently to be anticipated about

[redacted] what was to be specifically understood by the 'use of software', and referred to the solution found against the background of the debate about certification procedures for intermediaries. [redacted]

[redacted].

180 [redacted]

181 [redacted]

[redacted][182]

218. During the first half of 2009, the AK-OBV continued its work on the special conditions and submitted a final version of the revised terms to the associations for consideration. During the meeting of 26.01.2009, the conditions relating to the amendments proposed by the DSGV and the impact of the Payment Services Directive (PSD) were discussed. [183] The wording of the duties of care of customers when using their PIN and TAN was also revised. The provisions still stipulated that personalised security credentials must not be entered outside of the separately agreed web pages (e.g. not on merchant web pages). The explanations in the footnote text regarding the intention of exerting influence on the activities of intermediaries remained unchanged. No further amendments were made to the wording of the duties of care in later meetings. In its meeting on 26.01.2009, the AK-OBV resolved to send the OBC to the decisional bodies of Parties Two - Four for adoption of the resolution within the associations. [184] Following this, the editorial changes were discussed by GBIC on the basis of feedback from the associations, which did not result in any substantial changes to the OBC. The central associations accepted the final versions of the conditions on the dates defined below in more detail (under c.). On 05.08.2009, Party Two - as the last association of the GBIC to pass a resolution within the association - indicated that it intended to adopt the revised OBC and to recommend and submitted them to its members for use. As the GBIC does not act against the interests of its members as a consensually active body, the resolution regarding the version of the OBC contested in the present case was hereby established at the level of the GBIC. Accordingly, GBIC informed the FCO's Decisional Body about the new version of the terms and conditions agreement of the banking industry on 05.08.2009 and submitted the model texts.

---

182 [redacted]

183 [redacted]

184 [redacted]

c) Approval of the model terms and conditions within the individual central associations of the banking industry and adoption by the affiliated credit institutions

219. The Online-Banking-Conditions recommended by GBIC are indeed being used by the credit institutions. GBIC in turn presents the Online-Banking-Conditions as a standardised set of rules of the affiliated credit institutions.[185]

aa) Cooperative banks

220. The BVR participated in the resolution of the GBIC and was involved in, and provided advice on, GBIC's work in internal bodies in accordance with its mandate for a network-wide review of the OBC. The BVR informed the regional associations of the cooperative banking group about the status and results of the work on the terms and conditions and therefore also on the OBC.

221. [redacted][189]

222. In the association circulars from March 2009, June 2009, July 2009 and finally from 05.08.2009, the BVR informed the member banks about the implementation of the customer conditions and their content. [190] At the same time, arrangements were made within the associations to implement the required customer information regarding the

---

185 cf. press release to Stiftung Warentest, paragraph 233et seq.
186 [redacted]
187 [redacted]
188 [redacted]
189 [redacted]
190 [redacted]

pending changes to the terms and conditions , in which the DG Verlag was involved as a central institution in the cooperative sector. [191]

223. From among the cooperative credit institutions organised in the BVR, more than 98%[192] adopted the "Special Conditions for Online Banking" form provided by the DG Verlag in 2012 and used the rules developed by the GBIC towards their own customers.[193]

bb) Savings banks

224. The DSGV organised the work of the GBIC in parallel within its own association bodies and provided advice with regard to the content. [194] In addition to its various specialist departments, the legal departments of the DSGV and of the regional organisations were also involved in the drafting of the OBC. [195] The OBC were discussed several times in a Committee for Legal Affairs. The change requests developed in this context were included in GBIC's considerations.

[redacted]

---

191 [redacted]

192 According to the BVR's own statistics, a total of 1156 cooperative banks were active on 2009, of which 1086 have obtained the form and use it for their customers (http://www.bvr.de/p.nsf/0/F0F8A6D1636D3A1CC1257D0A00540564/$file/3_Entwicklung-seit-1970-2014.pdf), Version 29.05.2015. The number of such institutions which use the OBC was thus more than 93%.

193 [redacted]

194 [redacted]

195 [redacted]

196 [redacted]

197 [redacted]

225. In its meeting of 18.06.2009, the legal committee discussed the draft of the OBC agreed upon within GBIC and granted its approval[198] . [redacted] .[199]

226. The institutions of the savings bank group were informed about the amended OBC in a circular and via "professional announcements for practice"[200] on 13.08.2009.[201] The DSGV developed instructions for the introduction of the new OBC and an implementation guide for the affiliated credit institutions. The DSGV was also active in the area of customer information by developing a customer brochure. [202] The DSGV drew the attention of the affiliated savings banks to the negative effects of the failure to provide customer information and the associated consequence that the existing conditions become invalid and that the content of the customer contracts would be based on the new legal provisions of Sections 675 lit. c-z BGB and 676 lit. a-c BGB, which means that the institutions would not be able to use any deviation options provided by the law. [203]

227. As far as the DSGV is aware, almost all savings banks operating in Germany use the terms and conditions prepared by the GBIC for their customers. According to the DSGV, of the 459 savings banks and state banks operating in 2009, 429 – which is more than 93% of all credit institutions – implemented the amended model terms and conditions, which include the OBC, in their dealings with customers. In addition to individual orders [of the samples], further orders were also placed by buying syndicates, resulting in a practically nationwide use of the OBC in the savings bank sector.

---

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

cc) Member institutions of the BdB

228. Reports on the status of GBIC's work on the terms and conditions were provided to the working groups [redacted].[205] The working group [redacted] took over the legal support of this work. The topic of amending the OBC was discussed in a meeting on 22.08.2007 and subsequently during the meetings which took place in 2008 and 2009 [206] [redacted]

229. [redacted].[207]

230. The Legal Committee of the BdB [redacted] ,formally approved the OBC prepared by the GBIC in its meeting on 25.06.2009.

231. In a circular dated 22.07.2009, the BdB informed its members about the amendments to the terms and conditions previously recommended by the BdB, which was required for the implementation of the new payment service regulations on 31.10.2009 and sent them the amended version of the OBC.[208]

232. The Online-Banking-Conditions are used by the credit institutions organized in the BdB. In any case, the credit institutions of the BdB, such as Deutsche Bank and its subsidiaries, Commerzbank, HypoVereinsbank, ING DiBA and a series of further credit institutions operating in the retail banking sector, all use the rules prepared by the GBIC regarding customers' duties of care.

4. Medial activities of GBIC in connection with the offer of online payment services

233. When speaking to the press, GBIC was critical about Sofort's activities on the market, even after the adoption and introduction of the Online-Banking-Conditions, which included the duties of care for customers - as had been envisaged in the intermediary concept.

---

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

234. Stiftung Warentest asked GBIC for its opinion on Sofort's activities for an article in Finanztest magazine in January 2010. Finanztest was particularly interested in discussing GBIC's opinion of Sofort's services against the background that customers who used the payment initiation service sofortüberweisung.de entered their PIN and TAN on Sofort's web page so that Sofort's software could initiate the transaction.

235. After sending the request to the DSGV as central coordinator of the GBIC in 2010, a first draft reply that had been developed was sent to the managing director of giropay[209], and was then fine-tuned by the specialist bodies of the individual associations with the involvement of the legal departments.[210]

236. In the joint response to the query sent by Stiftung Warentest, GBIC warns against disclosing personalised security credentials to third parties on the internet, referring to the Online-Banking-Conditions of the credit institutions, according to which PINs and TANs must only be entered on the bank or savings bank's web pages. GBIC considered (and still considers) the entry of PINs and TANs on web pages of unapproved payment initiation services such as Sofort to be a breach of the Online-Banking-Conditions. Online banking should not, in the view of GBIC, involve an intermediary payment service gaining access to an account, which GBIC described as *"essentially "phishing""*. On the other hand, it was possible to comply with the duty of confidentiality of the Online-Banking-Conditions if the service provider were to enter into an agreement with the credit institution, as a result of which PINs and TANs could be entered directly on the credit institution's website. GBIC mentions giropay as one such service. From the perspective of GBIC, there was a fundamental risk that the increase in services such as those provided by Sofort could result in customers becoming used to disclosing their confidential banking data. This carelessness could be exploited by criminals in a systematic way. [211]

237. Sofort objected to the wording "essentially "phishing" in connection with the services of sofortüberweisung.de used by the GBIC in its response to the query by Stiftung Warentest, as, from its point of view, this constituted a criminal defamation of the service.[212]As a result, GBIC deleted the addition "essentially

---

209 [redacted]

210 [redacted]

211 [redacted]

212 [redacted]

"phishing" " from the text sent to Stiftung Warentest and added another restrictive amendment relating to the issue of liability in cases of abuse, according to which it is questionable whether the credit institution would pay compensation in cases of abuse, as the customer acted in violation of the terms and conditions. [213]

5. Action taken against online payment services

a) Legal action at the District Court of Cologne

238. On 09.10.2009, giropay GmbH filed a lawsuit at the District Court of Cologne against Sofort, which was operating under the name Payment Network AG at the time, due to a violation of competition pursuant to Section 3, 4 Nos. 1, 9 and 10 of the Unfair Competition Act (UWG) (inducement to breach of contract, unfair non-objective influence, impediment of competition and exploitation of others' performance results).

239. The Federal Cartel Office issued a written statement in these proceedings on 28.02.2011 in accordance with Section 90 para. 2 GWB, which explained the antitrust complaint and the status of the administrative procedure.

240. The District Court of Cologne decided to stay the proceedings between the applicant giropay and the defendant Sofort in a decision of 29.04.2011 until the completion of the antitrust administrative procedure. [214]

b) Further measures

241. Various credit institutions in charge of accounts use the existing provisions of the Online-Banking-Conditions in order to discourage customers from using, or to warn them about, the payment procedure offered by Sofort. For example, the web pages of Sofort are explicitly described as "*incorrect addresses*" where PINs and TANs should not be entered.[215] Banks issue clear warnings about

---

213 [redacted]

214 p. 1576 of the file

215 Letter from attorney Kapellmann dated 24.03..2011, Annex 2, printout of the web page of Raiffeisenbank Oberpfalz Süd eG, Bl. 1454 of the file

the use of "*payment procedures where the access data for online banking [...] are entered on websites which are not operated by the bank*". [216]

242. Bank-independent payment procedures in e-commerce must not only market their business models to merchants but also assure customers that their services are secure. Notifications (e.g. Postbank) that consumers should only trust their bank or savings bank when paying with their PIN and TAN and warnings to consumers that, in addition to the payment procedures in e-commerce offered by banks, "*copycats also offer payments services for online transfers without adhering to the same security standards as the banks and savings banks*",[217] require additional efforts by these types of providers in order to survive amongst the competition.

C. Conduct of proceedings

I. Investigations

1. Investigations into the German banking industry and the various central associations

243. After the objection raised by Sofort on 15.07.2010, the FCO Decision Body opened the antitrust proceedings of its own motion.

244. To clarify the issue, the Decision Body exercised its information rights. In a letter dated 05.10.2010, it asked the GBIC to submit documents regarding the revision of the Special Conditions for Online Banking. On 24.09.2012 the four central associations working together in the area of payments (cf. para 13-17) were additionally asked to explain the procedures used within the associations during the development of the Special Conditions for Online Banking.

245. These central associations working together within GBIC held several meetings with the Decision Body to explain and discuss the facts and the legal situation.

246. During the proceedings, GBIC has sent several briefs outlining the options for the development of a collaboration between payment initiation services

---

[216] Letter from attorney Kapellmann dated 24.03.2011, Annex 2, printout of the web page of Volksbank Freiburg eG, p. 1455 of the file

[217] Letter from attorney Kapellmann of 24.03.2011, Annex 1, printout of the web page of Postbank of 15.03.2011, p. 1444.

and account-servicing credit institutions. None of the proposed models were presented as a commitment to resolve the antitrust concerns. Essentially, the proposals made so far were based on the approval of payment initiation services by the GBIC in connection with the conclusion of bilateral contractual agreements between approved payment initiation services and the credit institutions in charge of the accounts. Another approach proposed was be the creation of an own online banking website, which payment initiation services could use to obtain the information required to operate their business models. In this case, the basic implementation would once again be performed by GBIC.

247. In a letter dated 29.07.2014, the law firm Oppenländer indicated that it would be representing the BVR, the BdB, the VÖB and the DSGV by submitting a power of attorney.[218] Since March 2016, the BdB has been represented by the law firm Dentons Europe LLP.[219]

2. Investigations of third parties

248. Buhl Data Service GmbH, Neunkirchen, was asked to send information about the products it sells on 20.06.2012.

249. The Decision Body obtained information about Datev eG, Nuremberg, about the company's organisation and products related to online banking in a request for information on 17.01.2013 and a subpoena for information on 19.02.2013.

250. Prior to the merger of the cooperative data processing centres Fiducia and GAD, they were individually questioned, along with Finanzinformatik, about the core banking systems and the products they provided in relation to online banking in a subpoena of 11.03.2014.

II. Summoned Parties

251. Sofort requested a third party summons on 16.11.2010. The letter was received by the Federal Cartel Office on 17.11.2010. Parties One - Four and VÖB, which was still involved in the proceedings at this stage, were given the opportunity to comment on the third party summons request in a letter sent to the central coordinator of the GBIC on 23.10.2010. In a letter dated 30.11.2010, the DSGV

---

218 p. 6200 ff.. of the file
219 Letter from the attorney Denton of 04.03.2016.

explained its position and expressed no objection to the third party summons on behalf of GBIC. [220] By decision of 2.11.2010, Sofort was invite to the proceedings as a Summoned Party. [221]

252. giropay GmbH requested a third party summons in a letter dated 10.01.2011.[222] Parties One - Four, the VÖB and Summoned Party Five were each given the opportunity to comment in a letter dated 13.01.2011.[223] In a letter dated 18.01.2011, the BdB explained its position and expressed no objective to the third party summons on behalf of the GBIC.[224] The Summoned Party Five also responded in a letter dated 20.01.2011 and had no serious objections to the summons.[225] BY decision of 27.01.2011, giropay GmbH was invited to the proceedings as a Summoned Party.[226]

III. Inspection of files

253. The Decision Division granted the Parties the right to inspect the case files on 20.06.2011 and 03.05.2012 in letters to the BdB as central coordinator of GBIC, and to the BVR respectively, also as central coordinator of GBIC. To this end, copies of the case files were prepared and sent to the GBIC. [227]

254. The Summoned Parties were also granted access to the files. Copied sections of the case files were sent to Summoned Party Five on 01.07.2011 and 03.05.2012 and to Summoned Party Six on 30.06.2011 and 03.05.2012.

255. After delivery of the draft decision on 23.09.2015, Parties One - Four and the VÖB were granted further access to the case files on 21.12.2015. [228]

IV. Participation and instruction of other authorities

256. On 25.03.2011, the European Commission was informed about the initiation of the proceedings in accordance with Art. 11 para. 3 Reg. No 1/2003. [229] The FCO Decision Body

---

220 Bl. 685 of the file
221 Bl. 694ff.. of the file
222 Bl. 840ff.. of the file
223 Bl. 846 und 848 of the file
224 Bl. 862 of the file
225 Bl. 870ff.. of the file
226 Bl. 919ff.. of the file
227 Bl. 1630 f. of the file and p. 2985f. of the file
228 Bl. 7509 of the file
229 Council Regulation (EC) No. 1/2003 of 16.12.2002 on the implementation of the principles laid down in Articles 81 and 82 of the Treaty competition rules, OJ. No. L 1/1.

discussed the case several times within the scope of the European Competition Network with the European Commission and the national competition authorities represented in this committee.

257. On 10.09.2015 the Federal Cartel Office informed the European Commission in accordance with Art. 11 para. 4 of Regulation 1/2003, as well as the regional anti-trust authority of the state of Berlin, about the intended decision. To this end, the draft decision and a summary of the case were sent to the European Commission and the regional anti-trust authority of Berlin (LKB Berlin).[230] The European Commission commented on this decision during a telephone conference, which was summarised and sent an email on 19.11.2015. LKB Berlin did not express an opinion.

258. During the course of the proceedings, the Decision Body made contact with the Bavarian State Office for Data Protection[231] and discussed the permissibility of Sofort's activities in relation to data protection within this context.[232]

259. Fundamental questions about the permissibility of payment initiation services were also discussed with representatives of the Federal Commissioner for Data Protection,

260. Within the scope of Section 50c para. 2 sentence 1 GWB, the Decision Division exchanged findings relevant to the proceedings with Deutsche Bundesbank, The Federal Ministry of Economics and Technology, the Federal Ministry of Finance and the Federal Financial Supervisory Authority, while preserving the business secrets of the Parties.

V. Granting a fair hearing

261. GBIC submitted a statement regarding the compatibility of the Special Conditions for Online Banking with German and European anti-trust law on 28.07.2014. In the statement, GBIC explains that the OBC were not a resolution passed by an association of undertakings. GBIC also submits there was also no restraint of competition, neither by object or by effect . The intention of the duties of care was not to restrict competition, but to ensure the security of online banking. GBIC maintained the security of online banking was a legitimate purpose and the duties of care were necessary and appropriate in order to achieve this purpose as well as recognised by case law. According t G BIC, this reasoning was supported by the fact that the European Central Bank, BaFin

230 cf. p. 7159 of the file
231 Sofort is domiciled within the jurisdiction of the Bavarian State Office for Data Protection.
232 p. 2991 ff.. of the file, letter of 23.05.2012.

and other national central banks from Europe opposed the disclosure of PINs and TANs. GBIC asserted that the duties of care were a permissible agreement in addition to the agreement regarding the use of online banking. GBIC objected to the view that the joint development of the duties of care in the OBC would foreclose access to the market for payment schemes in e-commerce. And if the agreement of joint duties of care in the OBC constituted a decision by GBIC with a restrictive effect on competition in the market for payments in e-commerce, then this would not fall within the definition in Art. 101 para. 1 TFEU, as this would be a limitation of unlawful competition. Due to the reasons laid out, GBIC came to the conclusion that the Decision Body was not in a position to conclude the proceedings with a decision in accordance with Section 32 GWB. GBIC suggested ending the proceedings without a decision.[233]

262. On 09.23.2015, the Decision Body sent the Parties and the VÖB the draft decision for an opportunity to comment. The deadline for comments on 02.11.2015 was initially extended until 28.12.2015 at the request of the Parties on 13.10.2015. In a letter dated 07.12.2015, a further extension of the deadline for submissions until 22.02.2016 was requested. The Decision Body granted this request. In a letter dated 26.01.2016, the Parties once again requested an extension of the deadline for submissions until 31.03.2016. The Decision Division rejected this request on the grounds that the committee meetings required to prepare submissions, which were cited as the reason for the extension request, could have taken place as much as five months ago, and that, also in light of the pending court proceedings and the transitional provisions of PSD II, the Decision Body would now prepare the decision.

263. The Parties submitted their responses regarding the draft decision on 22.02.2016 and made a general statement with no further details that the Decision Body had not taken their previous legal and factual arguments regarding the admissibility of the Online-Banking-Conditions under antitrust law into account. With regard to their opinion that the duties of care did not aim to cause a restraint of competition

---

[233] cf. p. 6084 ff.. of the file

or result in such restraints of competition, the Parties referred to their submission of 28.07.2014.

264. Previously, Parties had sent a letter dated 02.12.2015 containing a draft public service contract and the draft of an amended version of the Special Conditions for Online Banking in order to bring the proceedings to an end. The Parties distanced themselves from the implementation of these changes in the form of a commitment, which the Decision Body could have declared as binding in accordance with Section 32 GWB; GBIC withdrew the suggestion to remove the limitation, which the Decision Body had considered to be appropriate in principle.

265. In a letter dated 26.02.2016, the VÖB stated that it participated in the preparation of the terms and conditions agreements as a member of GBIC and as an association. However, it only represented credit institutions offering online banking to a limited extent. It did not recommend the use of the OBC to its members at any point. Even in internal working groups, the OBC were only handed out as part of the rules which were developed within the scope of the implementation of the Payment Services Directive.

266. In letters dated 04.03.2016 for the BdB (received on 08.03.2016), as well as for the other Parties (received on 07.03.2016), Parties One - Four requested the suspension of the immediate enforcement of the decision by way of precaution.

267. In a letter dated 07.06.2016 and supplementary email dated 15.06.2016, the Decision Body informed the Parties and Summoned Parties that it was also considering basing the decree on Section 19 para. 3 GWB, if the circumstances remained unchanged. The Parties in the proceedings were granted until 21.06.2016 to file submissions in this regard.

268. In letters dated 10.06.2016 and 20.06.2016, the law firm Oppenländer[234] on behalf of Parties One – Three, and the law firm Detons[235] for Party Four, did not comment on the content, but criticised the vague wording of the abuse allegation. In its submission of 04.03.2016, Dentons also requested the suspension of the immediate enforcement of the decision.

---

234 cf. p. 7621 et seq. and 7625 et seq. of the file
235 cf. p. 7619 et seq. and 7629 et seq. of the file

D. Legal analysis

269. The decision by GBIC to create uniform Special Conditions for Online Banking, and the decisions of Parties Two - Four concerning the group-wide harmonised use of the OBC by their group members, both violate Art. 101 para. 1 TFEU, Section 1 ff.. GWB, to the extent that they, as resolutions of an association of undertakings that coordinate market behaviour, impose duties of care on customers that prevent the forwarding personalised security credentials to payment initiation services in e-commerce, e.g. via online merchants' web pages, in accordance with 7.2 para. 1 in conjunction with para. 2, third bullet point OBC, para. 10.2.1 para. 5, bullet point OBC.[236] The implementation of the underlying economic master plan to prevent the activities of payment initiation services by establishing legal barriers to market entry, also represents - even in the case of a hypothetical admissibility of the coordination – an unfair impediment of other companies, and therefore constitutes an abuse within the meaning of Section 19 paragraph 3 sentence 1 in conjunction with para. 1, para. 2 no. 1 GWB.

270. The OBC decided by GBIC, and the decisions of Parties Two - Four to recommend the use of the OBC by its members in their contractual relationship with their customers, both are embedded in a strategic and conceptual consideration of GBIC for handling payment schemes in e-commerce. The competing credit institutions coordinate their market behaviour, and hinder the activities of bank-independent payment initiation services, via their central associations. The overall plan is based on the decades-old practice to conclude joint terms and conditions , which had been adapted over time in accordance with identified current requirements. Within this context, GBIC defines what must be considered a threat or a risk (e.g. risks resulting from internet browsers, payment initiation services), and then creates corresponding provisions that, on the one hand, address these security concerns, and that on the other hand create a competitive situation beneficial for its member associations and their affiliated credit institutions. The overall plan of the banking industry, represented by GBIC, includes the development of a strategic concept for dealing with payment initiation services

---

[236] The term 'customer' refers to the contractual relationship with a credit institution in charge of an account. The term 'user' in the Online-Banking-Conditions of the banking industry is not used in a differentiated way for reasons of simplicity and due to the fact that this differentiation is not relevant to the antitrust complaint.

(intermediaries concept). Once agreed, the central associations recommended the OBC to their members for use. These recommendations have been implemented on a broad basis. On the basis of these standardised provisions and based on the communication strategies developed within the GBIC, credit institutions warned customers not to use payment initiation services. And on the basis of the agreed OBC, GBIC discussed the alleged illegality of using bank-independent payment initiation services with the press. The cases being considered by the courts due to an alleged inducement of the customers to breach their agreements, or the alleged confusion of consumers by offering bank-independent payment initiation services that are being classified as illegal, also resulted from this overall plan of GBIC. The liability provisions corresponding with the duty of care are formulated in the OBC in such a way that it is not immediately clear to customers using a payment initiation services, under which conditions such use might result in negative consequences regarding their legal liability.

271. The adopted Online-Banking-Conditions of the banking industry contain various duties of care that must be observed by customers. As the antitrust complaint refers only to some of these duties of care, the other provisions will not be considered in the present legal assessment. Paragraph 7.2 para. 1 in conjunction with para. 2, third bullet point OBC, para. 10.2.1 para. 5, fourth bullet point, however, breach Article. 101 para. 1 TFEU, Section 1 et seq. GWB, to the extent that the prohibition of entering personalised security credentials outside of separately specified online banking access channels applies to all providers that allow purchasers of goods or services in e-commerce to rely on their online banking (so-called payment initiation services).

272. The antitrust judgment was made on the basis of Art. 101 para. 1 TFEU, according to which all agreements between companies, decisions by associations of undertakings and coordinated practices are prohibited, if they could potentially affect trade between Member States, and if they result in the prevention, restraint or distortion of competition within the single market or are intended to have such consequences. The assessment on the basis of Section 1 ff.. GWB, according to which agreements between undertakings, decisions by associations of undertakings and coordinated practices which result in the prevention, restraint or distortion of competition within the single market, or are intended to have such consequences, does not lead to a different conclusion.

273. The decision by GBIC, and the decisions of Parties Two - Four (cf. I), have as their object to exclude bank-independent payment initiation services from being competitors on the market for online payments in e-commerce (cf. B.II.3). They do not represent an ancillary agreement to a main agreement that is otherwise permissible under antitrust law. Neither are they exempted from the prohibition of restrictive practices based on Art. 101 para. 3 TFEU (cf. IV). The Parties did not demonstrate any efficiency gains achieved through the adopted clauses. And in any event, the Parties failed to sufficiently demonstrate that the restrictions of competition were indispensable in order to achieve the alleged efficiency gains. The alternatives discussed by the Parties with the Decision Body for dealing with payment initiation services on the market for payment schemes in e-commerce in fact demonstrated that there were specific opportunities to deal with such service providers, which both would guarantee security and at the same time restrict competition to a lesser extent.

274. The overall plan of Parties One - Four, which contains the unlawful decisions of the GBIC and Parties Two - Four as a building block for the implementation of the overall concept to hinder payment initiation services, also represents an unfair impediment of another company within the meaning of Section 19 para. 3 sentence 1 in conjunction with Section 19 para. 1, para. 2 no. 1 GWB (cf. V).

I. Decision by an association of undertakings

275. The standardised creation and application of the duties of care formulated in the Online-Banking-Conditions (Section 7.2 para. 1 in conjunction with para. 2, third bullet point, para. 10.2.1 para. 5, fourth bullet point) is based on resolutions by associations of undertakings within the meaning of Art. 101 para. 1 TFEU.

1. GBIC and the central associations of the banking industry are associations of undertakings

276. GBIC is an association of undertakings. The central associations of the GBIC act as associations of their economically active members, who, if not directly, are indirectly related to credit institutions and therefore constitute companies within the meaning of competition law.

277. Neither European nor German antitrust law have particularly high requirements for the organisational form of an association of undertakings. The association must have a degree of communal organisation, without the need for a specific legal form.[237]

It does not matter whether the association of undertakings is a company itself. The decisive factor is that its members themselves are directly or indirectly companies. Associations, whose members are associations of companies themselves, are included in this definition.[238] The term 'association of undertakings' is not primarily orientated towards the organisational and legal form of an association, but is to be considered against the background of the area of expansion and application of the ban on cartels. Art. 101 para. 1 TFEU applies to associations of undertakings whose activities or whose affiliated companies' activities aim to achieve situations that the ban on cartels aims to stop. [239]

278. GBIC, as a civil law company, is an association of undertakings which acts in the interests of its members and has a high degree of community organisation. GBIC pursues the goal of forming shared opinions and intentions on behalf of the associations within the banking industry in Germany with regard to banking law, banking policy and practical banking issues. It represents the common positions of the central associations when dealing with legislators, government authorities and banking and financial institutions at national, European and international level.[240] Common positions are developed between the central associations of the banking industry in the responsible committees of the GBIC, e.g. in the working groups, for the achievement of common objectives.

279. The members of GBIC include the central associations of the German banking industry, which are also associations of undertakings. The members of the central associations represented by GBIC are companies within the meaning of antitrust law. Both the BVR and the BdB are active in the area of representing the interests of their members, which are credit institutions. In the case of the BVR, these are the cooperative banks. [241] The BdB also directly represents the interests of its member banks. The regional associations are

---

[237] Zimmer in: Immenga/Mestmäcker, Wettbewerbsrecht, Vol. 2 GWB, Part 1, 5th edition, Section 1, paragraph 76.

[238] Hengst in: Langen/Bunte, Kartellrecht Kommentar, Vol. 2, Europäisches Kartellrecht, 12th Ed., Art. 101 TFEU, paragraph 68; public bodies can also be associations of undertakings if, in addition to their public legitimacy, they intervene in the competition of their members among each other or in connection with third parties.

[239] ECJ, judgement of 08.11.1983, C-96/82, IAZ, paragraph 20.

[240] http://www.die-deutsche-kreditwirtschaft.de/dk/die-deutsche-kreditwirtschaft.html,Version 16.12.2014.

[241] http://www.bvr.de/Wer_wir_sind/Unsere_Aufgaben,Version 15.12.2014.

also members of the BdB. [242] The DSGV indirectly represents the interests of savings banks operating regionally. Its immediate members are the regional associations of the savings bank system, which are public bodies. The savings banks and their municipal guarantors have compulsory memberships [243] in the respective regional associations. The regional associations represent the interests of the savings banks at the regional level when dealing with regional governments and regional authorities. [244]

280. The individual credit institutions of all of the organisations involved are undertakings within the meaning of Art. 101 para. 1 TFEU. They provide fee-based banking services and are therefore economically active.

2. The common Online-Banking-Conditions were created and implemented by passing resolutions

281. The Online-Banking-Conditions were agreed through decisions made by associations of undertakings. This applies both to the decision at the level of the GBIC and to the implementation of decisions in the respective central associations (Parties Two - Four), which also includes the recommendation to use the OBC circulated to the respective member institutions.

282. Decisions are defined as all legal acts that associations of undertakings use to formulate their position, irrespective of how the decision was made. In this regard, no distinction is made as to whether, for instance, there were internal rules regarding the passing of resolutions and whether all members of the association of undertakings took part in the decisions which aimed to create a situation that the prohibition of restrictions of competition aims to prevent.[245] The actual degree of liability, e.g. whether non-compliance by the member companies is associated with sanctions, is also irrelevant to the assessment under cartel law. In order to establish the existence of a decision, it is sufficient that there is a sincere intention of the association of undertakings to

---

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

243 Only free savings banks become members of the respective regional association on a voluntary basis. (http://www.dsgv.de/de/sparkassen-finanzgruppe/organisation/verbaende.html,Version 15.12.2014).

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

245 BGH, 14.08.2008, "Lottoblock", quoted from juris, paragraph 21 with further references to the case law of the European courts.

coordinate its members' behaviour in the market. [246]

The Parties argue, with reference to the case law of the German Federal High Court of Justice, that the recommendation of terms and conditions by an association alone is not sufficient to presume the intention to coordinate. [247] However, a recommendation made by an association of undertakings does in fact fall within the scope of antitrust law, if this recommendation, as is the case here, is accepted and adopted by the members.[248] According to the outcome of the investigation, this was not merely a recommendation by the GBIC (cf. a)), because the central associations developed the terms and conditions in accordance with their mandates, and the credit institutions accepted and applied the Online-Banking-Conditions in the revised form (see b)).

a) Not a mere recommendation by GBIC

283. The Online banking conditions developed by GBIC and its central associations do not represent a mere recommendation for credit institutions. The Online-Banking-Conditions were developed with the aim of achieving standard use in practice by the credit institutions tht are members of the associations on as broad a basis as possible. The same is also reflected by the manner in which GBIC presents itself to third parties.

284. When drafting the duties of care, GBIC pursued the aim of creating a harmonised standard for dealing with payment initiation services for the entire banking industry. GBIC considered it necessary to revise the duties of care on the basis of the observation that individual credit institutions decided to *independently develop* the duties of care in their Online-Banking-Conditions in this regard in mid-2005 as a result of criminal phishing attacks on online banking.[249] There was also general agreement within GBIC regarding a harmonised implementation of the requirements from the Payment Services Directive into the terms and conditions agreement.

285. Online banking regulations have always been developed jointly within the GBIC as an industry standard. As explained by GBIC, security issues are a central

---

246 Krauß in: Langen/Bunte, Section 1 GWB, paragraph 86, with further references to national and European law.

247 BGH, decision of 22.03.1994, KVR 23/93.

248 ECJ, judgment of 08.11.1983, C-96/82, cited by Juris, paragraph 20 et seq.; Krauss in: Langen / Bunte, Section 1 GWB, paragraph 86.

249 Letter from the GBIC, 02.11.2010, p. 484 of the file

aspect of online banking. To the extent that technical security is questionable in individual cases, GBIC assumes that this would completely destroy the trust of bank customers. GBIC therefore considers it essential to pursue high standards of security in order to avoid a loss of confidence among customers in online banking for all credit institutions that would result form security issues with one individual credit institution in the framework of its online banking.[250]

286. The work performed on the Online-Banking-Conditions in the various working groups of GBIC continued for several years, during which feedback was continuously provided by the individual central associations of GBIC to the affiliated institutes regarding the results (cf. para 197ff.). Due to the mandate of the central associations, which is derived from the statutory tasks or corresponding committee resolutions for the development of the conditions, the individual institutes were not expected to develop their own Online-Banking-Conditions, and indeed did not do so(see para 284).

287. Contrary to the view of the Parties, according to which the model conditions allowed individual banks to determine which websites they "*accept as an access channel to online banking in the security policy*",[251] the OBC aim to form the basis for a harmonised application by all credit institutions. This is evident from the specific objective of the associations participating in the development of the Online-Banking-Conditions in the GBIC (cf. para 284) and the division of responsibilities when organising online banking, which specifically precludes individual authorisation of individual services by individual banks. It would be contradictory to the rationale of the participants to develop standardised agreements for the entire banking industry and design the framework conditions for online banking and take over responsibility for the (continued) development of security procedures, if individual credit institutions were as a rule required to autonomously decide which websites they approved as being sufficiently secure for entering PINs and TANs. The participants have taken action on behalf of the affiliated credit institutions precisely because of the fact that issues in connection with online banking are particularly complex, and have created a framework within which online banking is to operate.

---

250 Letter by GBIC, 02.11.2010, p. 478 of the file
251 Letter by Oppenländer lawyers, 29.07.2014, p. 6151 of the file

288. Many of the affiliated credit institutions also lack the resources and expertise required for an approval process to assess the security of web pages and payment initiation services. This is also evident by the fact that savings banks and cooperative banks, in addition to various BdB banks, need to use the external data processing centres of the respective banking group (cf. 106et seq.), which offer a complete technical service package for banking operations, for the technical realisation of their online banking services. These institutions cannot, in fact, make such decisions themselves, and they are only in a position to make decisions about the security of services in the area of online banking via their data processing centres which were, therefore, represented in the relevant working groups of the GBIC during the formulation of the duties of care.

289. The fact that, from the point of view of GBIC, the Online-Banking-Conditions which were effective until 2009 were an industry standard and therefore represented far more than a mere recommendation, is also clear from the way GBIC approached the Online-Banking-Conditions when dealing with third parties. GBIC referred L'Tur, which introduced a payment initiation service that required entry of the customer's PIN and TAN and therefore online banking access, to the Online-Banking-Conditions used in the German banking sector, which impose the standardized obligation onbanking customers to ensure that no other individuals gain access to their PIN and TAN (cf. para 174).[252] GBIC did not, however, inform L'Tur that the conditions were a mere "sample" developed by the associations, which is actually only used by some credit institutions in this form, so that credit institutions could in fact authorise L'Tur's activities. In fact, GBIC performs its function as a representative of the interests of the German credit institutions in such a way that it becomes clear to outsiders that GBIC is referring to a decision that generally applies nationwide and that GBIC also intends to enforce. This shows that the duties of care are in fact an industry standard and that GBIC is representing the interests of all affiliated credit institutions on this basis.[253]

---

[252] [redacted]

[253] The GBIC also informed Moneyshelf AG, which is part of Deutsche Bank, that the products offered by the bank would result in customers being misled into breaching the duties of care formulated in the Online-Banking-Conditions 2000 by passing on the PIN and TAN, which they are required to keep confidential, to Moneyshelf and Deutsche Bank AG (cf. paragraph 175,). Again, there was no limitation in that ca[redacted]s of those credit institutions that actually use the Online-Banking-Conditions prepared by GBIC. GBIC also referred

290. GBIC also describes the product sofortueberweisung.de without limitations as a breach of contractual specifications, namely the obligation of the customer to keep their PIN and TAN confidential. GBIC clarified to the operator of the system, which was known as Promido Internet GmbH at the time, that the concerns regarding sofortueberweisung.de were shared by all associations represented within GBIC.[254] No differentiation was made between credit institutions that used such conditions and those that used different conditions.

291. Ultimately, the communication between GBIC and external third parties demonstrates that the participants assumed there was a uniform application of the Online-Banking-Conditions, also after the development of the Online-Banking-Conditions in 2009. As GBIC stated to Stiftung Warentest in 2010, credit institutions' conditions for online banking envisage a standardised approach to PINs and TANs. In this regard, GBIC asserted the following:

"However, if the access data to be kept confidential are entered on the web page of an online payment process, which has not been approved by the customer's credit institution (e.g. Sofortüberweisung.de), the customer will thereby breach the Online-Banking-Conditions."[255]

292. Finally, the action by giropay GmbH at the District Court of Cologne also demonstrates that it is generally known in banking circles that the Online-Banking-Conditions represent an industry standard. giropay, which initiated proceedings against Sofort at the District Court of Cologne with reference to the duties of care in the Online-Banking-Conditions, based its action on the fact that Sofort's activities represented an incentive to breach a contract, as customers would violate their duties of care formulated in the Online-Banking-Conditions.[256] The fact that individual credit institutions could choose to use different rules was not mentioned at all.

T-Online International AG to the generally established duties of care of online banking customers, which prohibited the use of the services offered by T-Online (cf. paragraph 176,). GBIC consi[redacted] and to represent an encouragement for online banking customers to breach their contracts.

254 [redacted]

255 [redacted]

256 A[redacted]on 08.10.2009, p. 18

b) Adoption and implementation of the Online-Banking-Conditions by credit institutions

The member institutions of Parties Two – Four, cooperating within GBIC, implemented the Online-Banking-Conditions through their own resolutions which, in turn, do not represent mere recommendations. As shown above (see. para. 219 ff..), the Online-Banking-Conditions apply in all areas for savings banks and cooperative banks within the scope of the business relationships with customers. Even among private banks, the largest member institutes (e.g. Deutsche Bank, Commerzbank, HypoVereinsbank, ING DiBa) have all adopted the online banking conditions and corresponding duties of care and displayed them on their websites.

II. Restraint of competition

293. The duties of care developed by the GBIC and used by the affiliated credit institutions represent a coordination on the market for personal current accounts, the objective and effect of which is the restraint of competition in the national market for online payments in e-commerce. They prevent customers from entering personalised security credentials when using bank-independent payment initiation services. This is therefore a restraint of competition in a third-party market (market for online payments on the internet). Such third-market restrictions are also included in the ban on cartels (Article 101 TFEU and Section 1 GWB). The jointly-established duties of care have the potential to affect trade between Member States.

1. The relevant product market

294. The relevant market (market-relevant assessment), the factual boundaries of which have to be established first, forms the basis for the competitive assessment. The starting point for defining this market's boundaries is the demand market concept. According to this concept, all products that are so similar in terms of their characteristics, their economic purpose and price range that a reasonable consumer would consider them to be suitable for a specific purpose, justifiably compares them with each other and considers these products to be exchangeable

form a single objective market.[257] The actual action taken by the customer is decisive, whereby this must be based on a reasonable average consumer.[258] Exchangeability assumed by only a few consumers is not sufficient.[259]

295. The coordination of the behaviour of the central associations of the GBIC by creating a standard definition of duties of care in the OBC affects the relationship between the providers of current accounts compatible with online banking with their customers and therefore the current account market, which is not to be defined in any narrower sense in these proceedings. The coordination aimed to limit competition on the market for online payments on the internet. In this market, providers of secure online payment in e-commerce are in competition with one another along with merchants who sell their goods or services on the internet and therefore require the purchase price payments to be settled using secure payment procedures.

296. All of the procedures that merchants use to not only settle payments but also for additional services, such as for protection against bad debts, are to be attributed to this market for online payments.[261] On the other hand, payment procedures in which the merchant limits itself to using payment options available outside of e-commerce, such as debit or credit transfer schemes, that do not involve the services of a provider, are not part of this market.

a) Framework conditions for payment procedures in e-commerce

297. In addition to physical retail and distance selling, e-commerce has established itself as an additional distribution channel with high growth rates in recent years. In e-commerce, where the customer and merchant only meet in person or have contact by telephone in exceptional cases

---

257 Established case law, cf. Federal High Court of Justice, decision of 05.10.2004, WRP 2004, 1502, 1504 – Staubsaugerbeutelmarkt; Federal High Court of Justice, judgement of 19.03.1996, WuW/E BGH 3058, 3062 – Pay-TV- Durchleitung.

258 Established case law, cf. only Federal High Court of Justice, decision of 22.09.1987, WuW/E BGH 2433, 2436 – Gruner+Jahr/ Zeit; KG, decision of 14.04.1978, WuW/E OLG 1983, 1984 with further references – Rama-Mädchen; Paschke in: Frankfurter Kommentar, Kartellrecht, IV §§ 1-23 GWB, Section 19, paragraph 74.

259 Established case law, cf. KG, decision of 19.03.1975, WuW/E OLG 1599, 1602 – Vitamin B 12; KG, decision of 05.01.1976, WuW/E OLG 1645, 1649 – Valium; Paschke in: Frankfurter Kommentar, l.c., Section 19 paragraph 75. For this legal concept in common law, see the case law in Fardell v. Potts in A.P. Herbert, Uncommon Law, 3rd Edition, 1980, page 7, 8 ff..

260 The market therefore does not include the contractual relationship between the merchant who sells goods on the internet and the customer who selects a payment method to pay the invoice amount.

261 For example, a merchant can commission a service provider to issue the invoice and deal with the payment management and collection in the event of payment problems. Such services are part of the market, but the use of credit transfer or direct debit schemes, if necessary supplemented by services provided **within** the company to reduce the risk of default, should not be included.

and where the concurrent fulfilment of the contractual obligations cannot usually be achieved when purchasing goods, the payment procedure is of particular importance from the point of view of the merchant.

298. The main risk when concluding a contract of sale in e-commerce for both the customer and merchant is the non-fulfilment of the main obligations by the contractual partners. The main obligations are the delivery of the goods by the seller and payment by the buyer. As no physical meeting typically takes place between the contractual partners in e-commerce, it is not possible for the buyer and seller to directly fulfil the contractual obligations in the same way as in retail stores. In e-commerce, each of the parties need to provide advance performance, either by sending the goods or paying the purchase price.

299. The risks of e-commerce for customers can be reduced by using internet shops which they are familiar with or which have a quality seal or by using payment procedures which provide buyer protection, through which a conditional refund is made under some circumstances in the event of non-delivery. The merchant can also reduce the risk that the customer will not pay for the received goods by integrating suitable payment procedures. The extent to which merchants consider explicit guarantees or less formal assurances regarding the execution of the order to be sufficient depends on their respective risk assessments and risk preferences.

b) Typification of payment methods in e-commerce

300. A variety of payment options are offered for e-commerce which are based on conventional payment methods as used in retail stores or have been adopted from distance selling (cf. c) aa)). The methods developed specifically for e-commerce include those which are processed through the customer's online banking (cf. c) bb)), as well as methods where customers manage their own accounts which handle the payments (cf. c) cc)).[262]

---

[262] The depiction of the payment procedures used in e-commerce is orientated towards the Online Payment Study 2014, Daten, Fakten, Hintergründe und Entwicklungen, EHI Retail Institute e.V., Cologne, p. 101 et seq. p. 6336 ff.. of the file. In addition to these methods, there are also additional payment methods in each category. Furthermore, there are additional variants such as

301. Merchants can choose from a range of different payment procedures in e-commerce. Merchants usually offer their customers several different payment procedures. If customers know or use payment procedures, this can contribute to an increase in the conversion rate[263] within the shop.

302. The most widely used instrument to settle cashless payments in retail stores in Germany, the **girocard**, has so far not been available to merchants and customers, as it can only be used with terminals approved by the German banking industry.[264] For reasons of practicality, **cash payments** in the form of the handing over of legal tender is generally unavailable due to the lack of physical contact between the contractual parties.[265]

c) Payment methods in e-commerce are a separate product market

303. Conventional payment procedures where the payments are processed by a third-party service provider (payment by invoice, payment in advance or direct debit) can be attributed to the market for online payments in e-commerce. Instalment agreements and payment on delivery, which are standard in the case of distance selling, also belong to this market. Payment processing through the use of credit cards is also part of the objectively relevant market. Furthermore, payment procedures developed for e-commerce that are managed by service providers whose products are offered in conjunction with the use of online-compatible current accounts (giropay, sofortueberweisung.de, Paydirekt) or through service providers who manage their own accounts for payers and settle the invoice amounts using these accounts (PayPal, Click&Buy, Scrill), are also part of this market. There are also payment options such as the use of

---

mobile payments by phone or using vouchers, which are conceivable, but less widespread alternatives.

263 Conversion of a buying interest into an order during the use of online shops.

264 International schemes issue debit cards that can also be used from a distance. The only prerequisite is that they are equipped with a Primary Account Number (PAN). This is currently not the case for debit cards issued in Germany. Maestro (MasterCard) and V-PAY (Visa) are only used as a cobrand on a girocard.

265 The situation is different if merchants operate a physical store in addition to their internet shop and offer collection and payment of the goods from this store. In such cases, the buyer can also pay in cash or using a debit card in exceptional cases. According to an investigation of the 1000 largest online shops in Germany, more than half operate at least one physical store in addition to e-commerce (cf. Der E-Commerce- MarktDeutschland 2014, Weitere Vertriebskanäle von Online-Shops, Fig. 4, p. 12, issued by EHI Retail Institute e. V. and Statista GmbH 2014).

mobile devices which have hitherto only played a minor role in practice.

aa) Usability of payment procedures from conventional distance trade and physical stores

304. Traditional payment procedures used in distance trade include payment on **account**, **payment in advance,** collection of the receivables by **direct debit** and payment as **cash on delivery**. **Credit cards** are widely accepted in physical retail stores. The use of **partial payment agreements** also comes into consideration for the payment of goods.

305. Such conventional payment alternatives should only be attributed to the market for online payments in e-commerce if merchants do not organise the settlement internally and use specialised service providers.

(1) Transfer (purchase on account, in advance) and direct debit

306. In the case of **purchases on account**, the merchant sends the goods along with an invoice, which the buyer usually settles by submitting a transfer instruction to his or her bank. The seller can specify a due date for payment. If the seller wants to minimise the risk of payment receipt, they can request purchase on account in the form of **payment in advance**. When purchasing on account, the customer transfers the invoice amount to the merchant's account. In order to use this payment procedure, the merchant only needs a current account in order to accept the payments. Both payment types transfer the risks of the fulfilment of all obligations of the purchase agreement parties unilaterally, either at the expense of the buyer or the merchant: in the case of advance payment, there is no risk of default for the merchant, while the merchant is required to accept the full risks in the case of payment on account. In the case of advance payment, the buyer bears the risk of non-delivery of the goods, while they are completely protected from this risk in the case of purchase on account.

307. The payment of the purchase price can also be made by direct debit. In this case, the merchant requests the collection of the receivables due from the buyer's account after the direct debit order has been made. Payment by **direct debit** is also a procedure which was developed long before the existence of e-commerce. The buyer needs to do no more than issue a direct debit mandate and transfer the corresponding account data to the merchant in order to pay the purchase price. The merchant uses the data to generate a direct debit which it submits to its bank for collection. The bank credits, subject to receipt, the direct debit amount to the merchant's account and collects the direct debit amount from the customer's bank,

which debits the account of the payer. When using the direct debit procedure, the risk of default lies with the merchant, as it is risking that a redeemed direct debit could subsequently be returned by the customer or that the payer's bank rejects the redemption due to insufficient funds and the debit is charged back to the merchant.

308. To the extent that merchants are unable to sufficiently assess disadvantages with regard to the default risk of their contractual partners in the case of payment on account on the basis of their own available information when using conventional payment procedures in e-commerce, providers are active on the market who offer to assess the default risk of the customer and the settlement of payments for a fee. The companies operating in the market offering these services do not only offer the settlement of purchases on account. In some cases, their range of services also includes settlement via direct debit or hire purchase. These offers therefore result in the transfer of the risk management and administrative activities to the external service providers in exchange for a fee.

309. Typically, service providers offer to take over and settle the payment process in connection with factoring models. In factoring, a service provider acquires the claim against the customer[266] and pays the invoice amount less a discount to the merchant. While the merchant receives the liquidity, the financial service provider takes over the collection of the payment or debts in the case of payment failure. Merchants who do not want their customers to be in contact with a service provider have the option of choosing so-called "white label solutions", where the service providers' offers are integrated into the internet shop and perform the settlement in the name of the merchant (cf. paragraph 326).[267]

310. The merchant can either integrate such offers into their internet shop as a brand of the corresponding service provider or use them for support during their own settlement of the payment procedure. RatePAY GmbH[268], Berlin, offers merchants both invoicing with payment guarantee and direct debit settlement with risk assessment or payment in instalments within the scope of the payment procedure. [269] According to the

---

[266] Depending on the factoring model, the receivables can also only be taken over by the service provider when the due date for payment has passed and the customer is therefore in default (maturity factoring).

[267] EHI Retail Institute e.V., Online-Payment-Studie 2014, Daten, Fakten, Hintergründe und Entwicklungen, p. 101 et seq., p. 6364 et seq. of the file

[268] RatePay GmbH is a company in the Otto Group.

[269] https://www.ratepay.com/produkte, Version 16.03.2015.

market studies of EHI Retail Institute, the most well-known methods in Germany are Billpay[270], Klarna[271] and Paymorrow[272].

(2) Partial payment agreements

311. The conclusion of a **credit agreement** to finance the purchase price also represents an alternative payment procedure. The purchase price is credited to the merchant by a credit institution, which concludes a credit agreement with the customer. In doing so, the customer undertakes to repay the credit amount, including interest, either in instalments or on an agreed date in the future.

(3) Cash on delivery

312. Another common procedure in distance selling is shipping with payment by **cash on delivery**: In this case, the merchant sends the goods via a parcel service, which takes over the delivery and accepts the payment in order to pass it on to the merchant. Payment in the form of cash on delivery removes the main risks of performance for both the merchant and the customer, as the parcel service replaces the physical meeting of the merchant and customer and ensures that the goods are handed over in return for payment of the purchase price. The parcel service provider receives a fee for this service.[273]

(4) Credit card payments

313. Credit card payments are another payment instrument which was developed before e-commerce existed and which is also attributable to the market. The

---

[270] BillPay was founded in 2009 and is based in Berlin. According to the company, it currently has 115 members of staff and offers its services in more than 4,000 online shops. BillPay offers its services in Germany, Austria, Switzerland and the Netherlands. Since 2013, the company has been owned by the Wonga Group, a British online financial services provider based in London.

[271] Klarna, the parent company of Sofort, was founded in Sweden in 2005 and offers purchases on account and purchases in instalments in e-commerce as payment methods. Various financial investors have holdings in Klarna. In addition to Sweden, Klarna also operates in Denmark, Norway, Finland, Germany, the Netherlands and the United Kingdom. The company employs more than 1200 people. According to the company, more than 50,000 merchants use Klarna's services.

[272] Paymorrow was founded in 2008 and has been providing secure purchase on account services in e-commerce ever since, mainly to small and medium-sized merchants in Germany. According to the company, more than 2,000 merchants use Paymorrow's services. Inter Card AG, Taufkirchen, (a network operator) has held a majority stake in the company since 2013. In addition to secure purchases on account, Paymorrow also provides direct debit services.

[273] Traditionally, customers pay in cash when using this type of payment, although more recently, delivery services have also started to accept card payments.

the vast majority of all credit card transactions in Germany are processed in so-called four-party systems, in which the merchant commissions a service provider, the acquirer, to settle the credit card payments.[274] On the basis of the acceptance agreement, the merchant is given the opportunity to accept credit card payments. In the case of credit card payments, a differentiation should be made between the authorisation of a payment and the clearing and settlement of credit card transactions. If a merchant's customer initiates a payment transaction using a credit card, the merchant submits an authorisation request with the corresponding data (amount, card number, validity period of the card etc.) to the acquirer, if necessary with the involvement of additional technical service providers. The acquirer passes this on to the bank which issued the card via the international authorisation networks of the credit card organisations.[275] In the case of a positive authorisation of the payment transaction, the acquirer then approves the payment for the merchant. However, the merchant is not protected from chargebacks, which can occur if the credit card holder reports the misuse of their credit card data and objects to the charge.

314. The credit institution which issues the card receives a fee from the acquirer in MasterCard and Visa's major credit card systems. This interchange fee represents a significant source of revenue for banks. According to investigations by the Decision Division, the card-issuing banks generated € 350 million from the interchange fees of the five largest acquirers in 2009 (only transactions within Germany).[276] From 09.12.2015, the Interchange Fee Regulation[277] limited the level of the interchange fees for consumer credit cards to 0.3% of the respective sale.

315. Credit card payments on the internet are associated with higher risks than credit card payments in retail stores, as no check is performed to confirm whether the customer is the actual owner of the relevant credit card due to a lack of physical contact between the merchant and customer. A signature verification is also not possible

---

[274] The other two parties in such systems are the cardholder and the issuing bank.

[275] In Germany, this authorisation "online for issuer" is the standard, to the best of the Federal Cartel Office's knowledge.

[276] The Federal Cartel Office currently estimates that at least 20% of these revenues are attributable to transactions in e-commerce.

[277] Regulation (EU) 2015/751 of the European Parliament and of the Council of 04.29.2015 on interchange fees for card-based payment transactions, Official Journal of the European Union, L 213/1 of 19.5.2015.

in these cases. For these reasons, acquirers and credit card companies regularly establish special duties of care for merchants with regard to the use of credit cards for distance selling, including e-commerce, and in some cases take further measures to limit risks. [278] In addition to MasterCard and VISA, other credit cards which are less common in Germany can also be used in e-commerce as a payment alternative. These include, for example, American Express, Diners Club and JCB.

bb) Payment procedures in e-commerce with settlement via online banking

316. Various procedures have been established in e-commerce which are used to pay the invoice amount by gaining access to the customer's online banking account. The customer is sent to the web page of the respective payment procedure from the merchant's web page, from where the payment procedure is initiated. As this procedure initiates the payment of the invoice amount via the customer's account, this is also described as a payment initiation service.

317. The **giropay** procedure offered by companies in the banking industry, the Paydirect procedure and the bank-independent procedure **sofortüberweisung.de** offered by Sofort are all based on access to the online banking account and the issuing of transfer instructions. The customer can issue a transfer instruction for the purchase price to their credit institution in charge of the account. The merchant then receives direct feedback from the respective system operator stating whether this transfer instruction will be accepted and executed by the bank in charge of the account. As in the case of payments in advance, the buyer transfers the purchase amount to the merchant before delivery. The merchant does not need to wait until receipt of the purchase amount upon delivery for assurance that the contractual partner will fulfil their obligations arising from the purchase agreement and instead immediately receives a notification about the execution of the transfer in the online banking procedure. This faster processing makes this procedure much more attractive for both parties than

---

[278] The credit card organisations aim to increase the security of credit card payments in order to make credit card payments more attractive. Examples of this include the "MasterCard SecureCode process" from MasterCard and the "Verified by Visa" process from Visa, where customers are asked to enter specific security credentials which only they know in order to initiate the payment.

payment in in advance with delivery only after receipt of the purchase amount in the merchant's bank account.[279]

318. With giropay, a procedure offered by the banking industry, the merchant receives an unconditional guarantee of payment from the credit institutions that have entered into a corresponding agreement with giropay. Customers of credit institutions with no contractual links with giropay cannot use this process.

319. Sofort does not provide merchants with a guarantee in the sense used by the banking industry and instead gains access to the account with the agreement of the account holder and passes on the customer's transfer instructions to the credit institution. If the transfer is executed, the merchant will receive a confirmation that the transfer has been submitted and sufficient funds were available.[280] The submission and execution confirmation provided to the merchant is not a guarantee in the legal sense.

cc) Payment methods in which customers manage their own accounts for settlement

320. A further option for the settlement of payment processes in e-commerce is the use of payment methods in which customers maintain their own account – usually in addition to their current account – which is used to settle invoices.

321. The most well-known method of this type is **PayPal**. However, services such as **Scrill**, a payment alternative used in Germany for e-commerce by merchants as a payment procedure, which functions as an e-wallet, are based on the same principles. The customer opens an account with PayPal or Scrill in order to use this payment method. They enter account details or credit card data for this account, which will then be used to transfer funds by direct debit or in a credit card transaction to the account of the respective payment procedure. The transfer of funds using processes such as giropay or

---

[279] For the classification of these procedures as variants of payment in advance, cf. Stahl, Krabichler, Breitschaft, Wittmann, E-Commerce-Leitfaden, 2nd revised and extended edition, Regensburg 2009, updated on 14.10.2010, ibi research 2009 (www.ecommerce-leitfaden.de), p. 114 (Annex XXVII, Chapter 4).

[280] The system checks the existing funds in the account in various ways. In the case of banks whose systems display all relevant transactions in real time, the level of the available funds is checked. In the case of credit institutions whose systems do not always display the current account balance, the system checks the available funds on the basis of the displayed bank balance, taking pending payments into account. In the latter case, the system also checks the successful posting of business transactions between the customer and sofortüberweising.de within the last 30 days.

sofortüberweisung.de is also possible in some cases. If the customer chooses this type of payment method in the online shop, they will be sent to the web page of the payment procedure, where they enter the access data for the payment procedure and transfer the invoice amount to the seller's account. The invoice amount is either debited to the credit balance of the payment procedure's account or withdrawn from the client's bank account or credit card in an additional step. The invoice amount is credited to the merchant, who also has an account for the payment procedure.

dd) Other payment methods in e-commerce

322. In addition to the methods mentioned above, there are other less common options, e.g. mobile payments or payment with prepaid cards, although these play a minor role at most in the market.

ee) Summary

323. The objective market for online payments in e-commerce includes conventional processes settled through a service provider, such as payments on account, advance payments, direct debit, cash on delivery, instalment agreements and credit card payments. Furthermore, special payment methods settled through service providers whose products are offered with the use of online-compatible current accounts of the payer (giropay, sofortueberweisung.de, Paydirekt) or through service providers who manage their own accounts for payers and settle the invoice amounts using these accounts (PayPal, Click&Buy, Scrill) can also be attributed to this market.

d) Distribution of the payment methods in e-commerce

324. There are significant differences between the described payment methods in e-commerce in terms of their use by internet merchants. The payment methods used in retail stores and in distance selling are also very widely used by internet merchants. According to estimates by the EHI Retail Institute, they represent one of the major groups in the top 1,000 online internet stores that are used by more than 80% of the retailers surveyed. VISA and MasterCard credit cards in particular achieve a high prevalence rate in e-commerce, each offered by around 80% of the shops as a payment method. Other credit cards such as American Express, Diners Club and JCB have a significantly lower distribution.

325. Due to the major significance of PayPal, e-wallet solutions also achieve a high prevalence rate among internet merchants in Germany at over 80%. The

other methods in this group are used by less than 10% of merchants

326. The high distribution of accounting service providers is also significantly lower than 10%. According to estimations by the EHI, white label solutions are offered by just under 40% of merchants, i.e. services by providers who do not operate under their own name, so customers are not aware that the merchant deals with the payments itself (see paragraph 309).

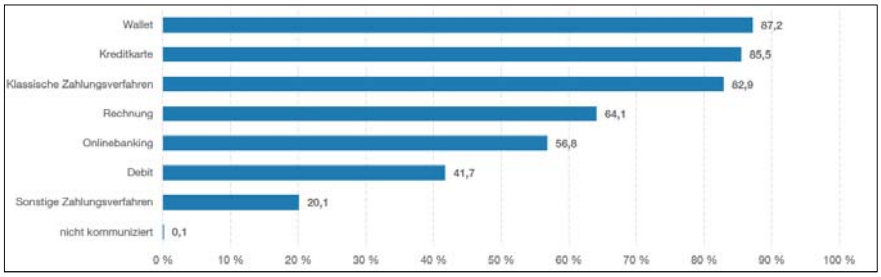

Fig. 6 - Payment methods in e-commerce 2014 [281]

327. In the field of "online banking", soforteuberweisung.de and giropay are substantially represented on the market as payment initiation services. At around 50%, Sofort's bank-independent procedure has a significantly higher penetration than giropay, which is offered by less than 10% of merchants[282]. There are major differences here, even when measured on the basis of growth rates. Although giropay was offered by fewer than 10% of merchants in the first EHI study in 2012 and was only able to increase its prevalence rate to an insignificant extent, the use of sofortueberweisung.de in e-commerce increased markedly, despite the measures introduced by the GBIC. While only 36% of merchants offered this payment method in 2011, this figure was at around 50% in 2012.

328. Deutsche Bundesbank also investigated payment behaviour in a study and came to the conclusion that there were significant differences between the payments for goods and services in retail stores and in e-commerce.

---

[281] Der E-Commerce-Markt Deutschland 2014, issued by EHI Retail Institute e. V. and Statista GmbH 2014, In Onlineshops angebotene Zahlungsverfahren, Fig. 26, p. 42.

[282] The mentioned figures relate to the merchants' offer and as such do not allow any references back to the degree of actual use by customers.

329. The Bundesbank notes in its study on "Payment Behaviour in Germany 2014"[283] that innovation in payments assumes that they are associated with an advantage compared to established procedures and that special attention needs to be given to security. The fulfilment of these conditions consequently results in steady but slow changes, which is particularly evident in the area of payment procedures in e-commerce.[284]

330. The payment behaviour of customers in e-commerce is significantly different to that in distance selling and retail stores. Nearly 85% of all transactions[285] in e-commerce are performed using internet payment procedures,[286] transfers and credit cards. The use of cash in e-commerce plays no role. In contrast, most transactions in retail stores are performed using cash or payment with a current account card.[287]

331. The results of the Bundesbank study demonstrate that e-commerce is a constantly growing market segment which customers are using more and more frequently. While the proportion of respondents who shopped online was at 42% in 2008, this figure had increased to 57% by 2011 and was at 63% by 2014.[288]

332. The study conducted by the Bundesbank shows that those who have stated that they shop online usually use transfers (56%) to pay for the goods and services, followed by internet payment methods (55%) and payment by direct debit (25%).

---

283 Deutsche Bundesbank. 2015. Payment behaviour in Germany in 2014. Third study of the utilisation of cash and cashless payment instruments, Frankfurt, 2015.
284 Ibid p. 6 et seq.
285 41.1% of the transactions are internet payment methods, 23% are transfers, 17.7% are credit card payments and 3.7% are performed using a current account card.
286 This includes payments which are made using PayPal, Sofortüberweisung.de and giropay.
287 Deutsche Bundesbank, Payment Behaviour in Germany 2014, Fig. 16 (use of payment instruments by payment and purpose), p. 63.
288 Ibid. p. 70 et seq.

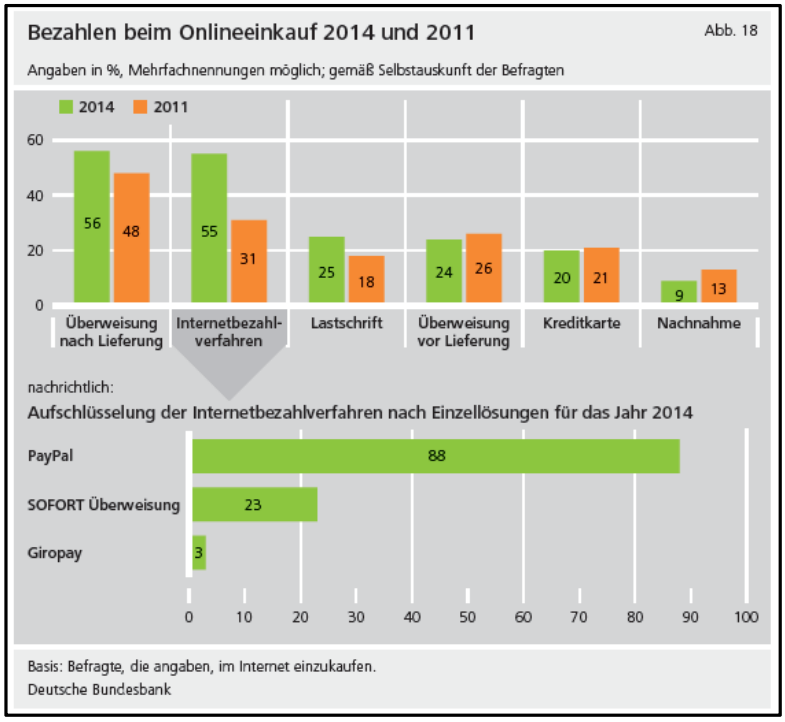

Fig. 7 - Bundesbank Study, Payment Behaviour in Germany in 2014, p.73

333. Other payment methods mentioned include transfer before delivery of the goods (24%), the use of credit cards (20%) and cash on delivery (9%). While the use of cash on delivery, credit cards and transfers before delivery of the goods or provision of the services has declined in comparison to the second study in 2011, the most frequently-used payment methods (transfers, internet payment procedures and direct debit) have increased during the comparison period. The use of internet payment procedures was only mentioned by 31% of the respondents as an alternative used in 2011, whereby this figure has now risen to 55% in 2014.

334. With regard to internet payment methods, PayPal is a particularly focus in the Bundesbank results. 88% of the respondents have used this payment method. In contrast, Sofortüberweisung achieved a share of 23%, while giropay was used by only 3% of respondents.

2. The regionally relevant product market

335. The market for online payments in e-commerce covers the entire territory of Germany, but does not currently go beyond this region for the forecast period relevant for this process, even though various payment methods are also offered in other Member States of the European Union. Demand preference and the particular importance of international payment methods vary considerably in the various European countries.

336. The geographic market also needs to be defined on the basis of economic criteria. In principle, the determination of the regionally relevant market follows the same criteria as the objectively relevant market, i.e. according to the functional exchangeability from the point of view of the consumer.[289] It includes all areas where the relevant product is regularly sold and in demand, with homogenous competition conditions and neighbouring areas which have noticeably different competition conditions.

337. The payment methods can be used nationwide at the very least in the market for online payments in e-commerce. However, a further regional market delimitation beyond Germany is not currently expected and is also not expected during the forecast period. User behaviour in Austria and Switzerland is significantly different to the behaviour in Germany.[290]

338. Although some providers of methods such as PayPal and credit card payments are currently also active in other Member States, this is not relevant to many other companies which offer innovative new payment methods. However, their area of activity is limited to individual Member States. For instance, Sofort offers its payment initiation services in fewer than half of the Member States of the European Union (cf. paragraph 21). giropay is also only directly available in Germany. One reason for the restraint to individual Member States is that, from the operators' point of view, the system is based on agreements with credit institutions which are connected using the interfaces developed and operated by the GBIC. An extension of activities to credit institutions in other Member States has therefore not yet taken place. Without access to bank customers of a Member State, the use of giropay would only be possible for merchants who wanted to reach German customers in cross-border trade. On the basis of a cooperation with

---

[289] Established case law; cf. Federal High Court of Justice, decision of 19.12.1995, WuW/E BGH 3037 - Raiffeisen.

[290] EPSM Market Research Newsletter 03-04/16, p. 3 et seq., p. 5.

the Austrian system eps, the payment procedure was only able to extend its reach to a small extent. Currently, however, it does not appear that European-wide activity can be accomplished within the forecast period.

339. Other methods, such as eps and iDEAL, are only available in Austria and the Netherlands (market leader here at 56%), but not in the rest of Europe. Its field of activity mainly aims to provide consumers with Austrian or Dutch current accounts with payment options.

340. The payment procedure Trustly, which was previously only available in Scandinavian countries, Estonia, Poland, Spain and Italy, has not achieved any significant market position outside of its traditional areas of activity, even after expanding its activities to the rest of Europe in 2016. In France, the national payment procedure Cartes Bancaires (CB) also dominates as a payment method in e-commerce (80%). Merchants who want to be successful in e-commerce therefore need to be able to (still continue to for the moment) offer national payment procedures.

341. Whether and how quickly the harmonisation of the European payment processing area (SEPA: Single European Payment Area) and the capping of fees for credit card payments will lead to a convergence of a standardised internal market in which payment procedures in e-commerce are also marketed across Europe for domestic transactions is currently unclear, which is why the Decision Division still assumes that payment procedures in e-commerce will continue to operate within national markets.

3. The decisions aim to restrict competition

342. The online banking conditions adopted by the GBIC and Parties Two - Four aim to restrict competition within the meaning of Article 101 para. 1 TFEU and Section 1 GWB to the extent that the duties of care regarding the use of PINs and TANs included in these conditions excludes the use of bank-independent payment initiation services.

343. A restraint of competition exists when the restraint is by nature likely to restrict competition. These are restraints that have such a high potential for negative effects on competition that proof of their actual impact on the market is not

required. [291] In the case of an intentional restriction of competition, the enforcement of the ban on cartels is not dependent on the combined market share of the competitors taking part in the restraint. [292] When assessing the purpose of an agreement or a decision, it depends on the content of the restraint of competition (see under a)), the aims to be achieved (see under b)) and the economic and legal context (see under c)). In the latter case, the type of goods and services affected by the restraint, the existing actual conditions and the structure of the market are also to be taken into account. Even if the intention of the participants is not a necessary element of the assessment of the purpose of an agreement, this can be used in the assessment (see under d)).[293] Within the scope of this assessment, it does not matter if the parties pursue other permissible purposes in addition to the restraint of competition.

a) Content of the decisions contrary to cartel law

344. The actual wording of the duties of care being discussed here is directed against the use of PINs and TANs by payment initiation services in e-commerce. This results in a restraint of competition from bank-independent payment initiation services which have no contractual connection to the credit institutions offering online banking compared to credit cards and the payment initiation services marketed by the banks which are in competition with these services.

345. The wording of these terms and condition clauses aim to restrict the activities of payment initiation services by actually preventing their use by customers. As customers are required by the Online-Banking-Conditions to keep personalised security credentials confidential and only use the online banking access channels specified by the bank when issuing instructions,

---

[291] Commission Notice, Guidelines on the Application of Article 81 paragraph 3 of the EC Treaty (2004/C 101/08), OJ of 27.04.2004, no. C 101, p 97, para. 21; also Notice on agreements of minor importance which do not restrict competition within the meaning of Article 101, paragraph 1 of the Treaty on the Functioning of the European Union to a noticeable extent (de minimis notice) 2014/C 291/01,), para. 2.

[292] Notification of the Commission, Notice on agreements of minor importance which do not restrict competition within the meaning of Article 101, paragraph 1 of the Treaty on the Functioning of the European Union to a noticeable extent (de minimis notice), Official Register of the European Union, 2014/C 291/01 of 30.08.2014, paragraph 2.

[293] European Court, judgment of 11.09. 2014 in case C-67/13 P, Groupement des cartes bancaires (CB)/Commission, cited by curia.europa.eu, paragraph 53 et seq.

[294] ECJ, judgment of 20.11.2008 in Case C-209/07 BIDS, paragraph 21 with further references, quoted from juris.

these provisions restrict the competition of the various payment systems with regard to internet merchants. The web pages which have no agreement with credit institutions in charge of the accounts and online merchant websites are expressly and exclusively listed as an example of a use of PINs and TANs excluded by the duties of care and as prohibited options.

346. By referring to "entry on online merchant webpages" in the duties of care, providers of bank-independent payment initiation services are specifically excluded. As the services provided by bank-independent payment initiation services are offered on the basis of agreements with merchants and the payment initiation services are performed by making a connection between the webpage of the merchant with the payment initiation services, this duty of care formulated in the OBC aims to prevent the use of payment initiation services by Internet merchants and consumers.

347. The wording of the duties of care alone includes products with comparable risks which are not, from the perspective of the GBIC, potential competitive products to payment procedures linked to the GBIC, namely giropay, Paydirekt and credit cards. As the reach of giropay only relates to banks who have concluded a contract with giropay, this payment initiation service is not covered by this provision, even though the merchant also passes the customer on to the payment service in this case.

b) Objectives pursued by the restraint of competition

348. The objective of the GBIC when prohibiting the entry of personalised security credentials on online merchant websites is not to ensure that the PINs and TANs are only entered on channels which are fully controlled by the banks themselves or to minimise potential risks arising from the entry of PIN and TAN on paths which are secured by third party service providers: the OBC provision prevents the use of procedures which are operated on the basis of Java applications from being made subject to the approval of the credit institution. Such products, which are operated on the basis of Java applications, cannot be controlled by credit institutions with regard to their security and, to this extent, pose potential security risks. The avoidance of habituation to the input of PIN and TAN on third-party websites is not sufficiently ensured by the provisions of this duty of care.

349. The OBC as a whole represents a standardised form of the online banking agreement between customer and bank and form a framework in which the contractual parties use or provide the services. The essential content of the provisions represent, among other things, security issues and the distribution of liability between the provider and user of the online banking services.

350. The wording of the duties of care creates the basis for a distribution of the liability between the bank and the user, among other things in the event of potential financial damages resulting in misconduct by the user.

351. The GBIC's objective in developing the duties of care was, however, not a systematic and comprehensive security concept to prevent abuse. In fact, the provision stating that PIN and TAN should not be entered on the websites of online merchants is mainly aimed at creating a clear differentiation between bank-independent payment initiation services and other intermediaries, including the bank's own products e.g. account information and payment initiation services, but also products provided by third parties where customers enter their PIN and TAN to initiate transfer instructions, although these take place within the scope of the individual customer’s use of the online banking account (software operated on the customer's device) with no connection to an online merchant.

352. The specific rules for entering PIN and TAN only on the websites agreed between the customer and bank leads to the establishment of industry standards which the customer cannot avoid, regardless of their choice of credit institution. As an industry standard, customers cannot choose between banks with a restrictive access policy and those with pro-competitive provisions.

353. The GBIC and Parties Two - Four refer to the specific entry of PIN and TAN for third parties on the internet in the contested decisions regarding the duties of care. The way the GBIC uses the term web pages does not in any way aim to prohibit the entry of PIN and TAN on the internet in general - outside of the website of the bank in charge of the account. Services like StarMoney and Starmoney.Web (see para. 116 et seq.) are examples of account information services which can also be used to send instructions to the credit institution in charge of the account on the internet, which are not subject to any restraint of use according to the duties of care. StarMoney, a product developed by Finanzinformatik

(savings bank group) which is compatible with multiple banks, constitutes a third-party product that, at least for the credit institutions of the BdB and BVR, has a technical design which cannot be controlled. No credit institution can verify which account data is saved and processed on the servers of Finanzinformatik or its subsidiaries and how the entry of PIN and TAN for third parties is secured. It is obvious to the user that they are entering their PIN and TAN on a third-party website rather than exclusively on web pages or within the scope of products which their credit institution in charge of the account has approved itself for this purpose.

354. The assertion of the GBIC that the customer would "get used" to passing on personalised security credentials is therefore not stringent.

355. The GBIC has considered and accepted the fact that customers would not exclusively use their PIN and TAN in communication with the credit institution in charge of the account when developing the online banking system: the duties of care were not intended to question, among other things, the option of entering PIN and TAN within the scope of the use of financial management software such as Finanzinformatik's Starmoney service and comparable non-banking products if they use the GBIC interface. The customer would also "get used" to not using their PIN and TAN exclusively within the scope of communication with their credit institution. The fact that such products also require the entry of a PIN and TAN and then pass these on via the internet to the credit institution in charge of the account (in order to gain access to the account and retrieve data or issue instructions) is not considered by GBIC to be a security risk of online banking which need to be countered with specific duties of care of the customer or security requirements for these products. GBIC's internal documents in fact indicate that they wanted to word the duties of care in such a way that these instructions would not be hindered by individual banking groups. [295] If software components such as JAVA applications are used for these products to create encrypted communication with the credit institution in charge of the account, the GBIC considers this an appropriate technical solution and as

---

[295] In the footnote relating to the customer's duties of care, according to which authentication information cannot be entered on web pages which are not part of the credit institution (e.g. merchant websites), (draft of the Online-Banking-Conditions dated 16.04.2008) states that the formulation no longer excludes the use of online banking software (e.g. Starmoney), for which the user enters the authentication information offline.

satisfies their security requirements. In fact, they are accepting greater risks with these products than in the case of payment initiation services, as such Java applications are not reviewed and approved by the GBIC or their commissioned bodies and are programmed by the service producers themselves, with no acceptance of the products by the GBIC.[296] It is not taken into consideration that programming such a Java application or local software installed on the customer's computer, which uses the GBIC interfaces to transfer the PIN and TAN to the credit institution, can also result in an unapproved passing on of the data to a third party on the internet.[297] The fact that such risks are not recognisable to the customers when using the corresponding products, as customers are unable to determine the type of programming used in the financial management software and Java applications, is also not a problem for the GBIC. With regard to practical application, the GBIC in fact refers the product kontoblick.de[298], of all things, which provided access to customers' account details via a Java application, saved the customer data on the company's server, prepared it graphically for the customers and finally used it in an anonymous form for market research purposes, until the company withdrew from the market due to bankruptcy.[299] Such services do not, however, guarantee that PINs and TANs are protected from unwanted misuse when using the product.

356. Instead, the Parties have created an impermissible connection between the service offered by a bank-independent payment method in e-commerce active on the market and the risks of online banking with regard to criminal activities by claiming that the OBC in the contested form was to be regarded as a reaction to increasing risks to online banking from criminal attacks.

357. The GBIC expressly specifies that the entry of PINs and TANs is prohibited in relation to online merchant websites. In connection with online retailers, the disclosure of PIN and TAN relates only to payment processes and therefore to the use of payment initiation services. In addition to the bank-independent payment initiation services, no use in connection with online merchants is evident where the entry of

---

296 Letter from the GBIC dated 09.08.2011, p. 1706 of the file
297 cf. description of GBIC's dealings with Buhl Data products, paragraph 134 et seq.
298 cf. paragraph 161 cf.
299 Letter from the GBIC dated 09.08.2011, p. 1709 et seq. of the file

PINs and TANs is required and their use is expressly defined as being subject to approval in the wording of the special conditions.

358. A standardised and stringent security concept would require the establishment of comprehensive regulations for dealing with service providers, which would result in either an authorisation of service providers on the basis of reasonable provisions which are applicable to all or the formulation of suitable and abstract security criteria. The intermediary concept in which such considerations have been made was not developed into a comprehensive and practical security concept. The work on this concept was halted within the working groups of the GBIC after it became more difficult to deal with bank-independent payment initiation services, while the formulation of the OBC otherwise allowed the continued use of bank-related services.

c) The economic and legal context of the duties of care

359. When assessing the question of whether a coordination between companies is, by its very nature, harmful to the functioning of competition, relevant aspects relating to the economic or legal context in which this coordination is embedded in are to be taken into account. These include the nature of the services in question, the structure of the market and the conditions in this market.[300]

360. In addition to the content of the duties of care, the actual market conditions are evidence that the duties of care aim to restrict competition on the market for online payments in e-commerce.

aa) Existing legal framework when developing the duties of care

361. The activities of payment initiation services were not subject to any legal restraints when the duties of care were decided upon and adopted in 2009. At this time, payment initiation services were not subject to any state supervision for payment services. The banking industry has used the legal freedom to develop duties of care in order to exclude competitors from the market.

---

300 European Court, judgment of 11.09. 2014 in the case C-67/13 P, Groupement des cartes bancaires (CB)/Commission, cited by curia.europa.eu, paragraph 53 et seq.

362. When drafting the special conditions, there were no mandatory legal provisions applicable to the provision of payment initiation services at that point in time. The national legal regulations provided the credit institutions with leeway to create their own general terms and conditions regarding the secure use of personalised security credentials. In this context, legal regulations and their leeway to be developed do not mention any different treatment of services depending on whether they are offered by banks, are bank-related or provided by bank-independent service providers. In any case, existing payment initiation services were permitted to continue to operate following the entry into force of the PSD2. However, they were restricted by the contested wording of the OBC.

363. The adopted duties of care in the OBC only refer to bank-independent payment initiation services, but not those which have a contractual agreement with the banks. To the extent that the GBIC refers to the legal framework conditions changed by the implementation of the PSD,[301] which necessitated an amendment of the Online-Banking-Conditions, they had broad discretion when developing the issues not conclusively regulated by the legislators.

364. The legal provisions of Section 675l para. 1 BGB stipulate that customers need to protect personalised security credentials from unauthorised access, but do not specify what "unauthorised" actually refers to. However, as the use of a PIN and TAN has effects on the distribution of liability between the credit institution and customer (Section 675v para. 1 BGB), the credit institutions are required to enter into an agreement with their customers to determine how a payment authentication tool is to be kept secure (Art. 248 section 4 para. 1 no. 5 a EGBGB as implementation of Art. 42 no. 5a PSD). When specifying the obligations of the customer, the legislator took into account that the obligations of the customer could not be conclusively legally defined and that some of the obligations would be stipulated in the contractual agreement between the customer and the credit institution, as only the credit institution would be able to duly take the special features of the use of PIN and TAN into account. In this respect, the legislator only required that customers must be provided with information about how to keep personalised security credentials secure. No content requirements for the banking industry were associated with this.

---

[301] Letter by Oppenländer lawyers dated 29.07.2014, p. 609 et seq. of the file

365. Statutory regulations which need to be specified in more detail or leeway in the implementation of the legal requirements in general terms and conditions are to be interpreted and developed in compliance with antitrust law. The specific design of the duties of care by those involved, on the other hand, reflected the intention of the GBIC and its members to drive bank-independent payment initiation services from the online payment market in e-commerce.

366. The GBIC cannot rely on the fact that by developing these provisions, the agreement relevant to antitrust law would protect other legal values, such as data protection or copyright issues.[302] Insofar as these and other legal areas are significant for the activities of a payment initiation service, the authorities and courts are responsible for monitoring adherence to statutory requirements and this does not justify any antitrust agreements between private companies or associations of undertakings.[303]

367. The legal framework has not changed during the process: the earlier applicable directives and regulations relating to payment services were modified in 2015 and supplemented by a new directive. No later than following the implementation of the PSD2 revised by European legislators in 2018, all leeway for the German banking industry to restrict payment initiation services active on the market will be lost.

368. PSD2 includes new regulations regarding the supervision of payment services. Significant changes have been made to the assessment of new types of payment services, which will be subject to supervision in the future. The Member States have two years, i.e. until 13.01.2018, to make the required adjustments to national legislation in order to apply the new rules.

369. The provisions of PSD2 will not be directly enforceable until the end of the transposition deadline, as they also need to be transposed into national law by the German legislator. However, the new Directive will have an advance effect which is linked to the clearly formulated aims and the operating procedures for Member State authorities specified in recital 33 of PSD2

---

302 Letter by Letter by Oppenländer lawyers, 29.07.2014, p. 6190 ff.. of the file

303 Judgment of the European Court of First Instance in Case C-68/12 of 02.07.2013, Slovenska sporitel, paragraph 20, (cited in: http://curia.europa.eu).

when making the future decision about approving payment initiation services.[304]

370. The declared objective of the PSD2 is to ensure continuity in the market until the Directive is implemented into national law while at the same time providing existing service providers with the option of offering their services within a clear and harmonised legal framework, irrespective of their business model. Notwithstanding the need to address the security of payment transactions and consumer protection to protect them against the demonstrable risk of fraud, the Member States, Commission, European Central Bank and the European Supervisory Authority (EBA) should secure fair competition on the market until the application of those rules, that is, until their transposition into national law. In doing so, unjustified discrimination against the existing market participants should be avoided.[305]

371. The (national) administration obligations arising from the principle of effectiveness (effet utile) of Article 4 TFEU in relation to the procedure proposed by the union[306] therefore demands that the national antitrust authorities take the regulatory objectives of PSD2 into consideration when applying the European and national competition laws. This means that the Federal Cartel Office, as a national competition authority, is not permitted to make or fail to make any decisions which would put the purpose of this Directive at risk, to the extent this is permissible according to the national law (no advance effect contra legem). Any unjustifiable discrimination against payment initiation services through an order issued by the cartel authorities or by the failure of the cartel authorities to intervene should therefore be avoided.

372. Such discrimination would result from the fact that the duties of care for online banking agreed by the banking associations would still prohibit the passing on of PINs and TANs on online merchant websites. As a result of the existing regulations, there is at least a certain degree of uncertainty for the user of the services as to whether this use is illegal. Discrimination of players on the market is also associated with the fact that existing provisions can be used as a basis for lawsuits against payment initiation services.

---

304 For the advance effect of directives, see:.. Grabitz / Help / Nettesheim, Nettesheim, The Law of the European Union, Volume 3, Article 288 RN 118.

305 Recital no. 33 and Art. 115 para. 6 PSD2.

306 cf. Grabitz / Help / Nettesheim, von Bogdandy / Schill, The Law of the European Union, Volume 3, Article 4 RN 90.

373. Based on the scope of PSD2, these discriminatory provisions in the special conditions must therefore be put an end to by the German supervisory authorities.

bb) Actual conditions on the market and the structure of the market

374. The actual market conditions also demonstrate that the design of the duties of care aimed to directly restrict competition on the market for online payments. The regulations relate to innovative, growing competitors in the market where credit institutions have so far largely only been able to generate revenue through the use of credit cards, the undiminished realisation of which has been put in doubt by the emergence of this new competition.

375. PayPal and credit cards are currently the most widely spread options among the payment methods in e-commerce, with only minor differences between the credit card systems of VISA and MasterCard. Only two other methods attributable to the market achieve a prevalence rate of more than 50%, i.e. they are offered by more than half of retailers. These include payment on delivery and the payment initiation service Sofort. All other methods, in particular the giropay method offered by the banking industry, have so far achieved much lower prevalence rates.[307] It is currently difficult to assess the extent to which the new payment method Paydirekt will achieve a stronger market penetration due to the fact it has only recently been launched on the market.

376. The services offered by payment initiation services are a response to online merchants' need for an inexpensive, secure and simple payment method. Online merchants each offer several payment procedure options. The merchant, who incurs costs for the use and settlement of a purchase within the scope of a payment method, has limited influence over the customer's choice of payment method. However, the merchant can influence the selection of the method by, for instance, charging different amounts for shipping and many do in fact do this in order to limit their costs associated with the payment procedure or at least partially refinance them.

---

307 E-commerce market Germany 2014, market study of the 1,000 B2C online shops for physical goods with the highest sales, EHI Retail Institute, Cologne, p. 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

Fig. 8 - Results of the EHI Retail Institute study on the average cost of payment methods in e-commerce, e-commerce market in Germany 2014

377. In addition to PayPal, financing and the use of service providers for the settlement of invoice purchasing, credit cards are currently by far the most expensive payment method for online merchants. The acceptance of giropay is associated with significantly higher costs for the merchant than the use of payments using methods such as the one offered by Sofort.

378. Card-issuing credit institutions generate revenues from the interchange fee to be paid by the merchants when credit cards are used, which have a market share of around 15%, according to the findings of the EHI Retail Institute. In contrast, the credit institutions do not receive any proceeds from the use of bank-independent payment initiation services.

379. The increased popularity of payment initiation services and the control options of the merchants as shown in paragraph 376 represent a risk of lost revenue for the banking industry from their original products.[308] To the extent that services are offered by the bank-independent payment initiation services, they benefit from the readiness of the merchant to offer products which are cheaper for the merchant compared to PayPal and credit cards and point their customers in the direction of cheaper payment procedures within the scope of their options.

---

[308] When the regulation on interchange fees for card-based payment transactions comes into effect, the upper limit for interchange fees for credit card payments will be 0.3% of sales.

380. The prohibition of the use of payment initiation services without the approval of the respective credit institution in charge of the account therefore in particular protects the revenue interests of the credit institutions affiliated with the central associations in their dealings with bank-independent service providers. Such an approach to the design of the contested duties of care in the OBC was considered necessary from the point of view of the GBIC in order to restrict the spread and economic success of methods which had not already been forced out of the market on the basis of bilateral "discussions" (cf. paragraph 289ff.).

381. To the extent that the GBIC has made concrete proposals for dealing with intermediaries who offer services associated with online banking in addition to the development of the Online-Banking-Conditions, these proposals also focus on the question of [redacted].[309] This illustrates that the generation or preservation of sources of income plays a central role when assessing the activities of intermediaries.

382. The strategy of preventing the activities of bank-independent payment initiation services is therefore also to be assessed in the light of the income directly accrued by the credit institutions from the settlement of payments in e-commerce via bank-supported payment transactions.

d) The intention of the Parties to exclude existing payment procedures in e-commerce from the market

383. By designing the duties of care, the GBIC continued its action against bank-independent payment initiation services whose systems involves the use of account information of the customers and in this context the entry of PINs and TANs on online merchants' web pages. The development of online banking conditions is to be assessed in the light of the approach taken by the GBIC against payment procedures on the basis of the previous terms and conditions regulations. The correspondence with L'Tur, T-Online and Promido shown above are evidence[310] that the main intention of the GBIC was to suppress the services of bank-independent payment initiation services on the market for online payments in e-commerce on the basis of the existing terms and conditions regulations across the entire sector. Also

---

309 [redacted]

310 cf. paragraph 173 et seq.

in their dealings with Stiftung Warentest, Sofort's activities were described as a breach of the existing duties of care on the basis of the newly adopted new Online-Banking-Conditions (cf. paragraph 233et seq.).

384. When considering the risk and the possible dealings of the GBIC with service providers who gain knowledge of PINs and TANs (intermediaries), the GBIC is in favour of finding solutions at a business and legal level, e.g. the introduction of its own banking industry payment method in e-commerce or corresponding duties of care in the customer conditions. The aim was to prevent PINs and TANs from being entered on intermediary web pages under any circumstances (see paragraph 194).

385. By prohibiting the entry of PINs and TANs on websites other than those separately approved, the GBIC creates a legal basis for its efforts to prevent the activities of bank-independent payment initiation services on the market for online payments in e-commerce, which it had been pursuing for some time, without simultaneously preventing the use of those products originating from the banking sector.[311] In the corresponding working group, reference was in particular made to discussions already held with Sofort and the aim of formulating the duties of care in such a way that they would not lead to any new discussions with payment initiation service providers[312] or discussions with the Federal Cartel Office about the restraint of compeititon.[313]

---

311 cf. paragraph 214ff..
312 cf. paragraph 217.
313 [redacted]

4. The decisions result in the restraint of competition

386. The specific design of the duties of care in the OBC do, in any case, result in a restraint of competition.

387. The examination of the effect of the decision has been made in the alternative. To the extent that a provision which restricts the activities of payment initiation services on the market represents a restraint of competition by its very nature, the applicability of Art. 101 para. 1 TFEU and Section GWB is not dependent on the result of an assessment of its effectiveness. The purpose and effect of an agreement are alternative to each other and do not need to be cumulatively fulfilled.[314]

388. The effect of an agreement must be based on the existing economic, legal and actual market and competitive conditions, whereby the type of agreement, the actual implementation in practice and market power of the market are relevant.[315]

389. The impact on the competitive position of third parties on the market is sufficient to establish the restraint of competition caused by a decision, whereby the effect must be causally attributed to the decision.[316]

390. The banks use their position as providers of current accounts in a targeted way in order to create collective provisions for the use of the current accounts in online banking procedures in order to force bank-independent providers of payment initiation services out of the market. The restrictive effect on competition in the markets for online payments results from the sector-wide standardised approach to the design, implementation and enforcement of the regulations.

391. The associations working together in the GBIC represent all credit institutions operating in Germany. Their activity leads to nationwide effects on the market for online payments in e-commerce. The OBC developed by the GBIC and its central associations, which essentially rules out the activities of payment initiation services, are used by almost all credit institutions.[317] In total, more than 56 million current accounts with online access were held at German

---

[314] Cf. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Vol. 2 Europäisches Kartellrecht, 12th Ed., Article 101 TFEU, paragraph 218 et seq.
[315] Cf. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Vol. 2 Europäisches Kartellrecht, 12th Ed., Article 101 TFEU, paragraph 233.
[316] Cf. Hengst in: Langen/Bunte, Kartellrecht Kommentar, Vol. 2 Europäisches Kartellrecht, 12th Ed., Article 101 TFEU, paragraph 234.
[317] Cf. paragraph 219ff..

credit institutions in 2014.[318] As a result of the existing duties of care in the Online-Banking-Conditions, this market potential was removed from the competition of payment initiation services or made the successful expansion and growth of payment initiation services significantly more difficult.

392. With regard to the use of bank-independent payment initiation services, the GBIC established a legal provision in such a way that customers were unable to use these services without breaching what were, from their point of view, applicable contractual provisions. The duties of care aim to make it possible to legally sanction the services of bank-independent payment initiation services as illegal services, as presented by Summoned Party Six in the statement of grounds for the action before the District Court of Cologne ("inducement to breach of contract"). The provisions therefore have a direct detrimental effect on the business opportunities of bank-independent payment initiation services.

393. The provisions negatively affect the use of payment initiation services, whose services have been attacked by the GBIC for more than ten years with reference to the existing regulations.[319] The regulations relate to payment initiation services on the market for online payments in e-commerce, where there has been price competition over the past few years to the detriment of bank-related procedures. Even if the market shares of payment initiation services is still comparatively small compared to the large and established systems, this is a steadily growing market share. The agreement between the GBIC's central associations, which is contrary to antitrust law to the extent that the duties of care aim to prevent the use of payment initiation services, cannot completely exclude competition, but has significantly affected the development of competition over the years. For this reason, the market shares are still small, in particular due to the restraint of competition.

394. The provisions of the GBIC have prevented innovations in the area of online payments in e-commerce in the past[320] or made them more difficult[321]. The strategic and coordinated approach of GBIC has also already led to companies leaving market, thereby restricting innovation and competition from these

---

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

319 cf. paragraph 173cf.

320 cf. Action against the services offered by L'tur under paragraph 289.

321 cf. Action against German Telekom, paragraph 176and Sofort, paragraph 290.

service providers ([redacted]). The development of the duties of care and the approach by the GBIC against payment procedures which are offered despite the provisions of the general terms and conditions has resulted in a reduction of competitive pressure on products in the banking industry and bank-related products (giropay, Paydirekt, credit cards)[322] through innovation and in the limitation of competition, at least on the market for online payments in e-commerce. Without these rules, customers of online merchants would not need to worry about breaching contractual provisions if they choose to use payment initiation services. A large number of customers would accept the encouragement of online merchants to use payment procedures which are cheaper for the merchant.
Payment methods offered by payment initiation services would be more widely used and would achieve a higher level of acceptance.

395. The effect of the restraint of competition ultimately results from the fact that the rules force payment initiation services to use resources in order to protect themselves from attacks by bank associations, credit institutions and competitors against their competitive activities, in addition to the successful implementation of their business models. An example of this is the press release by the GBIC to Stiftung Warentest, in which Sofort's product was associated with illegal phishing attacks.[323] Only after the intervention of a lawyer, who demanded the submission of a declaration to cease and desist, was it able to prevent the use of this wording in the future. The same applies to the behaviour of individual credit institutions which inform their own customers about the unlawfulness of using payment initiation services and the giropay lawsuit.[324] Ultimately, the contested provision in the OBC of the GBIC and the central associations has given the banking industry time to develop its own product and place it on the market as a direct competitive product for existing payment initiation services. By "discrediting" existing payment initiation services over the course of several years, the GBIC and central associations of the banking industry have successfully created a negative image for these types of products, which has now allowed them to place their own product "Paydirekt" on the market as a competitive product which is operated by the banks and is therefore particularly trustworthy.

---

312 cf. paragraph 378.
323 cf. paragraph 235.
324 cf. paragraph 238et seq.

5. Substantial effect

396. The duties of care for customers in the Online-Banking-Conditions intend or in any case brought about restraint of competition on the market for online payments in e-commerce.

397. An agreement with the aim of forcing bank-independent payment initiation services from the nationwide market for online payments in e-commerce represents a substantial restraint of competition due to its very nature and irrespective of its actual effects.[325] The exclusion of competitors has a direct effect on the market structure and prevents the development of markets through innovations to the benefit of the demand side and consumers, who gain a greater selection of different products as a result of the competition and enjoy greater price competition between the providers of online payments in e-commerce.[326]

398. The criteria of substantial effect is also fulfilled if the resulting restraint of competition is assumed by way of the alternative. The agreement goes beyond what can be understood as a purely theoretically conceivable influence on the market. The external effects of the duties of care to be assessed here are substantial due to the fact that their adoption by the GBIC has limited the activities of competitors on the nationwide market for online payments in e-commerce and aims at forcing them out of the market. The contested duties of care have an influence on the existing market structure by reducing the diversity of services available to merchants as customers of payment procedures in e-commerce.

399. The duties of care have an impact on more than 50 million current account customers who are potential users of payment procedures in e-commerce. They have an effect on payment initiation services which, despite all preventative actions by the GBIC, have achieved a proportionally large and steadily increasing market penetration in the dynamically growing e-commerce market in recent years.

---

325 Judgment of the Court of the European Union on 13.12.2012, Expedia Inc./Autorité de la concurrence, paragraph 37, available at www.curia.eu.

326 Payment initiation services "offer both merchants and consumers a cost-effective solution and allow consumers to make purchases online, even if they do not have a payment card", cf. recital 29, PSD2.

400. Ultimately, the duties of care also protect the earnings interests of the credit institutions represented by the central associations of the German banking industry, e.g. as issuers of credit cards.

401. The decision made by the central associations of the banking industry working together in the GBIC affects a total of more than 50 million online current accounts in Germany (cf. paragraph 42), who are potential users of payment procedures in e-commerce and who could use payment initiation services. By specifying duties of care, the market for online payments is influenced in a significant way, as it rules out a possible method of payment for the majority of customers, which also has an effect on the competitive opportunities of payment initiation services compared to other payment methods. The assessment of whether the restraint of competition meets the requirement if substantial effect cannot be solely based on the current market penetration of payment initiation services and the scope in which customers actually use such payment methods. The ban on entry of personalised security credentials has resulted in uncertainty with regard to the legality of such methods among merchants and users. The usage patterns of customers has therefore remained low due to concerns about a possible breach of contract and the GBIC and credit institutions encouraged this perception in the past with press work and publications.

402. Payment initiation services also put competitive pressure on established payment methods such as PayPal and credit card payments. Credit cards, which generate revenue for the credit institutions which issue the cards, are attacked by the market penetration of payment initiation services and their competitive success in their market position. In 2013, credit cards were offered as a payment option in more than 80% of online shops with increasingly widespread use compared to 2012.[327] Sofortüberweisung.de achieved a distribution of 36% in 2011[328] and was able to increase this to approximately 50% in 2013[329]. Sofortüberweisung.de is particularly competitive due to its pricing for merchants and the security of

---

327 Online payment Study 2014 Data, facts, background and developments, YOY visibility of payment methods in the top 1,000 online stores in 2012 and 2013, EHI Retail Institute e.V, Cologne, p. 27.

328 Online payment Study 2012 Data, facts, background and developments, payment methods offered by the top online stores in 2011, EHI Retail Institute e.V, Cologne, p. 21.

329 Online payment Study 2014 Data, facts, background and developments, YOY visibility of payment methods in the top 1,000 online stores in 2013, EHI Retail Institute e.V, Cologne, p. 26.

incoming payments. The EHI Retail Institute estimates that, for companies with a turnover of more than EUR one million, costs for the payment method sofortüberweisung.de amount to an average of 0.93% of the turnover achieved. Only costs for payment on pickup, advance payment and purchase on account as a white label solution were cheaper in these cases. In contrast, the average cost of credit card payments was significantly higher at 2.28% of the transaction volume, the most expensive of all investigated payment methods.

403. Despite the restraint of competition intended by the PBC, merchant acceptance of Sofort's payment method shown relatively strong growth over the past few years. It can be assumed that this increase in customer acceptance would have been even greater without the unlawful restraints resulting from the OBC.

6. Applicability of Article 101 para. 1 TFEU, Section 1 GWB (supplementary agreements)

404. The applicability of Article 101 para. 1 TFEU, Section 1 GWB is also not excluded. Article 101 para. 1 TFEU, Section 1 GWB is applicable to the decision to collectively use the online banking conditions, including the ban on entering PINs and TANs on web pages not agreed with the credit institution in charge of the account due to the fact that this is not to be regarded as a supplementary agreement covered by the offense of cartel bans.

405. Within the scope of Article 101 para. 1 TFEU, "supplementary agreements" are to be understood as a restraint of competition which is directly associated with the execution of a main measure and are necessary for this measure to be carried out. Only those restraints which have a significance which is subordinate to the main element of this measure and are inseparably associated with it and are accordingly in an obvious relationship to it are considered to be directly associated. A restraint is necessary as long as it is objectively necessary for and proportionate with regard to the main measure. To establish a lack of objective necessity of a supplementary agreement, it is sufficient if it can be shown that the system operated with the main agreement would still be functional without this supplementary agreement. In contrast, it is not relevant if the lack of the supplementary agreement could have a negative effect on the function. Benefits potentially resulting from the supplementary agreement can be considered within the scope of Art. 101 para. 3 TFEU, Section 2[330].

The examination of the objective necessity of a restraint of competition does not lead to a "rule of reason", within the scope of which pro-competitive and anti-competitive effects of an agreement are balanced against each other. Such an examination can only take place within the scope of Art. 101 para. 3 TFEU, while only a comparably abstract approach can be taken within the scope of Art. 101 para. 1 TFEU. It follows in particular that it is not necessary to consider whether, in view of the competitive situation on the relevant market, the restraint of the commercial success of the main measure is essential, and it is sufficient to establish whether the restraint is necessary within the specific context of the main measure for the realisation of this measure. If the main measure were difficult or impossible to realise without the restraint, the restraint can be regarded as objectively necessary for its realisation.[331]

a) The Parties are entitled to jointly define rules of conduct for online banking customers in order to avoid cases of damage

406. The main purpose of the Online-Banking-Conditions is to guarantee security by defining appropriate rules of conduct for customers. To this end, the customer is obligated to keep their personalised security credentials confidential and to safely store authentication mediums (cf. para. 33). In addition, the Online-Banking-Conditions include rules for the apportionment of liability between the bank and customer in cases where financial damages are incurred due to unauthorised payment transactions.

407. In principle, the Parties can stipulate rules within the scope of antitrust law to increase the security of online banking and limit risks arising from the unauthorised disclosure and use of personalised security credentials and authentication mediums. Such a design is of benefit to all users due to the associated increase in the security of the overall system and the limitation of damage costs and is also required by law, such as the legal requirement for providers to pre-contractually provide

---

330 Decision by the European Court on 24.05.2012, MasterCard / Commission, Slg. II, paragraph 88.

331 Summarised presentation of the concept of supplementary agreements in the decision of the European Court on 24.05.2012, MasterCard / Commission, Slg. II-1, paragraph 77 ff.., with reference to the decision of the Court of First Instance on 18.09.2001, M6, Coll. II-2459, paragraph 105 et seq.

information about the specific content of the duties of care (Art. 248 Section 4 para. 1 no. 5 EGBGB). The Parties can also require that customers only enter the personalised security credentials on specific web pages in order to reduce the risk of phishing, for instance (cf. paragraph 52).

b) A general ban on entering personalised security credentials on web pages other than those separately agreed, in particular online merchant websites, is not necessary

408. The specific design of the customers' duties of care, according to which they are not permitted to enter personalised security credentials on web page other than those which have been agreed, e.g. not on online merchant websites, is not directly associated with and necessary for the main measure in the sense outlined above.

409. In order to achieve the aim of increasing security in the face of phishing and other abuse, the GBIC and its associations have a series of further options which cause less restraint of competition. For instance, it would be possible to introduce a certification process for payment initiation services and permit entry of the personalised security credentials on the websites of certified providers. The Parties themselves have discussed and developed the basic plans for such a process. Such an approval process would make it possible to monitor the processes of external service providers. Technical solutions that prevent the payment initiation services from processing the personalised security credentials are also conceivable.

410. The general ban on entering personalised security credentials on web pages other than those separately agreed, in particular online merchant websites is, on the other hand, excessive. Contrary to the view of the Parties, the competition-restricting effects associated with the decision cannot be regarded as being necessary in order to guarantee the security of online banking. The Parties are wrong to assume that the security risks arising from the entry of personalised security credentials on web pages other than those of the credit institutions in charge of the accounts could not be avoided in any way than by qualifying this as a gross breach of duties of care.[332]

411. The risks involved in online banking with regard to criminal activities alone cannot justify the almost complete exclusion of competition unless there is a specific connection

---

332 Letter by Oppenländer lawyers dated 29.07.2014, p. 6165 of the file.

between the criminal behaviour of phishing and the payment initiation services. To the extent that the GBIC raises security concerns, these do not regularly relate to the risks arising from the use of established payment initiation services operating on the market, whose reliability is also assessed by the online merchants, but to criminal activities such as phishing, which is a problem fundamentally associated with online banking. There are no evident online banking risks resulting specifically from the activities of existing payment initiation services. This is in particular the case against the background of the large amount of existing financial management software and other applications for mobile devices with security issues not controlled by the GBIC.

III. Ability to affect trade between Member States

412. The resolutions of the GBIC and its central associations (Parties Two - Four) are able to affect trade between the Member States - which not only includes the transitional cross-border exchange of goods and services but also all cross-border economic activities[333] - due to the fact that they apply to the entire territory of Germany. These types of cartel reinforce the partitioning of the markets at national level and prevent the economic integration intended by the Treaty on the Functioning of the European Union.[334]

IV. Lack of conditions for exemption under Article 101 para. 3 TFEU, Section 2 GWB

413. The prerequisites for exemption of the decisions (Art. 101 para. 3 TFEU, Section 2 GWB) are not evident and have also not been raised by the Parties. It does not appear that the contested decisions are essential for the achievement of the Parties' objectives. In fact, the submissions by the Parties in the proceedings show that it would have been possible for the Parties to introduce rules guaranteeing the security of online banking by taking other measures while

---

333 Notification of Commission decision on 27.04.2004, Guidelines on the concept of effect on trade between Member States contained in Articles 81 and 82 EC, 2004 / C 101/07, OJ. C 101/81, paragraph 19 ff.

334 Established case law, cf. judgment of the Court of the European Union on 19.02.2002, Collection p. I-1577, paragraph 95, "Wouters" with further references. Incidentally, the thresholds of the Guidelines on the concept of effect on trade between Member States contained in Articles 81 and 82 of the Treaty, paragraph 52 (market share of 5%, market volume of EUR 40 million) would be exceeded.

simultaneously restraining competition less in the market for online payment in e-commerce.

414. Decisions by associations of undertakings are exempted from the prohibition in Art. 101 para. 1 TFEU, Section 1 GWB in accordance with Art 101 para. 3 TFEU, Section 2 GWB if they contribute to the improvement of production or distribution of goods or support technical or economic progress, with reasonable participation of consumers in the resulting products, without limitations being imposed on the participating companies which are not essential for the achievement of these aims, or opportunities being created to eliminate a significant proportion of the products concerned.

415. When assessing the conditions for exemption, all four of these conditions must be met. Even if just one of these conditions is not satisfied, the overall conditions for exemption will not have been met. When assessing the conditions, it is not necessary to require compliance with a legal test sequence. [335]

1. Efficiency gains: Improvement in production (supports technical and economic development)

416. The first condition for exemption specified in Art. 101 para. 3 TFEU relates to the improvement of the production and distribution of goods resulting from the resolution which restricts competition. Similarly, the provision also applies to services along the same lines, even if they are not explicitly mentioned in the text. [336] Only objective benefits that must directly result from the decisions to be assessed under competition law provisions are to be taken into account. In addition to cost savings, quality improvements are also recognised as potential efficiency gains. These also include technical advancements of services, e.g. to increase security. [337]

417. At present it is not clear and is not argued by the parties that efficiency gains can be realised as a result of the decisions to be assessed in this case. Even if the

---

[335] Schneider in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1 Deutsches Kartellrecht, 12th Edition, Section 2 GWB, paragraph 26.

[336] Commission Notice, Guidelines on the Application of Article 81 paragraph 3 of the EC Treaty (2004/C 101/08), OJ of 27.04.2004, no. C 101, p 97, para. 48.

[337] Ellger, in: Immenga/Mestmäcker, Kommentar zum Europäischen Kartellecht, 5th Edition 2012, Art. 101 para. 3, paragraph 157.

general duties of care contribute towards the security of online banking by supporting the secure handling of the system and management of personalised security credentials, this does not apply to the general ban on entering personalised security credentials on web pages not separately agreed, in particular on the web pages of online merchants. It is not apparent that, as asserted by the GBIC, the use of payment initiation services, in contrast to the use of financial software products with comparable risk potential, would lead to habituation effects among customers which would result in the careless handling of personalised security credentials.

418. To the extent that the GBIC even mentioned this in its submissions so far, it bases the necessity of developing and clarifying the duties of care in the Online-Banking-Conditions adopted in 2009 on both the need to make adjustments due to changes to the legal framework and, most importantly, on the need to react to technical developments. The risks posed to online banking due to criminal attacks by third parties (e.g. through phishing, Trojans, man-in-the-middle attacks) in particular is described by the GBIC as an economic risk which was to be countered by revising the Online-Banking-Conditions.[338]

419. The duties of care in the Online-Banking-Conditions aim to develop a framework of action to counter the existing risks of misuse and manipulation by third parties and increase the security of the system to prevent financial damages. Standardised rules would help to promote a reliable and secure environment in which the contractual parties operate and where liability issues in the event of loss events are determined in advance. The duties of care therefore fundamentally have the potential to increase the security of the online banking system and therefore also to achieve efficiencies in the sense of the assessment under Art. 101 para. 2 TFEU and Section 2 GWB.

420. If and to what extent the duties of care result in the general qualitative improvement of security in online banking, which would be reflected by increased security and could be regarded as efficiency gains, does not need to be conclusively determined within the scope of this assessment of conditions for exemption. In this case, the assessment only extends to the question of which efficiency gains are associated with the specific obligation

---

[338] Letter from the GBIC dated 02.11.2010, p. 483 of the file

not to enter the personalised security credentials outside of the separately specified internet websites, especially not on online merchant websites.

421. The extent to which the implicit ban on using bank-independent payment initiation services in No. 7.2 para. 1 in conjunction with para. 2, third bullet point OBC might be considered an appropriate way to increase security in online banking is unclear. In this respect, the GBIC has associated the risks of criminal attacks (e.g. through phishing) with the activities of intermediaries. The duties of care, however, only target the activities of intermediaries, without taking the comparable risks arising from the use of financial software into account. This is evident from the footnote in the draft versions of the Online-Banking-Conditions, which mention the "*prevention of the involvement of intermediaries for security reasons*", while at the same time expressly enabling the use of products with a comparable risk potential, such as StarMoney.[339]

422. The prevention of threats generally represents an eligible improvement. As no conclusive justification has been put forward to explain which specific risks are associated with payment initiation services in particular, which can be prevented by the duties of care and why these risks are considered to be more significant than those associated with other services offered on the market in connection with online banking where no contractual relationship has been established between providers and credit institutions in charge of the account, there is no evidence of efficiency gains from the duties of care, i.e. security improvements of online banking.

423. The argument of the Parties that the corresponding duties of care would prevent a service which encountered concerns under data protection law cannot give rise to efficiency gains. To the extent that the duties of care are intended to exclude providers from the market who do not comply with data protection law or other legal areas according to the Standards of the GBIC, these are not efficiency gains within the meaning of Art. 101 para. 2 TFEU and Section 2 GWB. The verification of compliance with legal requirements is the responsibility of the competent authorities and courts and

339 [redacted]

cannot justify an antitrust agreement with adverse effects on competition.[340]

424. However, even under the assumption that the clause in the online banking conditions could be regarded as increasing efficiency on the basis of its purpose of preventing the use of a special service, this would not be sufficient for exemption of the resolution from the cartel ban, as such a rule is not essential and therefore does not meet the other conditions for exemption.

2. Indispensability

425. The contested decisions are not indispensable to achieve the aim of guaranteeing the security of online banking. There are other less severe measures, which have been considered by the GBIC itself and discussed with the Decision Division, which would allow the continued use of payment initiation services by customers in e-commerce and would prevent negative effects on competition.

426. The third condition specified in Art. 101 para. 3 requires that the decision does not result in any restraint of competition which is not indispensable to the achievement of the efficiency gains associated with the decision. The condition for exemption requires that the parties making a resolution to provide evidence that the implementation of the substantiated efficiency gains cannot be achieved in any other way. If the objectives of the decision can also be achieved with measures that have less of an impact on competition, the decision breaches the requirement to use the least severe measure to achieve the desired objective.[341]

427. When examining whether the intended measure can only be achieved by the adopted decision or if this would also be possible using solutions which are more compatible with competition, it should be clarified whether the decision is generally necessary in reasonable terms and whether the individual restraints of competition resulting from the resolution are reasonably necessary for this purpose.[342]

To the extent that payment initiation services accept personalised security credentials in order to gain access to the customer's online banking and inform the internet merchant whether the

---

340 Judgment of the European Court of First Instance in the case C-68/12 of 07.02. 2013, paragraph 20, (cited in: http://curia.europa.eu).

341 Schneider, in: Langen Bunte, Vol. 1, Section 2 GWB, paragraph 46.

342 Commission Notice, Guidelines on the Application of Article 81 paragraph 3 of the EC Treaty (2004/C 101/08), OJ of 27.04.2004, no. C 101, p. 97, para. 73 ff..

credit institution will accept the transfer for the settlement of the invoice amount from the transaction with the customer, the GBIC has developed criteria according to which such business models do not put the security and integrity of online banking in doubt. The GBIC passed the authorisation concept presented to the Decision Division on to what it considers to be the relevant economic participants for comment and assessment. Even the written submissions of the GBIC, which state that it considers a collaboration to be possible under the mentioned security aspects, are evidence that here are less severe measures which can be used when dealing with payment initiation services than to completely prohibit their use.

428. The approval process envisages the certification of the respective provider of payment initiation services by the GBIC. The payment initiation service must demonstrate compliance with safety requirements. By entering the personalised security credentials on the website of a certified provider, the online banking customer would not breach its duties of care.

429. As a prerequisite for the entry of a PIN and TAN on the web page of a payment initiation service, the GBIC requires reliable and error-free data processing by the operator, where malfunctions and abusive interventions are extensively excluded. The security requirements should be consistent with those of a credit institution when processing confidential data in its own system and systems of commissioned data processing centres.[343] The GBIC and its central associations have developed detailed requirements for the security of payment initiation services in e-commerce and has also described test requirements for service providers in this regard, which can be used to validate compliance with the security requirements by the operators of such procedures.

430. The content of the safety requirements relates to the data elements to be protected. In doing so, requirements are imposed on approved services regarding the protection of personalised security credentials, the protection of customer and transaction data, the use of specified interfaces, the duty of the payment initiation service to identify itself to the credit institution in charge of the account and the restraint of activities. In the context of the requirements concerning

---

343 Letter from the GBIC dated 09.08.2011, p. 1697 of the file
344 Letter from the GBIC dated 29.03.2012, p. 2854 ff.. of the file

the organisation of security, requirements regarding internal organisation as well as for external parties have been formulated. In addition to the personal security, which relates to requirements for employees and other individuals in relation to handling sensitive data elements, requirements for the safe environment of data processing centres to protect against unauthorised access by third parties make up a significant part of the conceptual approach developed by the GBIC. Access control and encryption techniques are required in this context, in addition to the operation of hardware security modules. The concept also includes requirements relating to communication and operations management, operational monitoring, the planning and acceptance of IT systems, protection against malicious software and security management of networks. Requirements regarding the control of access to data centres, networks and mobile devices are also formulated in the requirements. Finally, general requirements for the data centre operations are specified under the headline 'Procurement, development and maintenance of IT systems'. [345]

431. The test requirements also developed by the GBIC and its central associations describe which test steps would ensure compliance with the security requirements, which evidence would need to be provided for the execution of the test by the operator of the payment procedure and finally, in which way the execution of the test steps would be documented.[346] However, the central banks and in particular the European Central Bank are critical of this type of model, to the extent that it permits the entry of personalised security credentials on third-party websites. Under current law, such a model would, however, be conceivable.

432. The GBIC also presented requirements for other business models which, from the point of view of the GBIC, would be tolerable with less stringent requirements from the point of view of the GBIC, as they could work without the receipt of a PIN and TAN. Currently, service providers are not using these types of alternative business models on the market, which is why these considerations are no more than theoretically relevant constructs.

433. The concepts prepared and presented by the GBIC for dealing with payment initiation services suggest the development of an approval process and a contractual agreement between approved service providers and the

---

345 Letter from the GBIC dated 29.03.2012, Annex 1, p. 2860 of the file
346 Letter from the GBIC dated 29.03.2012, Annex 2, p. 2888 of the file

individual credit institutions. Those service providers who have successfully completed the registration procedure would, according to the GBIC, be added to a list of positives, from which the account servicing payment service provider could select those which it wishes to define as an access channel for online banking and therefore enable its use by their customers. There would be no obligation to cooperate with individual service providers. [347]

434. When assessing indispensability, the Decision Division focuses solely on the question of whether it appears to be safely possible, in the opinion of those involved, to deal with payment initiation services in a different way than to prohibit its use in general - as in the Online-Banking-Conditions. The assessment is essentially based on the fulfilment of the security criteria.

435. To the extent that the Parties assert that a contractual agreement between the operator of the payment initiation service and the account servicing payment service provider would be required regardless, this does not actually apply to the extent that this would require the presence of a separate contractual agreement. Within the scope of the options of third party providers to offer products for use in online banking, the GBIC has created standards by defining interfaces (FinTS, HBCI) which are sufficient for the commercial activities of a series of service providers, e.g. in the area of home banking software. Regardless of whether these services are offered on customers' devices or as web applications, there are not usually any individual agreements between account servicing payment service providers and the service providers. For example, both a PIN and TAN are transferred to the account servicing payment service provider through the use of the "Starmoney.web" product and the account data is saved in the technical infrastructure of the provider. There are no contractual agreements between the provider and credit institutions in charge of the accounts and these are also not required by the GBIC or individual associations or credit institutions. Such services are offered solely on the basis of the security standards of the providers with no authorisation or review by the GBIC or individual credit institutions. For this reason, it appears to be appropriate and non-discriminatory to view the approval of a payment initiation service under security aspects to be sufficient for the activity of such service providers on the market. This does not rule out that contractual agreements may be concluded between the respective

---

[347] Letter from the GBIC dated 15.04.2011, p. 1554 of the file

institution managing the account and provider of payment initiation services regarding the acceptance of framework conditions and standards. An example of this are the merchant conditions of the electronic cash agreement, which establishes a direct contractual link between the card issuer and the card-accepting merchants. The conclusion of a framework agreement of the central associations of the banking industry, acting on behalf of their members, and the respective provider of a payment initiation service, would be another possibility.
Such a solution – with recognition of appropriate safety standards – is, for example, practiced in relation to the system operators in the electronic cash system.

436. If the GBIC were to establish such an authorisation procedure, the conclusion of agreements between payment initiation services and credit institutions would not be an essential element of such a concept. In addition, such a requirement would be contrary to the requirements of the PSD2, which does not make the provision of payment initiation services dependent on the existence of a contractual relationship between the payment initiation service and credit institutions in charge of the accounts (cf. Art. 115, para. 6, recital 33 PSD2).

V. Breach of 19 para. 3 sentence 1 in conjunction with para. 1, para. 2 no. 1 GWB

437. The overall plan of Parties One - Four described above, with the aim of impeding payment initiation services, also represents an unfair hindrance of payment initiation services in accordance with Section 19 para. 3 p. 1 in conjunction with Section 19 para 1, para 2 no 1 GWB.

438. According to Section 19 para. 3 sentence 1, the prohibition of unfair hindrance of other companies (Section 19 para. 1, para. 2 no. 1 GWB) applies to associations of competing undertakings within the meaning of Section 2 GWB. The area of application of the special behaviour supervision of Section 19 para. 1, para. 2 no. 1 GWB is in this respect also extended to include associations of undertakings which are not market-dominant (Section 18 GWB) or have relative or superior market power (Section 20 GWB). Parties Two - Four are to be regarded as such associations of undertakings. The term association corresponds to the term association of undertakings in Section GWB or Art. 101 TFEU. This follows from the reference to the rules on the exemption offenses in Section 2, Section 3, Section 28 para. 1, Section 30 para. 2, Section 31 para. 1 GWB. In this respect, reference can be made to the previous remarks regarding the concept of an association of undertakings (above under I.1.).

439. According to the wording of Section 19 para. 3 sentence 1 of the GWB, only those cartels exempted from the GWB are covered by the area of application of the standard. In the current system of legal exception from the cartel ban, the application of Section 19 para. 3 sentence 3 GWB is only available with no explicit exemption if the antitrust admissibility of the respective activities of the "association of competing companies" itself is not in any doubt. In the system of legal exception it is therefore not necessary to clarify in these cases whether the activity of the association of undertakings, during the course of which the conduct to be assessed in accordance with Section 19 para. 3 sentence 1 GWB (here: the establishment of the banks with the general terms and conditions) already satisfies the elements of the offence at the level of Section 1 GWB and Art. 101 para. 1 TFEU, or whether it is only excluded from the cartel ban at the level of the exception, especially as the limit can be flexible in the case of recommended conditions.[348] This limit is particularly flexible in the case of banking and insurance conditions in view of the special conditions in these markets. [349] The aim of the special provisions of Section 19 para. 3 sentence 1 GWB for undertakings is to make the market power of the member companies gained through a prima facie permissible cooperation subject to the restraints of
Section 19 para. 1, para. 2 nos. 1 and 5 GWB.[350] The particular market power of the prima facie legal association of undertakings is therefore fundamental for the application of the standard. An association of undertakings which is prima facie illegal would not have such market power, as its leeway for action would already be limited by the threat of penalties.[351]

440. According to these principles, the GBIC and the central associations of the banking industry are norm addressees in accordance with Section 19 para. 3 sentence 1 GBIC. The joint preparation of general terms and conditions for banks has been one of the tasks of the corresponding associations of undertakings for decades. The Parties do not consider these activities to be prima facie contrary to competition law, nor has the Federal Cartel Office or the EU Commission considered it to be appropriate to make the terms of the AGB banks themselves the subject of proceedings pursuant to Art. 101 TFEU and Section 1 GWB. In economic terms, the GBIC and its central associations

---

[348] cf. Horizontal Guidelines of the COM of 14.01.2011 (C 11/1), para. 270-272, 300-307, 312 et seq., 320, 335.

[349] l.c., paragraph 259 at the end. See also Braun in: Langen/Bunte, Kartellrecht Kommentar, Vol. 1, Deutsches Kartellrecht, 12th Edition, according to Section 2 paragraph 175.

[350] cf. Nothdurft in: Langen/Bunte, Kartellrecht Kommentar, Bd. 1 Deutsches Kartellrecht, 12th Edition, Section 19 GWB, paragraph 82.

[351] For standard application also with regard to illegal cartels: Nothdurft in: Langen / Bunte, Kartellrecht Kommentar, Vol. 1, Deutsches Kartellrecht, 12th Edition, Section 19 GWB, paragraph 80.

have set an industry standard through the creation of general terms and conditions, which provides a sufficient basis to measure the assertion of the corresponding discretion during the development of the conditions, including according to the special standards of Section 19 para. 3 sentence 2 GWB.

441. To the extent that there needs to be an identity or at least a correlation between the market to which the exemption (or even the lack of elements required for the offence) of the association of undertakings' actions refers and the market in which the restraints occur[352], this condition is also fulfilled here. The coordination of the Online-Banking-Conditions in the OBC relates to the market for private current accounts. The impact established here, in particular the unfair restraint of competitors, have an effect on competition in the nationwide market for online payments in e-commerce. There is an interaction between these markets: the regulations of the banking industry relate to the use of online banking and therefore the situation in the market for private current accounts. As payment initiation services are based on customers of an online shop being able to use their online banking access to pay for goods and services in e-commerce, the regulations in the banking industry also affect the services of online payments providers in e-commerce. If bank customers comply with the OBC, the services offered by bank-independent payment initiation services will have no users. In terms of access to this market, the OBC has created a legal barrier to entry. Only payment initiation services operated by the banking industry itself are unaffected by these provisions. The OBC has resulted in an arrangement of the market by excluding or promoting certain competitors in the field of payment services in e-commerce.

442. The prohibition of this conduct lies in the intended scope of Section 19 para 3 sentence 1 GWB, so that the operative provisions of this ruling may also be supported by this legal basis: the constellation of the AGB banks by the GBIC and its central associations, which is in principle permissible under antitrust law, they are subject to a special obligation to take the market effects of their adopted standard conditions into account, irrespective of their permissibility under the aspect of the coordination of its members' market behaviour (Section 1 GWB or Art. 101 TFEU). Even if there were no objections to the standard conditions laid down by the GBIC under the aspect of

---

352 cf. Nothdurft, in: Langen/Bunte, Kartellrecht, Kommentar, Bd. 1, Detusches Kartellrecht, 12th edition Section 19 paragraph 81.

coordination between the banks which have joined forces within the GBIC, it would be required to ensure, pursuant to Section 19 para. 3 sentence 1 GWB, that the conditions did not have any negative effects on individual players on the market, particularly those not involved in the development of the conditions. An association of undertakings is therefore prohibited from using a version of business conditions which may still be admissible from the aspect of coordination, but hinder third parties in competition with their member companies and promote their own services from within the association of undertakings (or of affiliated companies) to the detriment of outsiders. The fact that this was the case and intended here has already been demonstrated (in this regard cf. above, in particular under II). 3. d.). In this respect, the behaviour of the GBIC and the central associations was still unlawful and prohibited within the meaning of the operative provisions of this order if the OBC was, contrary to the view taken here, still to be regarded as permissible under the aspect of coordination (Section 1 GWB, Art. 101 TFEU). The illegality of this would result from the restrictive effect within the meaning of Section 19 para. 1, para. 2 no. 1 ARC at the expense of bank-independent payment service providers.

443. The remaining conditions for the application of this provision are fulfilled. The disadvantageous effect of the OBC on the business operations of the providers of bank-independent payment initiation services is to be regarded as a restraint, as the use of their services is associated with legal risks with regard to the business relationships with their credit institutions. This restraint is also unfair, as the interests of the GBIC and its central associations, when balanced with the interests of the providers of payment initiation services, taking the objective orientation of the law towards freedom of competition into account[353], falls in their favour: the decisive factor is that the OBC are in general aimed at preventing market access by providers of bank-independent payment initiation services. The market access restraints created by the OBC do not affect only some of the business activities of payment initiation service providers, but their business model itself. The aim of the legislation to keep the markets open[354] therefore requires the application of abuse prohibitions to a particularly high extent. Secondly, it should also be noted that

---

353 established case law, most recently Federal High Court of Justice. Judgement of 06.10.2015, KZR 87/13, NZKart 2015, 535 paragraph 59 – Porsche- Tuning.

354 established case law, most recently Federal High Court of Justice. Judgement of 24.10.2011, KZR 7/10, WuW/E DE-R 3446, paragraph 37, 50 – Grossistenkündigung.

the services provided by Sofort and other bank-independent payment initiation services are a new and innovative type of service which is in demand among operators of websites and their customers, which was not covered by the services offered by the member companies of the central associations. In this respect, this case involved such service providers, particularly in relation to Sofort, remaining on the market, which also requires the intervention of the control of abusive practices to a particularly high extent. The interests pursued by the introduction of the OBC by the GBIC and its central associations do not outweigh these concerns. To this extent, reference can be made to the remarks made above (under 1. and 2.).

E. Offered commitments

444. The alternatives identified by the GBIC as to how the activities of payment initiation services could be changed so that they are, from the point of view of the GBIC, completely compatible with the banking industry requirements, were not sent to the Federal Cartel Office as a binding commitment. They were discussed with no binding effect and were not further assessed with regard to their suitability to solve the problem.

445. To the extent that the Parties intend to make commitments (Section 32 b GWB), these need to be capable of structurally safeguarding the competitive processes in the online payments market in e-commerce. In this respect, it is essential that the business models of bank-independent providers of payment initiation services developed on the market do not need to be fundamentally modified on the basis of technical requirements or are excluded right from the start. It should therefore be critically considered whether these providers would be dependent on upstream services of the institutions managing the account in the future.

446. If, due to technical changes, payment initiation services were no longer in a position to independently provide notifications to merchants in e-commerce that the transfer request has been received by the customer's online banking and will also be executed with a high degree of probability, there may be potential restraints of competition as a result of such technical solutions. This is especially the case if the payment initiation services were required to purchase confirmations regarding the existence of sufficient funds in the customer account for transfer of the invoice amount or an irrevocable bank guarantee when implementing such concepts by credit institutions or no longer participated in the confirmation to execute the payment by the credit institution in charge of the account.

447. In a letter dated 02.12.2015, the GBIC sent a draft public law contract and the draft of the amended Special Conditions for Online Banking in order to bring the proceedings to an end.

448. The provision that the entry of personalised security credentials "e.g. not on online merchant websites" was prohibited was to be deleted in the amended special conditions with no replacement. Furthermore, the GBIC suggested that a new duty of care should be added, stating that customers are permitted to use a payment initiation service active on the market at the time the PSD2 came into force to pay for goods and services on the internet as long as it was based in the European Economic Area. Without the use of such services being approved in advance by the respective credit institution, the customer would be required to carefully select the payment initiation service.[355]

449. The Parties distanced themselves from the implementation of these changes in the form of a commitment, which the Decision Division could have declared as binding in accordance with Section 32 GWB and withdrew the suggestion to remove the restriction, with would have been appropriate in terms of its content.

F. Discretion

450. This decision was taken on the basis of Section 32 GWB. According to Section 32 para. 1 GWB, the competition authority decides, after due consideration, whether it will act upon suspicion of a breach of German or European antitrust law.[356] This also applies to the question of whether the Federal Cartel Office only identifies an infringement and waives the establishment of measures to retract the accusation of antitrust activities. To the extent that the wording of Section 32 para. 3 GWB requires a justified interest for the Federal Cartel Office to be able to identify an infringement even after its cessation; this restraint does not apply to the identification of an on-going antitrust infringement. In the legal assessment of on-going activities, a special establishment of interest, conversely to Section 32 para. 3 GWB and general principles, is not required. Within the scope of the principle of proportionality, the operative part of the decision can be limited to a mere statement if this is deemed to be adequate on the basis of the circumstances of the case

---

355 cf. Letter dated 02.12.2015, Annex Public Service Contract, p. 3
356 cf. Bornkamm, Langen Bunte, Section 32 paragraph 9.

due to the face that it can be assumed that the lawful status will be recovered in another way in the future. [357]

451. When exercising its discretion, the Decision Division decided to limit the decision to the establishment of illegality of the GBIC's and central associations of the banking industry's decisions. When making its decision, the Decision Division in particular considered that there appear to be a wide range of possible measures which would avoid the antitrust violation while preserving the justified security interests of the banking industry. Among other things, the GBIC presented two different concepts which would be appropriate. A finding according to the one in the operative provisions is sufficient in order to, on one hand, maintain sufficient room for manoeuvre for Parties One – Four, and on the other, to highlight the clear limits of the room for manoeuvre under antitrust law.

Such a finding that the coordination and implementation of the contested clauses of the Online-Banking-Conditions is illegal is still appropriate and necessary at this point in time. It is true that, during the implementation of the PSD2, the European legislator commissioned European institutions to draft Regulatory Technical Standards to specify the coordinated activity of payment initiation services and credit institutions. The Decision Division assumes that anti-competitive behaviour such as that contested in these proceedings will be prevented by these types of standards in the future and through the transposition of the PSD2 into national law. However, the companies affected by the breach of competition law should not be expected to accept the unfair hindrance and the current legal uncertainty, which also has an impact on the pending civil proceedings, until the end of the transposition period for the PSD2 into national law.

It is in the public interest, for the Division to take a binding decision, particularly in light of these pending civil proceedings which have been suspended due to these proceedings. These proceedings have handled this decision in the form of a detailed justification of the legal interpretation of the Division on the basis of the facts, which have been fully clarified by way of an official appraisal. In view of what have been, at times, lengthy suspensions of civil proceedings, the issuance of a declaratory judgement is therefore also in the interest of a successful interlocking of public and private enforcement.

---

[357] cf. Emmerich, Immenga/Mestmecker, Section 32 paragraph 48 et seq.

452. In accordance with the requests of Parties One - Four, (see above paragraphs 262, 264), the immediate execution of this decision will be suspended pursuant to Section 65 para. 3 sentence 2 GWB. The suspension of the immediate execution also comes into consideration in the case of a strictly declaratory decision (see. Section 80 para. 1 sentence 2 Code of Administrative Procedure (VwGO)). The suspension does not prevent the ruling from fulfilling its purpose with regard to the pending civil proceedings, as the ruling and the investigative results laid down in the ruling can be used without enforceability of these proceedings. Moreover, a further binding effect pursuant to Section 33 para. 4 GWB would in any case be issued from definitive and legally effective government or court decisions. The fact that Parties One - Four - to the extent that they consider it necessary to request suspension measures as a result of the declaratory official decision - should not need to take such measures into account on the basis of the legal opinion of the Office, only to potentially need to change them again if corrections are made by the Senate, speaks in favour of the suspension.

G. Fees

453. Official acts on the basis of Section 32 GWB are subject to a fee pursuant to Section 80 para. 1 sentence 2 no. 2 GWB. The fee percentage must not exceed € 25,000 pursuant to Section 80 para. 2 sentence 2 No.2 GWB. If the personnel or material costs are particularly high, taking into account the economic significance, this fee can be doubled (Section 80 para. 2 sentence 3 GWB).

454. The amount charged depends on the personnel and material expenses of the competition authority, taking into account the economic significance of the subject of the chargeable act (Section 80 para. 2 sentence 1 GWB). The economic significance is the most important determination factor. If the economic significance established on the basis of these determination factors is average, an average fee is appropriate. According to the current fee framework, this amounts to € 12,500. Depending on the economic importance and the workload, this average must be increased or reduced by sums the amount of which is at the discretion of the Federal Cartel Office.[358] The restraint of competition and its intensity, along with the market significance of the parties in the proceedings,

---

358 cf. OG Düsseldorf, WuW 2000, 894 "Tequila"; KG WuW/E OLG 5259 "Kleinhammer"; KG WuW/E OLG 5287 "Finanzbeteiligung Gebühr".

are to be taken into account when determining the economic significance.[359]

455. [redacted]

456. [redacted]

457. [redacted]

458. [redacted]

459. [redacted]

359 Stockmann, in: Immenga / Mestmäcker, GWB, 4th Edition, Section 80 paragraph 15.

[redacted]

[redacted]

460. [redacted]

461. [redacted]

H. Right to appeal

462. An appeal can be made against this decision. It is to be submitted to the Federal Cartel Office, Kaiser-Friedrich-Straße 16, 53113 Bonn no later than one month after notification of the decision. However, it is sufficient if the appeal is received by the appellate court, the Higher Regional Court Dusseldorf, within this period.

463. A statement of grounds for the appeal is to be submitted to the Federal Cartel Office or appellate court. The deadline for the statement of grounds is two months. This period will begin upon notification of the contested court order and can be extended upon request by the judge of the appellate court. The statement of grounds must include a statement regarding the extent to which the decision is being challenged and its amendment or repeal, along with the facts and evidence - including any new ones - on which the appeal is based.

464. The notice of appeal and statement of grounds must be signed by a lawyer. The appeal shall have suspensive effect.

E.-M. Schulze | Holin | Jakobi

TABLE OF CONTENTS