Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 30 April 2020[1]

Case C-287/19

DenizBank AG
v
Verein für Konsumenteninformation

(Request for a preliminary ruling
from the Oberster Gerichtshof (Supreme Court, Austria))

(Reference for a preliminary ruling — Consumer protection — Payment services in the internal market — Unfair terms — Change in the conditions of a framework contract — Review of transparency — Validity of terms including tacit consent and transferring to the payment service user the risk of liability for unauthorised payments — Derogation for low-value payment instruments — Personalised payment card with near-field communication (NFC) functionality — Anonymous payment instruments — Unblockable payment instruments)

1. Technological innovation is having an enormous impact on payment services in the internal market. Testament to this is the adoption of Directive 2007/64/EC[2] and its replacement a few years later by Directive (EU) 2015/2366.[3] That update was essential in the light of the new payment systems available, the growing volume of electronic payments and the increased security risks associated with both those developments.

2. One of those innovations, which has quickly become popular, is near-field communication (NFC) functionality, which is added to certain payment cards.[4] This functionality allows low-value payments to be made anonymously and without the need for strong authentication.

3. Banking institutions that issue NFC-enabled cards aim to speed up standard-form contracting in order to make it easier to manage, but the conditions which they attach to the use of such contracting may operate to the detriment of consumer rights. The questions raised by the referring court are underpinned by the tension between those two objectives.

1 Original language: Spanish.

2 Directive of the European Parliament and of the Council of 13 November 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 (OJ 2007 L 319, p. 1).

3 Directive of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ 2015 L 337, p. 35). The repeal of Directive 2007/64 is effective from 13 February 2018.

4 The addition of NFC technology to contactless cards allows a wireless connection to be established between the cards and any compatible terminal near to which they are held, without the need for any further operation. NFC is a short-range, high-frequency wireless communication technology which enables data to be transmitted almost immediately between devices. It is used in various applications, including credit and debit cards, and, increasingly, in mobile phones. The NFC standards cover communication formats and data exchange formats based mainly on ISO 14443, which is jointly managed by the International Organisation for Standardisation and the International Electrotechnical Commission (IEC).

I. Legal framework

A. EU law. Directive 2015/2366

4. The recitals of the Directive include the following:

'(6) … Equivalent operating conditions should be guaranteed, to existing and new players on the market, enabling new means of payment to reach a broader market, and ensuring a high level of consumer protection in the use of those payment services across the Union as a whole. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonised payments market.

…

(63) In order to ensure a high level of consumer protection, Member States should, in the interests of the consumer, be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change.

…

(91) Payment service providers are responsible for security measures. Those measures need to be proportionate to the security risks concerned. Payment service providers should establish a framework to mitigate risks and maintain effective incident management procedures. A regular reporting mechanism should be established, to ensure that payment service providers provide the competent authorities, on a regular basis, with an updated assessment of their security risks and the measures that they have taken in response to those risks. Furthermore, in order to ensure that damage to users, other payment service providers or payment systems, such as a substantial disruption of a payment system, is kept to a minimum, it is essential that payment service providers be required to report major security incidents without undue delay to the competent authorities. A coordination role by EBA should be established.

…

(96) The security measures should be compatible with the level of risk involved in the payment service. In order to allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale, whether or not they are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards. …'

5. Article 4(14) defines 'payment instrument' as 'a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order'.

6. Title III is devoted to 'transparency of conditions and information requirements for payment services'. Chapter 3 thereof, which governs 'framework contracts', includes Articles 52 and 54.

7. Article 52 ('Information and conditions') provides:

'Member States shall ensure that the following information and conditions are provided to the payment service user:

…

6. on changes to, and termination of, the framework contract:

(a) if agreed, information that the payment service user will be deemed to have accepted changes in the conditions in accordance with Article 54, unless the payment service user notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted;

(b) the duration of the framework contract;

(c) the right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with Article 54(1) and Article 55;

…'

8. Article 54 ('Changes in conditions of the framework contract') provides:

'1. Any changes in the framework contract or in the information and conditions specified in Article 52 shall be proposed by the payment service provider in the same way as provided for in Article 51(1) and no later than 2 months before their proposed date of application. The payment service user can either accept or reject the changes before the date of their proposed date of entry into force.

Where applicable in accordance with point (6)(a) of Article 52, the payment service provider shall inform the payment service user that it is to be deemed to have accepted those changes if it does not notify the payment service provider before the proposed date of their entry into force that they are not accepted. The payment service provider shall also inform the payment service user that, in the event that the payment service user rejects those changes, the payment service user has the right to terminate the framework contract free of charge and with effect at any time until the date when the changes would have applied.

…'

9. In Chapter 1 ('Common provisions') of Title IV ('Rights and obligations in relation to the provision and use of payment services'), Article 63 ('Derogation for low-value payment instruments and electronic money') reads:

'1. In the case of payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time, payment service providers may agree with their payment service users that:

(a) point (b) of Article 69(1), points (c) and (d) of Article 70(1), and Article 74(3) do not apply if the payment instrument does not allow its blocking or prevention of its further use;

(b) Articles 72 and 73, and Article 74(1) and (3), do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;

…’

B. National law. Zahlungsdienstegesetz 2018 [5]

10. Paragraph 4, point 14, defines ‘payment instrument’ in the same way as the article carrying the same heading in Directive 2015/2366.

11. As regards changes to framework contracts, Paragraph 48(1), point 6, reiterates the content of Article 52(6) of Directive 2015/2366.

12. In relation to changes in conditions of framework contracts, Paragraph 50(1) is framed in terms similar to those of Article 54(1) of Directive 2015/2366.

13. The same is true of Paragraph 57(1) of the ZaDiG and Article 63(1) of Directive 2015/2366, concerning the derogation relating to low-value payment instruments and electronic money.

II. Dispute and questions referred for a preliminary ruling

14. The Verein für Konsumenteninformation (‘the VKI’) is an association with standing to bring legal proceedings under Austrian law in order to defend the interests of consumers.

15. DenizBank AG is a banking institution active in Austria. In its dealings with customers, it employs general terms and conditions of business and standard-form contracts in connection with, inter alia, the use of NFC-enabled payment cards. NFC functionality is activated automatically when the customer uses the card for the first time.

16. By holding their card near to the point of sale terminal in an establishment equipped with a wireless-enabled device, customers can make payments up to a value of EUR 25 without entering a personal identification number (‘PIN’). Higher-value transactions require identification by PIN.

17. The general terms and conditions employed by Denizbank in its contracts include the following:

‘Clause 14:

Changes to the terms of use for customers: Changes to these terms of use for customers shall be proposed to the customer no later than two months before the planned date of their entry into force. The payment service user shall be deemed to have accepted these changes and the changes shall therefore be deemed to have been agreed unless the customer notifies DenizBank AG before the date of their proposed date of entry into force that they are not accepted. The aforementioned change proposal shall be communicated to the customer on paper or, subject to his consent, on another durable medium. In its change proposal, DenizBank AG shall advise and point out to the customer that his silence, within the meaning indicated above, shall be deemed to constitute consent to the change. In addition, DenizBank AG shall publish a comparison of the provisions affected by the change to the terms of use for customers on its website, and shall also send a copy thereof to the customer. So far as businesses are concerned, it shall be sufficient for the change proposal to be made available for consultation in a manner agreed with the business concerned. In the event of such an intended change to the terms of use for customers, customers who are consumers shall have the right to terminate their framework contracts for payment services (in particular the current account contract) free of charge and without notice before the entry into force of the changes. DenizBank AG shall draw the customer’s attention to this point too in its change proposal.

5 2018 Law on Payment Services (‘the ZaDiG’), which transposed Directive 2015/2366 into national law.

Clause 15:

No proof of authorisation: Since the purpose of enabling low-value payments to be made without a PIN is to provide a simplified, authorisation-free payment process, DenizBank AG shall not have to prove that the payment transaction was authorised, duly recorded, accounted for and unaffected by any technical failure or other deficiency.

Clause 16:

No liability for unauthorised payments: Since, when the debit card is used to make low-value payments without entering a PIN, DenizBank AG is unable to prove that the payment transaction was authorised by the cardholder, DenizBank AG is under no obligation, in the event of an unauthorised payment transaction, to refund the amount of the unauthorised payment transaction and to restore the debited account to the state in which it would have been had the unauthorised payment transaction not taken place. Any more extensive claims against DenizBank AG — in so far as they are based on slight negligence on the part of DenizBank AG — shall also be excluded.

Clause 17:

Caution: Any risk of misuse of the payment card for low-value payments not requiring a PIN shall be borne by the account holder.

Clause 18:

Unblockability of low-value payments in the event that the debit card is mislaid: It is technically impossible for the debit card to be blocked when used for low-value transactions. Should the debit card be mislaid (through loss or theft, for example), it shall still be open to use for low-value payments not requiring a PIN up to a value of EUR 75, even after a block has been placed on the card in accordance with point 2.7. Such sums shall be non-refundable. Since these are low-value payments within the meaning of Paragraph 33 of the ZaDiG (Zahlungsdienstegesetz (Law on payment services)), payments may not exceed EUR 25 per individual transaction and the debit card cannot be blocked for low-value payments made without entering a PIN, Paragraph 44(3) ZaDiG is not applicable.

Clause 19:

Unless point 3 expressly makes special provision for low-value payments, these too shall be governed by the provisions of point 2 (card service)'.

18. On 9 August 2016, VKI brought an action for a prohibitory injunction against DenizBank before the Handelsgericht Wien (Commercial Court, Vienna, Austria).

19. In the judgment of 28 April 2017, that court upheld the action in relation to clauses 14 to 19. In its view, clause 14 was manifestly unfair and the conditions governing the application of the exceptional regime for low-value payment instruments were not met because the card in question could be used to make other payments too. The additional functionality of unauthorised contactless payment could not even be classified as a payment instrument.

20. That judgment having been appealed to the Oberlandesgericht (Higher Regional Court, Vienna, Austria), that court, by judgment of 20 November 2017, confirmed in part the interpretation adopted by the court of first instance.

21. In the opinion of the appeal court, if regard is had to the contactless payment functionality alone, there is no use of a payment instrument, that process being, rather, a MOTO (mail-order telephone order) credit card transaction. That is demonstrated by the fact that NFC functionality, which does not require the entry of a PIN, is activated automatically in the case of low-value purchases, unlike what occurs with an 'electronic purse'. Moreover, the debit card used for NFC transactions is not anonymous but, rather, personalised and protected by a personal PIN.

22. VKI and Denizbank each appealed the judgment of 20 November 2017 to the Oberster Gerichtshof (Supreme Court, Austria), which has referred the following questions to the Court of Justice for a preliminary ruling:

'(1) Is point (6)(a) of Article 52 in conjunction with Article 54(1) of Directive [2015/2366] (Payment Services Directive), pursuant to which the payment service user will be deemed to have accepted proposed changes in the conditions unless the payment service user notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted, to be interpreted as meaning that tacit consent can also be agreed with the consumer for any conceivable contractual conditions without any restriction?

(2) (a) Is point (14) of Article 4 of the Payment Services Directive to be interpreted as meaning that the NFC function of a personalised multifunctional bank card by means of which low value payments are debited from the associated customer account constitutes a payment instrument?

(2) (b) If Question 2(a) is answered in the affirmative:

Is Article 63(1)(b) of the Payment Services Directive regarding the derogations for low value payments and electronic money to be interpreted as meaning that a contactless low value payment using the NFC function of a personalised multifunctional bank card [is] to be regarded as anonymous use of the payment instrument within the meaning of the derogation?

(3) Is Article 63(1)(b) [6] of the Payment Services Directive to be interpreted as meaning that a payment service provider can rely on that derogation only if it can be established, according to the objective state of technical knowledge, that the payment instrument does not allow its blocking or prevention of its further use?'

23. Although the legislation applicable *ratione temporis* to the facts is Directive 2007/64, the Oberster Gerichtshof (Supreme Court) has explained, at the request of the Court of Justice, that, when hearing and determining actions for a prohibitory injunction in relation to the validity of contractual terms ('Klauselprozess'), it must also apply Directive 2015/2366, as the legislation in force at the time when judgment is given. Given that, as far as this dispute is concerned, the content of the provisions of both directives is practically identical,[7] I shall refer to the provisions of Directive 2015/2366, in respect of which the referring court raises its questions.

24. Written observations have been lodged by VKI, DenizBank, the Commission and the Governments of Portugal and the Czech Republic. A hearing held on 13 February 2020 was attended by VKI, DenizBank and the Commission.

6 The referring court later corrected this question so that it refers to point (a) rather than point (b) of Article 63(1) of Directive 2015/2366.

7 At the hearing, the Commission submitted that Directive 2015/2366 placed more emphasis than Directive 2007/64 on the protection of consumers of payment services.

III. Assessment

25. The referring court's four questions can be analysed by changing the order in which they appear and grouping some of them together. Thus:

– In the first place, I shall examine whether the fact that payment cards are NFC-enabled allows that functionality to be classified as a payment instrument (Question 2(a)).

– In the second place, I shall deal with the use of NFC-enabled cards as anonymous payment instruments that cannot be blocked (Question 2(b) and Question 3).

– Lastly, I shall look at the scope for making tacit changes to the terms of framework contracts (Question 1).

26. Although DenizBank has argued that the effects of any judgment unfavourable to its case should be limited in time, such a measure, which neither the referring court nor the other participating parties has even asked for, would not be appropriate in my view. What is more, DenizBank confines itself in this regard to citing general arguments based on the potential financial impact of the judgment but does not adduce any specific evidence to show, as a basis for its exceptional claim, that those concerned acted in good faith and that there is a risk of serious difficulties, as required by the case-law of the Court of Justice. [8]

A. NFC functionality of personalised payment cards as a payment instrument (Question 2(a))

27. The referring court wishes to ascertain whether 'the NFC function of a personalised multifunctional bank card … constitutes a payment instrument' within the meaning of Article 4(14) of Directive 2015/2366.

28. According to that provision, a payment instrument is 'a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order'.

29. As the Court of Justice held in the judgment in *T-Mobile Austria*, [9] payment instruments may be:

– personalised, which is to say that they allow the payment service provider to verify that the payment order was initiated by a user authorised to do so;

– anonymous or non-personalised, in which case the payment service providers are not required to prove that the transaction in question was authenticated.

30. The existence of non-personalised payment instruments means that the concept [of payment instrument] defined in Article 4(14) of Directive 2015/2366 is capable of covering a non-personalised *set of procedures*, agreed between the user and the payment service provider, and used by the user in order to initiate a payment order. [10]

8 According to settled case-law, it is only exceptionally that the Court may, in application of the general principle of legal certainty inherent in the legal order of the European Union, restrict for any person concerned the opportunity of relying on a provision which it has interpreted with a view to calling into question legal relationships established in good faith. Two essential conditions must be fulfilled before such a limitation can be imposed, namely, that those concerned should have acted in good faith and that there should be a risk of serious difficulties (see in particular the judgments of 27 February 2014, *Transportes Jordi Besora*, C-82/12, EU:C:2014:108, paragraph 41; of 19 April 2018, *Oftalma Hospital*, C-65/17, EU:C:2018:263, paragraph 57; and of 3 October 2019, *Schuch-Ghannadan*, C-274/18, EU:C:2019:828, paragraphs 60 to 62).

9 Judgment of 9 April 2014 (C-616/11, EU:C:2014:242; judgment in '*T-Mobile Austria*'), paragraphs 33 and 34.

10 *Ibidem*, paragraph 35.

31. In that same judgment, the Court clarified the doubts prompted by the discrepancy in the use of the adjective 'personalised' as between the various language versions of Article 4(23) of Directive 2007/64,[11] the content of which is practically identical to that of the current Article 4(14) of Directive 2015/2366.

32. It is only the German version that defines payment instrument by using the term 'personalised' as a descriptor for both a device and a set of procedures.[12] In the light of the other versions and the objectives of Directive 2015/2366, it must be agreed that the definition of payment instruments allows for personalised and depersonalised or anonymous varieties.[13]

33. It is true, as the Portuguese Government notes, that bank cards are not expressly classified as payment instruments by Directive 2015/2366. Nonetheless, Annex I(3)(b) thereto defines a payment service as the 'execution of payment transactions through a payment card or similar device'.

34. Furthermore, Article 2(15) of Regulation (EU) 2015/751[14] defines 'payment card' as a 'category of payment instrument that enables the payer to initiate a debit or credit card transaction'.

35. Article 2(7) of that same regulation defines 'card-based payment transaction' as 'a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services'.

36. Those provisions of Directive 2015/2366 and Regulation 2015/751 (which are closely linked legislative texts) support the inference that payment cards are payment instruments within the meaning of that directive. It follows that a multifunctional bank card such as that issued by Denizbank may be regarded as a payment instrument that is subject to Directive 2015/2366.

37. Cards of this kind have a twofold nature or functionality:

– first, they are linked to a specific and clearly identifiable customer, so that they can be used as personalised payment instruments where the customer of the banking institution authorises the latter to pay the payee by entering a PIN or providing a signature. What is more, use of the bank card as a personalised payment instrument in this way may be established as being the only way in which the card can be used to make any payment transactions. There is no question, in my opinion, that bank cards featuring this single functionality are subject to the rules of Directive 2015/2633 and the provisions implementing it;

– secondly, they may have additional functionality in the form of NFC capability, as do the bank cards issued by DenizBank. The NFC functionality which such credit and debit cards feature allows a purchase to be made by means of the radio frequency identification technology that is embedded in the card itself. Customers make a payment by holding the card near to a point of sale

11 The Court of Justice states that, in all language versions, the adjective 'personalised' describes the phrase 'a device(s)'. However, in the French version ('tout dispositif personnalisé et/ou ensemble de procédures'), which is the same as, inter alia, the Spanish, Italian, Hungarian, Portuguese and Romanian versions, the adjective 'personalised' does not describe the phrase 'set of procedures'. In contrast, in the German version ('jedes personalisierte Instrument und/oder jeden personalisierten Verfahrensablauf'), the adjective 'personalised' describes the phrase 'set of procedures'. The English version ('any personalised device(s) and/or set of procedures'], which is the same as, inter alia, the Danish, Greek, Dutch, Finnish and Swedish versions, lends itself to both readings' (judgment in *T-Mobile Austria*, paragraph 31, as well as the Opinion of Advocate General Wathelet, delivered in the same case (EU:C:2013:691, point 36).

12 It may be that the divided opinion on this issue among the Austrian courts is in large part down to the literal wording of the German version of Article 4(23) of Directive 2007/64 ('jedes personalisierte Instrument und/oder jeden personalisierten Verfahrensablauf').

13 Judgment in *T-Mobile Austria*, paragraph 35 *in fine*: '… the concept of payment instrument defined in Article 4(23) of the directive is capable of covering a non-personalised set of procedures, agreed between the user and the payment service provider, and used by the user in order to initiate a payment order'.

14 Regulation of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (OJ 2015 L 123, p. 1).

terminal, without needing to run it through a swiper. Wireless communication between the NFC-enabled card and the point of sale terminal is sufficient to validate the transaction, irrespective of who is in possession of the card at the time, and dispenses with the need for the cardholder to enter his PIN or provide a handwritten signature.[15] This is therefore a depersonalised or anonymous payment procedure.

38. The NFC functionality of a personalised multifunctional bank card falls within the category of a non-personalised *set of procedures* agreed between the payment service provider and the user, who uses them to initiate a payment order, within the meaning of Article 4(14) of Directive 2015/2366.

39. The ability to make a payment is subject only, as I have already said, to possession of an NFC-enabled card. Such a card could therefore be used by any third party, even an unauthorised one. That significant risk explains why the NFC functionality embedded in the card works only for small payments up to a low-value threshold (in this case, EUR 25).

40. As I have just noted, anonymous payment instruments take the form of a non-personalised *set of procedures* 'agreed' between the payment service provider and the user. It falls to the referring court to verify whether such an agreement existed in this case, since, according to VKI, Denizbank activates the personalised multifunctional bank card's NFC functionality automatically, even without the user's consent.[16]

41. Classifying a personalised multifunctional bank card's NFC functionality as an anonymous payment instrument is the solution most consistent with a purposive interpretation[17] of Article 4(14) of Directive 2015/2366 and coincides with the objectives of that directive as described in recitals 5 and 6 thereof.

42. After all, *enhanced* protection for consumers (users of NFC-enabled cards) and the promotion of fair and transparent competition between the financial institutions that issue such cards plead in favour of their classification as payment instruments subject to Directive 2015/2366. As such, they would benefit from the guarantees which the directive itself lays down in order to increase the level of consumer confidence in a harmonised payments market.

43. The same assessment can also be inferred from Article 11 of Delegated Regulation (EU) 2018/389,[18] which governs 'contactless payments at point of sale' as a means of facilitating the development of user-friendly and low-risk payment services.[19]

15 On the use of contactless payment instruments, I refer to the analyses conducted by the European Central Bank, *Card payments in Europe — current landscape and future prospects: a Eurosystem perspective*, 2019 (https://www.ecb.europa.eu/pub/pubbydate/2019/html/ecb.cardpaymentsineu_currentlandscapeandfutureprospects201904~30d4de2fc4.en.html#toc1), and the European Cards Stakeholders Group, *Feasibility Study on the development of open specifications for a card and mobile contactless payment application*, 2017 (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/7th-ERPB-meeting/Annex_to_Stat_past_ERPB_Recommendations_ECSG_Interim_Report_contatless_feasibility_study_and_progress_indicators.pdf?115946678f056d5ccc9eba5f72cb4a88).

16 At the hearing, DenizBank was not entirely successful in rebutting VKI's claim to this effect. It confirmed that, in some cases, a user receiving the card by post (which is, it said, its usual method of delivery) may not be aware that the card features activated NFC functionality.

17 The Court of Justice has used the teleological criterion to interpret other concepts under Directive 2007/64, the predecessor to Directive 2015/2366. See judgments of 25 January 2017, *BAWAG* (C-375/15, EU:C:2017:38, paragraphs 40 to 45), on the concept of 'durable medium' within the meaning of Article 4(25) of Directive 2007/64; of 22 March 2018, *Rasool* (C-568/16, EU:C:2018:211, paragraphs 30 to 39), concerning the concept of 'payment service' within the meaning of Article 4(3) of Directive 2007/64; and of 4 October 2018, *ING-DiBa Direktbank Austria* (C-191/17, EU:C:2018:809), on the concept of 'payment account' within the meaning of Article 4(14) of Directive 2007/64.

18 Commission Delegated Regulation of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJ 2018 L 69, p. 23).

19 Recital 11 of Delegated Regulation 2018/389.

44. According to that provision, payment service providers are to be allowed not to apply strong customer authentication [20] where the payer initiates a contactless electronic payment, provided that the following conditions are met:

(a) the individual amount of the transaction does not exceed EUR 50; and

(b) the cumulative amount of previous transactions from the date of the last application of strong authentication does not exceed EUR 150; or

(c) the number of consecutive contactless electronic payment transactions since the last application of strong authentication does not exceed five.

45. Owing to their very nature, payments made through the use of an anonymous payment instrument (such as an NFC-enabled payment card) are not subject to the obligation of strong customer authentication, [21] an exemption [22] from which other instruments also benefit. [23]

46. The Czech Government, however, submits that the payment instrument is the personalised multifunctional payment card itself, and takes the view that NFC functionality is merely one of the ways in which such a card can be used. That card is not an anonymous payment instrument but can simply be used, less securely, for low-value payments authenticated through NFC technology (that is to say, without the need for the card holder to employ a security element such as his signature or PIN).

47. I do not share that view. In my opinion, as I have already explained, cards of the type issued by DenizBank feature two different payment instruments, namely:

– a *personalised* device which requires the use of one or two security elements (strong authentication) and is reserved for payments from a certain value;

– a *set of procedures* for making low-value payments without using those security elements, via NFC functionality.

48. The principle of technological neutrality, which informs various provisions of Directive 2015/2366 and to which recital 21 thereof refers, [24] suggests that two functionalities possessed by a single bank card in this way should be regarded as two separate payment instruments.

20 According to Article 4(30) of Directive 2015/2366, 'strong customer authentication' is 'an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data'. The strong authentication thus established in order to enable the delivery of electronic payment services that are more secure for consumers and more respectful of their personal data translates ultimately into the use of at least two of the aforementioned security elements: something only the user knows, such as a password or numerical code; something belonging to the user, such as his mobile telephone; and something inherent in the user, such as his voice or his fingerprints.

21 Recital 8 of Delegated Regulation 2018/389.

22 The 'exemptions' from the principle of strong customer authentication are laid down in Delegated Regulation 2018/389, as part of its implementation of Article 97 of Directive 2015/2366, on the basis of the level of risk, the amount, the recurrence and the payment channel used for the payment transaction.

23 Articles 10 to 18 of Delegated Regulation 2018/389 provide for other exemptions from strong authentication, in cases of payment account information, unattended terminals for transport fares or parking fees, trusted beneficiaries, recurring transactions, credit transfers between accounts held by the same natural or legal person, low-value transactions and secure corporate payment processes and protocols.

24 'The definition of payment services should be technologically neutral and should allow for the development of new types of payment services, while ensuring equivalent operating conditions for both existing and new payment service providers'.

49. This is the case because the traditional instrument (the classic personalised payment card)[25] has here recently been supplemented with another, NFC functionality, which is a different payment instrument subject to a distinct legal regime. The physical medium is identical (the card issued by the banking institution) but that medium now features two different payment instruments.

50. This, as I have already said, is the interpretation most in keeping with the principle of technological neutrality underpinning Directive 2015/2366, the provisions of which must not hamper the development of new payment instruments and services as and when advances in technology make this possible. Nothing must stand in the way of cards being equipped in future with other payment instruments additional to the personalised and NFC functionalities which they are already able to feature.

51. In short, a personalised multifunctional payment card's NFC functionality must be classified as a payment instrument within the meaning of Article 4(14) of Directive 2015/2366.

B. Use of NFC-enabled cards as anonymous and unblockable payment instruments (Question 2(b) and Question 3)

52. The referring court asks whether, in the case where a contactless low-value payment is made using an NFC-enabled card, 'the payment instrument is used anonymously' for the purposes of the *derogation* provided for in Article 63(1)(b) of Directive 2015/2366.

53. By its third question, it wishes to ascertain further whether those circumstances are covered by Article 63(1)(a) of that directive, which provides for another *derogation* similar (but not identical) to the one mentioned above, in the case where 'the payment instrument does not allow its blocking or prevention of its further use'.

54. Article 63 of Directive 2015/2366 establishes a number of derogations for low-value payment instruments (and for electronic money, although this is not relevant here), whereby certain 'rights and obligations in relation to the provision and use of payment services', as provided for in Title IV, do not apply.

55. Article 63(1) focuses on certain very specific payment instruments: those 'which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time'.

56. In those cases, payment service providers may agree with their users not to apply certain rights or certain obligations to which other provisions of Directive 2015/2366 refer:

– where the payment instrument 'does not allow its blocking or prevention of its further use' (paragraph 1(a)), the parties to the contract may not apply Article 69(1)(b);[26] Article 70(1)(c) and (d);[27] and Article 74(3);[28]

25 A payment card may also feature two distinct functionalities where it can be used as a credit card and as a debit card, meaning that a single bank card contains two personalised payment instruments.

26 User's obligation to notify the payment service provider of the loss, theft, misappropriation or unauthorised use of the payment instrument.

27 Payment service provider's obligation to make available means enabling the user to request unblocking of the payment instrument.

28 No economic liability on the part of the payer after notification for the loss, theft or misappropriation of the payment instrument.

– where the payment instrument 'is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised' (paragraph 1(b)), the parties to the contract have the right not to apply Article 72,[29] Article 73[30] and Article 74(1) and (3).[31]

1. Obligations on the issuing institution in the case where cards are not amenable to blocking or prevention of further use

57. The first derogation (Article 63(1)(a)) introduces a system of 'attenuated' liability on the part of the banking institution issuing the payment card.

58. If that card is not amenable to blocking or prevention of its 'further use' (for example, in cases of abnormal use through loss, theft, misappropriation or unauthorised use), the banking institution may agree with its customers that it is not to bear the general obligations laid down in the Directive to enable the card to be blocked and its further use prevented in the event of abnormal use.

59. As the referring court rightly notes, a banking institution issuing an NFC-enabled card will be able to avail itself of that derogation only if it can demonstrate that it is not *technically feasible* to block that card or prevent its further use in the abovementioned circumstances. The burden of proving that these measures are impossible therefore lies with the banking institution, since the derogation must be interpreted strictly.

60. The referring court is also right to make the further point that, if the banking institution were not required to show that the card is unblockable, it would only have to market a technically mediocre card (which cannot be blocked at all) in order to adversely affect the interests of consumers by making them bear the risk arising from any unauthorised payments.

61. I concur with those assessments, since the exemption from liability would otherwise be contrary to recital 91[32] and Article 73 of Directive 2015/2366, which impose on the payment service provider the obligation to guarantee the security of payments and assume liability (albeit subject to a minor limitation) for unauthorised payment operations.

62. While it is for the referring court to verify that this is the case, everything would indicate that the state of technical knowledge is such that a banking institution can block a personalised multifunctional payment card.[33] Certain provisions of the Directive (Articles 69, 70 and 74, among others) take that capability as read. The addition of NFC functionality to such cards does not therefore appear to preclude their amenability to blocking.

63. If that is the case, a clause in a framework contract which, like that pre-inserted by DenizBank (clause 18), states that 'it is technically impossible for the debit card to be blocked when used for low-value transactions' (and provides that certain amounts unduly paid in the event of the loss or theft of that card are non-refundable) would be contrary to Article 63(1)(a) of Directive 2015/2366.

29 Payment service provider's obligation to prove that payment transactions have been authenticated and executed.

30 Payment service provider's liability for unauthorised payment transactions.

31 Payer's liability up to a maximum of EUR 50 for any losses resulting from unauthorised payment transactions in the event of loss, theft or misappropriation of the payment instrument, except where the payer has acted fraudulently or failed to fulfil the obligations in relation to appropriate use of the instrument and protection of the security credentials (paragraph 1); and absence of any economic liability on the part of the payer after notification for the loss, theft or misappropriation of the payment instrument (paragraph 3).

32 'Payment service providers are responsible for security measures. Those measures need to be proportionate to the security risks concerned. Payment service providers should establish a framework to mitigate risks and maintain effective incident management procedures …'.

33 DenizBank recognised as much at the hearing, in response to the observations presented by VKI. The latter had submitted that 'almost all Austrian banks, with the exception of the defendant, provide in their general terms and conditions of sale that, after a blocking notification, the card's NFC functionality is required to be and is … blocked' (VKI's written observations, paragraph 5).

2. Liability of the issuing institution where the payment card is used anonymously

64. The referring court wishes to ascertain whether the use of a personalised multifunctional payment card's NFC functionality is an instance of such a card being used 'anonymously' within the meaning of the derogation provided for in Article 63(1)(b) of Directive 2015/2366.

65. That provision, as I have said, establishes a system of attenuated liability on the part of the service provider in the case where the payment instrument is used anonymously or where 'the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised'.

66. As the referring court and the Commission note, the feature common to both scenarios is the inability to demonstrate who actually authorised the payment transaction. That may explain why, in the judgment in *T-Mobile Austria*, the Court of Justice treated the derogation provided for in Article 53(1)(b) of Directive 2007/64 generically and without distinguishing between the aforementioned two situations. [34]

67. The arguments I set out above [35] led me to the view that a personalised multifunctional bank card's NFC functionality falls within the category of an anonymous payment instrument. I would add to those arguments the point that a distinction must be drawn between identification of the card holder (which is always possible because the card is personalised) and authorisation of the payment by the person in possession of the card (who may not be the true card holder in cases of loss, theft, cloning or misappropriation).

68. Payment authorisations using a personalised payment card's NFC functionality require only simple authentication (as demonstrated by mere possession of the card) rather than strong authentication (as would be the case if a PIN had to be entered or a signature provided). Such payment authorisations must therefore be regarded as anonymous, since the issuing institution cannot demonstrate that the payment was indeed authorised by the card holder rather than by a third party having stolen, cloned or misused it.

69. The anonymity of a personalised payment card's NFC functionality has advantages and disadvantages:

– on the one hand, it enables payments to be processed more quickly and is conducive to the development of new payment services and means of payment, in line with the objectives pursued by Directive 2015/2366; [36]

– on the other hand, it creates a risk of improper use of the card which is beyond the control of the card holder and the issuing banking institution. In order to minimise that risk, NFC functionality, as has already been noted, only supports low-value [individual] payments (up to EUR 30) and is always subject to a maximum [total] threshold (EUR 150).

34 Judgment in *T-Mobile Austria*, paragraph 34.

35 Points 36 to 51 of the present Opinion.

36 See recitals 15, 21 and 96 of Directive 2015/2366. In paragraph 28 of the judgment of 21 March 2019, *Tecnoservice Int.* (C-245/18, EU:C:2019:242), the Court took the objectives of automated processing and speed of payment set out in recitals 40 and 43 of Directive 2007/64 as the basis for interpreting Article 74(2) as meaning that it 'limits the liability of both the payer's and the payee's payment service provider, which thus relieves those providers of the obligation to check whether the unique identifier provided by the payment service user does in fact correspond to the person named as the payee'.

70. The balance which Directive 2015/2366 strikes between those margins is to say that, if the holder of a personalised payment card consents to having NFC functionality added to that card, the derogation provided for in Article 63(1)(b) of Directive 2015/2366 will apply. Consequently, any contractual terms that contain that derogation, as clauses 15, 16 and 17 of the DenizBank framework contract appear to do, will be compatible with that directive.

71. In short, a low-value contactless payment using NFC functionality may be classified as an instance of a personalised multifunctional payment card being used 'anonymously' within the meaning of Article 63(1)(b) of Directive 2015/2366.

C. Question 1: tacit change to the clauses of a framework contract

72. The referring court wishes to ascertain whether it follows from Article 52(6)(a) in conjunction with 54(1) of Directive 2015/2366 that a user consents to a change of contractual obligations proposed by the payment service provider simply by not rejecting it.

73. If that interpretation were accepted, the referring court goes on to say, the banking institution could '[agree] [tacit consent] with the consumer for any conceivable contractual conditions without any restriction'.

74. Article 52(6)(a) of Directive 2015/2366 provides that, 'if agreed, … the payment service user will be deemed to have accepted changes in the conditions in accordance with Article 54, unless [he] notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted'. [37]

75. The obligation to provide consumers with precontractual information is one of the key elements of EU consumer protection law. In the context of standard-form contracting, where there is an obvious asymmetry between the payment service provider and consumers, precontractual information helps consumers to make well-founded decisions. It also protects their contractual autonomy, enables them to compare the offers available on the market and promotes transparency in the execution of contracts. [38]

76. Directive 2015/2366 reflects that position both in its recitals (in particular recital 59) [39] and in Articles 51 to 54. [40]

77. Article 51 governs the form and procedure for providing precontractual information to payment service users. Article 52 sets out the content of the detailed and precise information that the provider must make available to the user. [41]

37 In this event, the payment service user is entitled to terminate the framework contract at no cost and with effect from any point prior to the date on which the change would have become applicable.

38 In specialist literature, doubts have been expressed as to whether providing this kind of information is of *real* use in the financial sector. For some, the ideal solution would be to regulate contractual conditions *ex ante* rather than to improve the prior information itself. See, for example, Alfaro, J. 'Providing information to less sophisticated — that is to say, less well-educated — consumers is of no benefit to them, because the cost to them of understanding, processing and understanding the consequences of the information supplied to them is high, so high as to mean that investing time and effort in trying to understand it, even if it is provided to them voluntarily by banks, is unreasonable, with the result that that information does not lead to "better choices" on the part of such less sophisticated consumers'. Blog https://derechomercantilespana.blogspot.com, entry of 25 November 2018 entitled *No todos los prestatarios son iguales: lecciones para el legislador*.

39 Provision should be made 'for the right of consumers to receive relevant information free of charge before being bound by any payment service provider. Consumers should also be able to request prior information as well as the framework contract, on paper, free of charge at any time during the contractual relationship, so as to enable them both to compare the services and conditions offered by payment service providers and, in the case of any dispute, to verify their contractual rights and obligations, thereby maintaining a high level of consumer protection'.

40 The same was true of Directive 2007/64, as was highlighted by the judgment of 25 January 2017, *BAWAG* (C-375/15, EU:C:2017:38, paragraph 45).

41 That information covers, inter alia, use of the payment service, charges, interest and exchange rates, communication between the parties, safeguards and corrective measures, redress, and changes to, and termination of, the contract.

78. One component of that information is that relating to changes to the framework contract, as provided for in Article 52(6)(a) of the Directive, which I reproduced earlier. The provider and the user of the payment service may, exceptionally, agree on tacit consent to changes to the contractual conditions ('if agreed').

79. Clause 14 of DenizBank's framework contract with its customers provides for that possibility. It allows for the tacit acceptance of changes proposed (and communicated) by the bank, on the understanding that customers will be deemed to have consented to such changes if they have not objected to them. [42]

80. According to DenizBank, tacit acceptance, which is permitted by Article 52(6)(a) of Directive 2015/2366, extends to *any type of contractual change*. In its opinion, it is unrealistic to expect, and difficult to persuade, payment service users to give express consent to changes to a contract such as that governing the legal rules applicable to a personalised multifunctional bank card.

81. According to DenizBank, tacit acceptance of changes is an indispensable mechanism of the banking business model. It should not operate to the detriment of consumers, since it makes it easier and quicker for them to access improvements to its payment instruments and to benefit from new advances in technology, such as the addition of NFC functionality to its cards.

82. In my opinion, the possibility of providing for the tacit acceptance of changes to contractual conditions, as allowed for in Article 52(6)(a) of Directive 2015/2366 if agreed between the user and the provider of the payment service, should be interpreted restrictively in the case where the content of such changes is unfavourable to the customer.

83. That possibility remains an exception to the general principle that, in common with the original conditions, changes to the framework contract require the user's express acceptance.

84. That strict interpretation is borne out by the objectives of Directive 2015/2366 (prominent among which is consumer protection) and the schematic location of Article 52(6)(a) among the provisions on the precontractual information which the payment service provider must provide to users in any event in order to offset the disadvantageous position in which the latter find themselves. The asymmetry of information to which I have referred is present both when users give their initial consent to the conclusion of the framework contract and when they accept subsequent changes to it.

85. I agree with the referring court and the Commission that any tacit acceptance cannot be extended to *all* of the framework contract's conditions. That would have the effect, in practice, of giving the payment service provider the absolute and, to all intents and purposes, unilateral power to change that contract: experience shows that most consumers carry out no critical analysis of proposed changes to the conditions of their contracts, in particular if those changes are in any way technically or legally complex.

86. At the hearing, DenizBank acknowledged that the use of tacit acceptance for substantial changes to contractual conditions does not form part of its banking practice. It did not, however, convincingly explain why it does not bring clause 14 of the framework contract into line with that practice and limit the use of tacit acceptance to the least significant changes to the contractual relationship.

42 That clause sets out the conditions governing the communication of the proposal, on paper or another durable medium, the required period of notice ahead of its entry into force, the time limit for tacit consent and the opportunity for the user to object to the change and terminate the framework contract.

87. The possibility of providing for the tacit acceptance of changes could, in my opinion, be available only for non-essential changes to the clauses of a framework contract, provided that the safeguards established in Directive 2015/2366 are respected. [43]

88. As I have already explained, giving a personalised multifunctional payment card NFC functionality for the purposes of low-value contactless payments adds a new payment instrument to that card. To the same extent, therefore, such functionality is either a *new* service, which should be the subject of a *new* added contract, or an *essential* change to the conditions of the previous framework contract [44] (which governed relations between the card-issuing institution and the consumer).

89. In both cases (new contract or objective novation of an essential element of the previous contract), the consumer, once informed of the advantages and risks associated with his card's NFC functionality, must unequivocally give his explicit consent to that payment instrument, a requirement which is not compatible with tacit acceptance.

IV. Conclusion

90. In the light of the foregoing, I propose that the Court's answer to the Oberster Gerichtshof (Supreme Court, Austria) should be as follows:

(1) The near field communication (NFC) functionality of a personalised multifunctional payment card must be classified as a payment instrument within the meaning of Article 4(14) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

(2) The making of low-value contactless payments using the NFC functionality of a personalised multifunctional payment card constitutes an instance of that card being used 'anonymously' within the meaning of Article 63(1)(b) of Directive 2015/2366.

(3) A banking institution issuing a personalised multifunctional payment card to which NFC functionality has been added may avail itself of the derogation provided for in Article 63(1)(a) of Directive 2015/2366 only if it can demonstrate that it is not technically feasible to block that card or prevent its further use in the event of loss, theft, misappropriation or unauthorised use.

(4) The possibility of tacit acceptance of changes to the framework contract, which is permitted under Article 52(6)(a) of Directive 2015/2366 where agreed between the user and the provider of the payment service, must be strictly interpreted and may not be applied to changes to the essential elements of that framework contract, such as ones relating to the addition of NFC functionality to a payment card.

43 In the order for reference (page 12), the referring court sets out its case-law, as reflected in a number of judgments (1Ob 210/12g; 2Ob 131/12x; 8Ob 58/14h; 9Ob 26/15m; 10Ob 60/17x), on the limits attaching to the tacit acceptance of contractual conditions. At the hearing, VKI also referred to the judgment of the Bundesgerichtshof (Federal Court of Justice, Germany) of 11 October 2007 (III ZR 63/07), which the Oberster Gerichtshof (Supreme Court) had itself cited in paragraph 2.20 of its judgment of 11 April 2013 (ECLI:OGH002:2013:0010OB00210.12G.0411.000) in order to confirm that the 'fiction of acceptance' (tacit acceptance) cannot extend to substantial contractual changes.

44 According to Article 4(21) of Directive 2015/2366, 'framework contract' means 'a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account'.