Case C-448/21

Request for a preliminary ruling

Date lodged:

21 July 2021

Referring court:

Tribunal Judicial da Comarca do Porto – Juízo Central Cível (Portugal)

Date of the decision to refer:

5 February 2021

Applicant:

Portugália – Administração de Patrimónios, SGPS, S.A.

Defendant:

Banco BPI, S.A.

Tribunal Judicial da Comarca do Porto (District Court, Porto, Portugal)

Oporto – JC Cível (Central Civil Section) – Juiz 5 (Court No 5)

[…] 5.º Juízo Central Cível do Porto do Tribunal Judicial da Comarca do Porto, Portugal [District Court, Porto (Portugal), Central Civil Section, Court No 5]

Applicant: Portugália – Administração de Patrimónios, SGPS, S.A., with registered office in Lisbon, Portugal […]

Defendant: BANCO BPI, S.A., with registered office in Porto, Portugal […]

REQUEST FOR A PRELIMINARY RULING

Interpretation of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015

[Article 267(1)(b) and (2) of the Treaty on the Functioning of the European Union]

The District Court, Porto – Central Civil Section – Court No 5 asks the COURT OF JUSTICE OF THE EUROPEAN UNION to give a preliminary ruling on the questions set out below concerning the interpretation of Articles 61, 72, 73 and 74 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, because it considers a ruling is needed in order to reach a decision in the case before it.

[…]

A. Questions referred to the Court of Justice of the European Union

For the purposes of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 ('the Directive'):

I. Does the execution, involving human intervention on the part of the payment service provider, of a payment order which is set down on paper, scanned and sent to the payment service provider by email from an email account created by the user, constitute a 'payment transaction' for the purposes of Article 73(1) of the Directive?

II. Must Article 73(1) of the Directive be interpreted as meaning that:

II.I. Without prejudice to the provisions of Article 71 or to duly notified reasonable suspicion of fraud, is a mere notification that a payment transaction was not authorised, without any supporting evidence, sufficient to give rise to an obligation (on the part of the payment service provider) to provide a refund (to the payer)?

II.II. If the answer to the preceding question is in the affirmative, is it possible to exclude the rule that a mere notification by the payer is sufficient by disapplying the rules on the burden of proof contained in Article 72 of the Directive by agreement between the parties (payer and service provider), as permitted by Article 61(1) of the Directive?

II.III. If the answer to the preceding question is in the affirmative, is the payment service provider under an obligation to reimburse the payer immediately only if the latter demonstrates that the transaction was not authorised in a situation where, following the exclusion of the application of Article 72 of the Directive, the applicable legislative or contractual rules require the payer to provide such evidence?

III. Does Article 61(1) of the Directive not only permit the disapplication of the provisions in Article 74 of the Directive but also, by agreement between the user (who is not a consumer) and the payment service provider, permit the rules that have been excluded to be replaced by ones that place a greater burden of liability on the payer, in particular as an exception to the provisions of Article 73 of the Directive?

B. Summary of the subject matter of the proceedings

1 The applicant, Portugália, SGPS, S.A. ('Portugália'), has a bank account with the defendant entity, Banco BPI, S.A ('Banco BPI'). Portugália has filed a claim against the bank for the sum of EUR 2 500 000 plus interest.

2 Portugália maintains that Banco BPI performed an unauthorised transfer of the aforementioned sum from its bank account.

3 In its defence, Banco BPI states that the transaction was carried out in accordance with the instructions received by email.

C. Summary of the relevant facts

4 Portugália, a public limited company with profits of EUR 9 039 882.33 in 2018, holds a current account with Banco BPI, a credit institution which is on the register held by the Bank of Portugal.

5 Portugália asked Banco BPI to permit it to carry out transactions from its bank account by sending orders to Banco BPI by email.

6 In January 2018 the parties concluded a written agreement to authorise the execution of instructions given by fax or email in respect of the applicant's bank account. The agreement was as follows:

6.1. 'Portugália – Adm de Patrimónios, SGPS, S.A. … authorises Banco BPI, S.A., to execute … all manner of transactions … issued by the former by fax or email … in respect of the accounts identified below which it holds with Banco BPI, S.A..'

6.2. 'For these purposes, Portugália – Adm de Patrimónios, SGPS, SA authorises Banco BPI, S.A., […] b) Not to execute instructions sent by email which are not accompanied by a scanned copy of the instruction duly bearing the valid signature(s) and having sufficient authority to perform account transactions.'

6.3. 'Portugália – Adm de Patrimónios, SGPS, SA accepts … that the liability of Banco BPI, S.A., shall be limited to verifying that the requirements defined above are satisfied …. Portugália – Adm de Patrimónios, SGPS, SA, assumes all liability and all consequences arising from unauthorised, abusive or fraudulent use … of email, and shall bear all damage and loss resulting from the execution of instructions in relation to its account(s) which have been forged or distorted in any way or which do not come from the account holder(s). … The Bank accepts no liability for any damage or loss arising from the use … of email, including damage or loss caused by delays, losses, intrusions, distortions or misunderstanding of the information sent, and by the forging of signatures or documents.'

7 The email account created by Portugália is protected by a password set by Portugália and is not part of the electronic banking service established by Banco BPI.

8 Banco BPI had no involvement in the creation of Portugália's email account, did not provide any user access authorisation and does not host the account on its servers.

9 On 25 March 2020 a third party gained unauthorised access by unidentified means to Portugália's email account and used it to send a transfer order to Banco BPI's services for the sum of EUR 2 500 000.00.

10 The transfer order of 25 March 2020, which was not authorised by Portugália, was executed by Banco BPI's administrative services, after the Bank had compared the signatures on the instruction it had received with the manuscript signatures of Portugália's representatives held in its computer system.

D. Content of national provisions applicable to the case

11 Article 100(2), Article 113(1) and (3) and Article 114(1) and (2) of Decree-Law No 91 (Legislative Decree No 91/2018) of 12 November 2018 (which transposes the Directive into domestic law) in particular are applicable to the present case.

12 These articles reproduce, with no significant changes, Articles 61, 72, 73 and 74 of the Directive, [1] and therefore it is not considered necessary to reproduce them here.

[…]

13 […]

14 […]

15 […]

16 […]

F. Reasons for doubts over the interpretation of the Directive

F.1. Preliminary observations – The proceedings in the context of the Directive

17 The defendant argues that the rule laid down in Article 73(1) does not apply to payment transactions carried out by means of 'payment instruments' that involve an intervening action (to execute the order) by the payment service provider in the

[1] Unless otherwise specified, all citations of articles are to be understood to refer to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.

form of (human) intervention by its employees […]. It also maintains that, where the user is neither a 'consumer' nor a 'microenterprise', the parties may establish by contract that the rule in Article 73(1) of the Directive is not to apply […].

18 It seems that, for the purposes of the Directive, the service provided by the service provider, as described above — that is, the execution, by an employee of the service provider, of orders sent by email, on the basis of a prior agreement which permits instructions to be sent by this means — is a 'payment service' which falls within the scope of Article 4(3) (and point 3 of the Annex) and is not covered by any of the exclusions provided for in Article 3 of the Directive.

19 Article 4(5) clearly includes within the meaning of 'payment transaction' the execution by the service provider of a transfer of funds in accordance with an order given by the client by email sent from a personal email account created by the customer (without the provider's involvement). This conclusion is supported by the wording of the final part of Article 4(13), which addresses the concept of 'payment order'.

20 The procedure adopted by the parties can be accepted as a 'payment instrument' for the purposes of Article 4(14). It is true that a simple instruction sent by personal email is not a 'physical device' or a special 'set of procedures' specifically designed for sending payment orders or for any other purpose of the business relationship between the user and the provider [see question 34 in the document entitled *Your questions on PSD*, published by the European Commission (https://ec.europa.eu/)]. However, if the parties establish that the instruction is only *properly* issued if it is set down on paper, signed by the payer's representatives in their own hand, and then scanned and sent to the service provider, it constitutes a procedure which can come within the concept of 'payment instrument'. With regard to this concept, in the light of the [first Payment Services Directive], the Court of Justice has already stated that 'Article 4.23 of Directive 2007/64 must be interpreted as meaning that both the procedure for ordering transfers by means of a transfer order form signed by the payer in person and the procedure for ordering transfers through online banking constitute payment instruments within the meaning of that provision' (judgment of the Court of Justice of 9 April 2014, *T-Mobile Austria*, C-616/11, EU:C:2014:242, paragraphs 29 to 44).

21 It can be seen from Article 64(1) and the second subparagraph of Article 64(2) that a payment transaction is considered to be 'unauthorised' where it is carried out by someone who is not authorised (in that he is not the payer or someone authorised by the payer). If the user whose email account has been accessed unlawfully does not authorise the transaction that has been ordered, it appears that the transaction should be classed as an 'unauthorised payment transaction' (see judgment of the Court of Justice of 11 April 2019, *Mediterranean Shipping Company*, C-295/18, EU:C:2019:320, paragraphs 43 and 54).

22 While it is clear that it is for the service provider to prove *authentication*, it is not clear that it is for the service provider to prove *authorisation* (authorship of the order), even if this appears to be the solution provided for by Articles 4(29), 72(1) and 73(1), and also (*a contrario*) by Article 63(1)(b): where a user denies having authorised an executed transaction, the service provider bears not only the burden of proving formal authentication of the transaction — in other words, in cases such as the present one, of proving that the 'valid signatures' were compared (and were similar) — but also the burden of proving that the transaction was actually authorised by the payer (or of fraud, wilful misconduct or gross negligence on the part of the user).

F.2. First question referred: applicability of Article 73(1) of the Directive

23 It appears that, in Articles 73 and 74, the EU legislature ascribed the risk of the losses arising from the execution of an unauthorised transaction to the person who is able to control the risk. The notion of controlling the risk (by controlling the payment service) also seems to be present, for example, in the rules laid down in Article 68(2), Article 69(1)(a), Article 69(2), Article 70(1)(a), (c) and (e), and Article 70(2).

24 In itself, controlling the source of the risk explains the (almost) *automatic* attribution of the losses from an 'unauthorised payment transaction' to the service provider only where the transaction is executed using an *automated* 'payment service' established by the service provider, which includes the allocation of 'security credentials'. This is thus the situation in cases involving a 'remote payment transaction' or the use of a bank card, in which, since user activity is excluded, the processing of the payment is thus completely automated (with no human intervention on the part of the payment service provider).

25 In the context of 'online banking' services (telebanking or home banking), the solutions offered by Articles 73 and 74 are understandable. The banking institution controls the risk inherent in the use of the electronic platform which it itself has *established — the institution owns the platform, is responsible for managing it and owns the server on which it is installed* — and which its customers can access remotely, via the internet, using access credentials *supplied by the institution*, thus enabling customers to perform transactions, for example, *directly* — that is, without any human intervention on the part of the bank. The customer already largely controls the risk of unlawful access to his or her access credentials, to which Article 4(31) refers.

26 This distribution of risk also applies, for example, to the execution of transactions using bank cards protected by personalised security devices.

27 The execution, entailing human intervention by employees of the service provider, of a payment order that is signed, scanned and sent by email from an email account belonging to the payer, is substantially different from the cases of 'online banking' and use of a bank card described above. In this type of execution, the

payment instrument and security credentials are neither supplied nor controlled by the service provider. They are created, and essentially controlled, by the user; and it is the user who, for example, creates his or her email account, defines the level of security of the chosen password, determines the level of security of the devices used to access his or her email account and chooses the (fixed or mobile) networks used to access the internet.

28 Where a 'payment transaction' is preceded by a 'payment order' that has been *duly authenticated* in accordance with the 'payment instrument' adopted by the parties, and there is an intervening action, performed by a human (to execute the order), on the part of the payment service provider (that is, by its 'physical' employees), the substantive defect of lack of authorisation necessarily has its origin in at 'payment order' stage (which is entirely controlled by the payer), rather than at the stage where the service provider executes that order. Consequently, being best placed to control *the source* of the risk does not appear to be enough, on its own, to explain the possible application of the provisions of Article 73(1) in cases such as the present one.

29 The question that arises is, therefore, whether Article 73(1) attributes liability for unauthorised payment transactions to the payment service provider *where the provider is not best placed to control the source of the risk*.

30 In that connection, it must be recognised that certain users of payment services are also in a position to 'assess the risk of fraud and take countervailing measures' appropriately (see recital 73 to the Directive), and the notion that it is the service provider who benefits most from using the 'payment instrument' is not valid where that instrument requires human intervention by its employees in order to execute the orders, as the process is inevitably slower and more costly.

31 However, it is also possible that the EU legislature deliberately attributed a level of liability that is disproportionate to the risk controlled by the service provider in order to provide an element of compulsion, with the aim of 'promoting the issuance of safer instruments' (which, as noted in recital 34, is one of the objectives of Directive No 2007/64/EC of the European Parliament and of the Council of 13 November 2007).

32 If the view is taken that Article 73(1) was not designed for cases such as the present one and does not apply to such cases, the liability of those involved must be assessed in the light of domestic law and, in particular, liability for the damage and loss resulting from the transaction is to be attributed to one or both parties in the light of the court's assessment of their specific conduct.

F.3. Second question referred: conditions for an immediate refund and amendments to those conditions

33 The first part of Article 73(1) is a rule on civil liability for losses arising from an unauthorised transaction. But this rule also establishes, or deems it to be

established by preceding provisions (that is, by Article 72), that (without prejudice to Article 71 and to the possible existence of reasonable grounds for suspecting fraud), in order for the service provider to be required to reimburse the payer immediately, *the payer is required only to notify (claim) that the payment transaction was unauthorised*, not to demonstrate (*prove*) that this is so.

34 In the light of that legal framework, the question arises whether, where the rule on civil liability for the losses arising from the unauthorised transaction continues to apply unchanged — with the payment service provider being liable for the losses suffered by the payer — the rule (also laid down in Article 73(1)) that the obligation to refund arises *immediately* (albeit without prejudice to subsequent demonstration of the existence of fraud, wilful misconduct or gross negligence on the part of the payer — *solve et repete*) on the mere notification (claim) by the payer that a payment transaction was not authorised is excluded as a consequence of the disapplication of the rules on the burden of proof in Article 72 by agreement between the parties, as permitted by Article 61(1).

35 Therefore the question that arises is whether, even though Article 61(1) does not mention Article 73, the disapplication of the rules on the burden of proof established by Article 72 means that the payment service provider is required to reimburse the payer immediately only where (without prejudice to the provisions of Article 71 and to the possible existence of reasonable grounds for suspecting fraud) the payer *first* provides evidence to show that the transaction was not authenticated and that he or she did not authorise the transaction, provided that, once the application of Article 72 has been excluded, the rules that then apply (by virtue of another valid legal or contractual provision) require the payer to provide such evidence.

F.4. Third question referred: contractual limitation of the provider's liability

36 The second question posed by the defendant concerning the derogation from the rules established in Article 73(1), now as a consequence of the exclusion of the application of Article 74 by agreement between the parties, leads to the assertion that the rule in Article 61(1) not only permits such an exclusion but also allows the excluded legal provisions to be replaced by contractual provisions which place a *greater burden* of liability on the payer.

37 It is true that the wording of Article 61(1) establishes only that the user and the payment service provider may agree that Article 74 '[does] not apply in whole or in part'. Viewed in that light, it could be said that the provision in question only allows the parties to exclude the application of the rules (grouped together in Article 74) that establish the payer's liability, and that the other rules remain in place, meaning that it only permits the parties to reach an agreement *that benefits the payer* (by wholly or partially eliminating the legal source of its liability). For example, under this interpretation, Article 61(1) would provide the basis for a contractual provision that excluded the obligation on the payer to bear losses up to

the amount of EUR 50 (established in Article 74(1)), but would not allow a provision that increased this amount to EUR 500.

38 It is also true that, as noted in the opening recitals, the Directive provides a high level of protection to users, and particularly to consumers. However, precisely for this reason, the aforementioned interpretation of Article 61(1) contains a contradiction. If the application of Article 74 can be excluded only *to the benefit* of the payer, there is no reason for Article 61(1) to stipulate that an agreement to disapply Article 74 is possible only 'where the payment service user is not a consumer'. There is no reason to prohibit exclusion by contract if it can only operate to the consumer's benefit.

39 When viewed in the context of recitals 53 and 73 to the Directive, this conclusion suggests that the parties can *increase* the payer's liability for unauthorised payment transactions where the payer is not a consumer, thereby limiting the liability on the provider established in Article 73(1).

G. Relationship between the provisions of the Directive and the applicable national legislation

40 There is a direct relationship between the provisions of the Directive and the applicable national legislation, since the latter is contained in Legislative Decree No 91/2018 of 12 November 2018, which transposes Directive (EU) 2015/2366 into domestic law.

41 The just resolution of the dispute requires an interpretation of Article 114(1) and (2) of Legislative Decree No 91/2018, which reproduces the provisions of Article 73 of the Directive, in order to determine whether the rules laid down therein apply to the type of procedure adopted by the parties. The just resolution of the dispute can be achieved only through a correct (and uniform) interpretation of the Directive.

Porto, 5 February 2021

The Judge