Reports of Cases

OPINION OF ADVOCATE GENERAL
SHARPSTON
delivered on 3 September 2015 [1]

Case C-235/14

Safe Interenvios, SA
v
Liberbank, SA
Banco de Sabadell, SA
Banco Bilbao Vizcaya Argentaria, SA
(Request for a preliminary ruling

from the Audiencia Provincial de Barcelona (Spain))

(Prevention of the use of the financial system for the purpose of money laundering and terrorist financing — Directive 2005/60/EC — Customer due diligence measures — Directive 95/46/EC — Protection of personal data — Directive 2007/64/EC — Payment services in the internal market)

1. This dispute involves three credit institutions (Banco Bilbao Vizcaya Argentaria, SA ('BBVA'), Banco de Sabadell, S.A. ('Sabadell') and Liberbank, SA ('Liberbank'); collectively, 'the banks') and a payment institution (Safe Interenvios, SA; 'Safe'). [2] The banks closed accounts Safe held with them because they had concerns about money laundering. Safe claims this was an unfair commercial practice.

2. Questions have arisen as to whether EU law, in particular Directive 2005/60/EC ('the Money Laundering Directive'), [3] precludes a Member State from authorising a credit institution to apply customer due diligence measures to a payment institution. That directive provides for three types of customer due diligence measure (standard, simplified and enhanced) depending on the risk of money laundering or terrorist financing. Standard customer due diligence measures under Article 8 comprise, for example, identifying a customer and obtaining information on the purpose and intended nature of a business relationship. Article 11(1) foresees that simplified customer due diligence will apply when the customers of an institution or person covered by that directive ('a covered entity') are credit and financial institutions (including payment institutions) themselves covered by the Money Laundering Directive. Article 13 requires enhanced customer due diligence in situations presenting a higher risk of money laundering or terrorist financing. Moreover, Article 5 authorises Member States to impose stricter obligations than those laid down in other provisions of the Money Laundering Directive.

3. If a credit institution may be authorised to apply (enhanced) customer due diligence measures to a payment institution which itself is covered by the Money Laundering Directive, the Court is asked for guidance on the conditions under which Member States may provide for that to happen. Does their application depend on a risk analysis and may such measures include requiring a payment institution

1 — Original language: English.

2 — For the definitions of 'credit institution' and 'payment institution' under the relevant EU law, see points 16, 17 and 44 below.

3 — Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ 2005 L 309, p. 15), as last amended by Directive 2010/78/EU of the European Parliament and of the Council of 24 November 2010 (OJ 2010 L 331, p. 120).

to transfer to a credit institution data pertaining to its own consumers and the recipients of the funds transmitted abroad? Those questions also invite the Court to consider Directives 95/46/EC ('the Personal Data Directive'),[4] 2005/29/EC ('the Unfair Commercial Practices Directive')[5] and 2007/64/EC ('the Payment Services Directive').[6]

EU law

Treaty on the Functioning of the European Union

4. According to Article 16(1) TFEU, '[e]veryone has the right to the protection of personal data concerning [him or her]'.

Charter of Fundamental Rights of the European Union

5. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') states that '[e]veryone has the right to the protection of personal data concerning him or her'. In accordance with Article 8(2), '[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

6. Article 52(1) provides that '[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

Money Laundering Directive

7. Recital 5 in the preamble to the Money Laundering Directive explains that measures taken in the field of money laundering and terrorist financing should be consistent with other action undertaken in other international fora and take particular account of the recommendations of the Financial Action Task Force ('FATF'),[7] which constitutes the foremost international body active in the fight against money laundering and terrorist financing. The Money Laundering Directive should be in line with the FATF Recommendations as substantially revised and expanded in 2003 ('the 2003 FATF Recommendations').[8]

4 — Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended in certain respects by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1).

5 — Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ 2005 L 149, p. 22).

6 — Directive 2007/64/EC 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), as amended.

7 — See also point 72 below.

8 — A more recent version dates from February 2012: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations ('the 2012 FATF Recommendations'). Both versions are available on the FATF's website: http://www.fatf-gafi.org/.

8. Recital 10 states that covered entities should identify and verify the identity of the beneficial owner. When doing so, it should be left to them whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

9. Recital 22 recognises that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be that simplified customer due diligence is allowed in appropriate cases.

10. At the same time, according to recital 24, EU legislation should recognise that certain situations present a greater risk. Thus, although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

11. Recital 33 states that disclosure of information as referred to in Article 28[9] should be in accordance with the rules on transfer of personal data to third countries as laid down in the Personal Data Directive and that, moreover, Article 28 cannot interfere with national data protection and professional secrecy legislation.

12. According to recital 37, Member States are expected to tailor detailed implementation to the particularities of the various professions and to the differences in scale and size of the covered entities.

13. Recital 48 states that the Money Laundering Directive respects fundamental rights, observes the principles recognised in particular by the Charter and should not be interpreted and implemented in a manner that is inconsistent with the European Convention on Human Rights.

14. Article 1(1) provides: 'Member States shall ensure that money laundering and terrorist financing are prohibited'. Article 1(2) identifies four types of conduct which, when committed intentionally, are to be regarded as money laundering:

'(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points'.

9 — See point 29 below.

15. In accordance with Article 2(1), the Money Laundering Directive applies to (1) credit institutions, (2) financial institutions and (3) a series of legal and natural persons acting in the exercise of their professional activities. Elsewhere, the Money Laundering Directive refers to these categories as being collectively 'the institutions and persons covered' ('covered entities' in this Opinion).

16. A 'credit institution' is defined in Article 3(1) by reference to the definition of that same term in the first subparagraph of Article 1(1) of Directive 2000/12/EC,[10] and thus means 'an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account'.

17. The definition of a 'financial institution' includes 'an undertaking, other than a credit institution, which carries out one or more of the operations included in points 2 to 12 and points 14 and 15 of Annex I to Directive 2006/48/EC'[11] (Article 3(2)(a)). That list of operations includes, under point 4, '[p]ayment services as defined in Article 4(3) of [the Payment Services Directive]'[12] and, under point 5, '[i]ssuing and administering other means of payment … insofar as this activity is not covered by point 4'. According to the Payment Services Directive, a payment service includes the execution of payment transactions and payment institutions are undertakings providing payment services which otherwise satisfy the requirements under that directive.[13]

18. Article 5 provides that '[t]he Member States may adopt or retain in force stricter provisions in the field covered by [the Money Laundering Directive] to prevent money laundering and terrorist financing'.

19. Chapter II ('Customer due diligence') contains, apart from general provisions on standard customer due diligence (Articles 6 to 10), separate sections on simplified customer due diligence (Articles 11 and 12) and enhanced customer due diligence (Article 13).

20. Under Article 7, covered entities are to apply customer due diligence measures: (a) when establishing a business relationship; (b) when carrying out occasional transactions amounting to EUR 15 000 or more; (c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold; and (d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

21. Customer due diligence measures include: 'identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source' (Article 8(1)(a)); 'identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity …' (Article 8(1)(b)); 'obtaining information on the purpose and intended nature of the business relationship' (Article 8(1)(c)); and 'conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship …' (Article 8(1)(d)).

22. Article 8(2) provides that covered entities may determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to the competent authorities that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

10 — Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions (OJ 2000 L 126, p. 1), as amended.

11 — Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (OJ 2006 L 177, p. 1). This directive repealed Directive 2000/12.

12 — See point 44 below.

13 — The full definition of a 'payment institution' is found in Article 4(4) of the Payment Services Directive: see point 44 below.

23. In accordance with Article 9(1), Member States must, subject to certain exceptions, require that verification of the identity of the customer and the beneficial owner takes place before a business relationship is established or a transaction is carried out.

24. Where a covered entity is unable to comply with Article 8(1)(a) to (c), Member States must, under the first subparagraph of Article 9(5), require that 'it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or [must] terminate the business relationship, and [must] consider making a report to the financial intelligence unit (FIU) in accordance with Article 22 [[14]] in relation to the customer'. Under Article 9(6), Member States are to require that covered entities apply the due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

25. Article 11(1) provides: 'By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), [covered entities] shall not be subject to the requirements provided for in those Articles where the customer is a credit or financial institution covered by this Directive, or a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements'. Article 11(2) sets out other circumstances under which, by way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow covered entities not to apply standard customer due diligence. Under Article 11(3), covered entities must in any case gather sufficient information to establish if the customer qualifies for an exemption as mentioned in paragraphs 1 and 2. [15]

26. Pursuant to Article 13(1), in addition to the measures set out in Articles 7, 8 and 9(6), Member States must require covered entities to apply, on a risk-sensitive basis, enhanced customer due diligence measures in particular in situations which by their nature can present a higher risk of money laundering or terrorist financing. They must do so at least with respect to the situations set out in paragraphs 2 to 4 of Article 13 but also in other situations representing a high risk which meet the technical criteria established in accordance with Article 40(1)(c). [16] The situations set out in Articles 13(2) to Article 13(4) are: where the customer has not been physically present for identification purposes; cross-frontier correspondent banking relationships with respondent institutions from third countries; and transactions or business relationships with politically exposed persons residing in another Member State or in a third country. For such situations, specific enhanced customer due diligence measures (or examples of appropriate measures) are listed.

27. In accordance with Article 20, Member States must require that covered entities pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing.

28. Article 22, which together with Article 23 contains reporting obligations, requires covered entities (and where applicable their directors and employees) to cooperate fully by, inter alia, promptly informing the FIU, on their own initiative, where they know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted (Article 22(1)(a)).

14 — See also point 29 below.

15 — Implementing rules were adopted in Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ 2006 L 214, p. 29). Whilst that directive lays down implementing measures as regards, inter alia, technical criteria for assessing whether situations represent a low risk of money laundering or terrorist financing as referred to in Article 11(2) and (5) of the Money Laundering Directive, it does not cover Article 11(1).

16 — See point 32 below.

29. Article 28 prohibits covered entities, their directors and employees from disclosing to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 22 and 23 or that a money laundering or terrorist financing investigation is being or may be carried out.

30. According to Article 34(1), Member States must require that covered entities establish adequate and appropriate policies and procedures of due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

31. Articles 36 and 37 concern 'Supervision'. In particular, Article 37(1) provides that Member States are to require that the competent authorities at least monitor effectively and take the necessary measures with a view to ensuring that all covered entities comply with the requirements of the directive.

32. In accordance with Article 40(1)(c), the Commission may adopt implementing measures that establish technical criteria for assessing whether situations represent a high risk of money laundering or terrorist financing as referred to in Article 13.

Personal Data Directive

33. Recital 8 in the preamble to the Personal Data Directive states that 'the level of protection of the rights and freedoms of individuals with regard to the processing of [personal] data must be equivalent in all Member States'. Recital 9 recognises that, whilst the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, they will be left a margin for manoeuvre which may (in the context of implementing the Personal Data Directive) also be exercised by business and social partners.

34. Article 1 provides: 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'. In accordance with Article 1(2), 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1'.

35. Article 2(a) defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject")' and 'an identifiable person' as 'one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

36. The 'processing of personal data' is defined in Article 2(b) as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

37. In accordance with Article 3(1), the Personal Data Directive applies to 'the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'.

38. Article 7 lays down the criteria that determine whether data processing is legitimate. According to, respectively, Article 7(c) and (f), that is so where processing is necessary 'for compliance with a legal obligation to which the controller is subject' and 'for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)'.

Unfair Commercial Practices Directive

39. Recital 8 in the preamble to the Unfair Commercial Practices Directive states that this directive directly protects consumer economic interests from unfair business-to-consumer commercial practices and indirectly protects legitimate businesses from their competitors who do not play by the rules it contains. This directive thus guarantees fair competition in fields which it coordinates.

40. A 'consumer' within the meaning of the Unfair Commercial Practices Directive is 'any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession' (Article 2(a)). A 'trader' is 'any natural or legal person who, in commercial practices covered by this Directive, is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader' (Article 2(b)). 'Business-to-consumer commercial practices' or 'commercial practices' means 'any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product [that is, any good or service [17]] to consumers' (Article 2(d)).

41. Article 3(1) provides that the Unfair Commercial Practices Directive 'shall apply to unfair business-to-consumer commercial practices, as laid down in Article 5 [which sets out the prohibition of unfair commercial practices and defines what such practices are], before, during and after a commercial transaction in relation to a product'.

42. Article 3(4) states that '[i]n the case of conflict between the provisions of [the Unfair Commercial Practices Directive] and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects'.

Payment Services Directive

43. The Payment Services Directive lays down, inter alia, the rules for distinguishing between six categories of payment service provider, including credit institutions within the meaning of Article 4(1)(a) of Directive 2006/48 (Article 1(1)(a)) and payment institutions within the meaning of the Payment Services Directive (Article 1(1)(d)).

44. Article 4(3) defines a 'payment service' as 'any business activity listed in the Annex', which includes execution of payment transactions. A 'payment institution' is, according to Article 4(4), 'a legal person that has been granted authorisation in accordance with Article 10 [which requires undertakings intending to provide payment services to obtain authorisation as a payment institution before commencing the provision of payment services] to provide and execute payment services throughout the Community'. A 'payment service' means 'any business activity listed in the Annex' (Article 4(3)). An 'agent' is 'a natural or legal person which acts on behalf of a payment institution in providing payment services' (Article 4(22)).

17 — See Article 2(c) of the Unfair Commercial Practices Directive.

45. According to Article 5, an application for authorisation as a payment institution is to contain a series of documents, including 'a description of the internal control mechanisms which the applicant has established in order to comply with obligations in relation to money laundering and terrorist financing under [the Money Laundering Directive]'. Article 10(2) provides that authorisations are to be granted 'if the information and evidence accompanying the application complies with all the requirements under Article 5 and if the competent authorities' overall assessment, having scrutinised the application, is favourable'. Under Article 12(1), authorisations may be withdrawn only in defined circumstances, including where the payment institution no longer fulfils the conditions for granting the authorisation (Article 12(1)(c)).

46. In accordance with Article 17(1), a payment institution intending to provide payment services through an agent must communicate to its home Member State certain information enabling that agent to be listed in a publicly available register provided for in Article 13. That information includes the name and address of the agent and a description of the internal control mechanism that will be used by agents in order to comply with the obligations under the Money Laundering Directive in relation to money laundering and terrorist financing.

47. Under Article 20(1), first subparagraph, Member States are to designate as competent authorities '… either public authorities, or bodies recognised by national law or by public authorities expressly empowered for that purpose by national law, including national central banks'. The second subparagraph states that such authorities must guarantee independence from economic bodies and avoid conflicts of interest. Without prejudice to the first subparagraph, such authorities should not themselves be payment institutions, credit institutions, electronic money institutions or post office giro institutions.

48. Article 21 ('Supervision') states:

'1. Member States shall ensure that the controls exercised by the competent authorities for checking continued compliance with this Title ["Payment Service Providers"] are proportionate, adequate and responsive to the risks to which payment institutions are exposed.In order to check compliance with this Title, the competent authorities shall be entitled to take the following steps, in particular:

(a) to require the payment institution to provide any information needed to monitor compliance;

(b) to carry out on-site inspections at the payment institution, at any agent or branch providing payment services under the responsibility of the payment institution, or at any entity to which activities are outsourced;

(c) to issue recommendations, guidelines and, if applicable, binding administrative provisions; and

(d) to suspend or withdraw authorisation in cases referred to in Article 12.

2. … [T]he Member States shall provide that their respective competent authorities, may, as against payment institutions or those who effectively control the business of payment institutions which breach laws, regulations or administrative provisions concerning the supervision or pursuit of their payment service business, adopt or impose … penalties or measures aimed specifically at ending observed breaches or the causes of such breaches.

...'

49. Article 79 on 'Data protection' provides: 'Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of such personal data shall be carried out in accordance with [the Personal Data Directive].'

National law

50. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing; 'Law 10/2010'), which transposed the Money Laundering Directive into Spanish law, distinguishes between three types of customer due diligence measure: (i) standard customer due diligence measures (Articles 3 to 6); (ii) simplified customer due diligence measures (Articles 9);[18] and (iii) enhanced customer due diligence measures (Article 11).

51. Standard customer due diligence measures include formally identifying the persons concerned (Article 3), identifying the real beneficiaries (Article 4), obtaining information on the object and nature of the envisaged business relationship (Article 5) and constant monitoring of the business relationship (Article 6).

52. In accordance with Article 7(3), persons subject to Law 10/2010 may not start a business relationship or carry out a transaction if they cannot apply the customer due diligence measures foreseen by this law. If such impossibility occurs during the course of the business relationship, they should terminate that relationship.

53. Article 9(1)(b) states that the persons subject to Law 10/2010 are authorised not to apply certain standard customer due diligence measures with regard to customers which are financial institutions having their seat in the European Union or in equivalent third countries and whose compliance with customer due diligence measures is subject to supervision. According to the referring court, the use of the word 'authorised' suggests that this provision does not set out an obligation. However, the referring court has doubts as to its exact meaning.

54. In accordance with Article 11, enhanced customer due diligence measures must be taken where, based on a risk assessment, there is a high risk of money laundering or terrorist financing. Certain situations, by their nature, present such a risk, notably services of sending money.

Facts, procedure and questions referred

55. Safe is a company that transfers customers' funds abroad (that is, to other Member States and to third States) through the accounts it holds with credit institutions.

56. The request for a preliminary ruling indicates that the banks closed Safe's accounts with them after it refused to provide them with information (regarding its customers and the destination of funds remitted) which they had requested on the basis of Law 10/2010, in response to irregularities regarding agents which were authorised by Safe to conduct transfers through its accounts and which had been verified by the Banco de España (Bank of Spain).

57. On 11 May 2011, BBVA communicated those irregularities to the Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias del Banco de España (Executive Service of the Commission for the Prevention of Money Laundering and Financial Crime of the Bank of Spain; 'SEPBLAC'). On 22 July 2011, BBVA notified Safe of the irrevocable closure of its account.

58. Safe challenged BBVA's decision to close its account (and similar decisions by the two other banks) before the Juzgado de lo Mercantil No 5 de Barcelona (Commercial Court No 5, Barcelona; 'the Commercial Court'), on the grounds that the closure was an act of unfair competition which prevented it from operating normally by transferring funds abroad. According to Safe: (i) sending

18 — Article 10 concerns simplified measures but with regard to products or transactions.

remittances abroad necessarily required it to hold accounts; (ii) it competed in the market with the banks; (iii) the banks had never previously required it to give them the requested data regarding Safe's customers and the origin and destination of the funds (the practice started when the banks relied on Law 10/2010); and (iv) providing the banks with such data would be contrary to legislation on the protection of personal data. The banks responded that their measures were in accordance with Law 10/2010, were justified in particular because of risks relating to the transfer of funds abroad, and were not contrary to competition law.

59. On 25 September 2009, the Commercial Court rejected Safe's application. It held that the banks were entitled to ask Safe to adopt enhanced customer due diligence measures and to provide data relating to its customers, subject to the condition that they detected in Safe's behaviour signs of conduct that infringed Law 10/2010. Whether the banks were justified in closing Safe's accounts had to be examined in each case. Whilst none of the banks had infringed any specific prohibition of anti-competitive conduct, Sabadell and Liberbank (but not BBVA) had acted unfairly by failing to set out the reasons underpinning their measures. BBVA's conduct was deemed to be justified because it was based on checks which showed that 22% of transfers made through Safe's account during the period from 1 September to 30 November 2010 were *not* undertaken by agents who had been authorised by Safe and verified by the Bank of Spain. Moreover, during that period, transfers were made by 1 291 persons, which far exceeded the number of Safe's agents. An expert report had further highlighted the risks of transfers not conducted by identified agents.

60. Safe, Sabadell and Liberbank appealed against that judgment to the Audiencia Provincial, Barcelona (Provincial Court, Barcelona; 'the referring court'), which is hearing the three appeals together.

61. The referring court states that all parties involved are subject to Law 10/2010, as they fall within the categories listed in Article 2 of that law, which include credit institutions and payment institutions. Furthermore, all parties compete on the market and carry out the same activity of sending remittances abroad. However, payment institutions (such as Safe) must do so through accounts held with credit institutions (such as the banks).

62. Safe argues, first, that BBVA was not required to adopt customer due diligence measures in relation to financial institutions because these are supervised directly by the public authorities, in particular by the Bank of Spain. Second, in Spain only SEPBLAC may access data relating to the customers of payment institutions. Third, even if BBVA was required to adopt customer due diligence measures, it had to conduct a detailed and exhaustive study of Safe's policy for complying with relevant legislation prior to adopting such measures. In the present case, BBVA had merely requested an expert report which had been prepared using BBVA's data. Fourth, Law 10/2010 does not apply to persons, such as agents, offering support to financial institutions for transfers of funds.

63. Sabadell's appeal addresses the fact that the Commercial Court's judgment accepted that Sabadell could in principle adopt enhanced customer due diligence measures, but not that it could do so in this case. Liberbank argues that closing the account was justified because Safe had failed to provide the information requested.

64. Against that background, the referring court seeks a preliminary ruling on the following questions:

'(1) On the interpretation of Article 11(1) of [the Money Laundering Directive]:

a. If this provision is read in conjunction with Article 7 of that directive, was it the Union legislature's intention to establish a genuine derogation from the possibility that credit institutions may adopt due diligence measures when their customers are themselves payment institutions in turn subject to their own supervision system, or is it simply an authorisation to derogate?

b. If this provision is read in conjunction with Article 5 of that directive, may the national legislature transpose the derogation laid down in the provision concerned in terms other than the actual wording thereof?

c. Does the derogation contained in Article 11(1) apply to enhanced due diligence measures too in the same terms as it applies to due diligence measures?

(2) In the alternative, should the reply to the above questions confirm that credit institutions may adopt due diligence measures and enhanced due diligence measures in relation to payment institutions:

a. How far does the possibility that credit institutions may supervise the operations of payment institutions extend? Can they be deemed to be authorised under the provisions of [the Money Laundering Directive] to supervise the due diligence procedures and measures adopted in turn by payment institutions or does that power belong exclusively to the public institutions referred to in [the Payment Services Directive], in the present case, the Banco de España …?

b. Does the application of that right of credit institutions to adopt measures require any special justification that may be deduced from the acts of the payment institution or may those measures instead be adopted generally, simply on account of the fact that the payment institution carries out a risky activity such as the sending of remittances abroad?

c. If it is held that a specific justification is required in order for credit institutions to be able to adopt due diligence measures in relation to payment institutions:

i. What is the relevant conduct that a bank must bear in mind for the purposes of adopting due diligence measures?

ii. Can a credit institution be considered authorised to assess, for that purpose, the due diligence measures which a payment institution applies in its procedures?

iii. Does the exercise of that power require the bank to have identified in a payment institution's operations conduct leading it to suspect collaboration in money laundering activities or in terrorist financing?

(3) In addition, if it should be held that credit institutions are authorised to adopt enhanced due diligence measures in relation to payment institutions:

a. Is it acceptable that those measures may include a measure requiring payment institutions to provide identification data for all their customers from whom the funds remitted originate, and the identities of the recipients?

b. Is the obligation of payment institutions to provide their customers' data to credit institutions with which they are forced to operate and with which they also compete on the market compatible with [the Personal Data Directive]?'

65. Written observations have been submitted by BBVA, Safe, the Spanish and Portuguese Governments and the European Commission. At the hearing on 6 May 2015, except for BBVA and the Portuguese Government, the same parties presented oral argument.

Assessment

Preliminary remarks

66. The essence of the dispute before the national court is whether the banks were entitled or required to take the action they did pursuant to the Money Laundering Directive (as properly implemented), or whether they were unjustifiably using that directive as an excuse for unfair competitive behaviour.

67. The questions referred arise only in so far as the banks and Safe are covered entities under the Money Laundering Directive.[19] No party has contested the referring court's decision, in formulating its questions, to characterise them as, respectively, credit institutions and a payment institution within the meaning of national law transposing Article 3 of the Money Laundering Directive.

68. By Question 1, the referring court seeks guidance on Article 11(1) of the Money Laundering Directive, in particular on whether that provision, when read together with Articles 5 and 7, precludes a Member State from authorising or requiring a credit institution to apply standard customer due diligence measures in relation to a customer which is a payment institution and also subject to the Money Laundering Directive (Questions 1(a) and (b)). By Question 1(c), it asks a similar question in relation to enhanced customer due diligence measures under Article 13.

69. As I see it, the answer to Question 1 depends first and foremost on the scope of Articles 7, 11(1) and 13 of the Money Laundering Directive. If, in implementing any of these provisions, Member States are not precluded from authorising or requiring a credit institution to close the accounts of a payment institution in circumstances such as those at issue, it is not necessary to consider Article 5, because the obligations under national law then merely correspond to those under the Money Laundering Directive.

70. Conversely if Articles 5, 7, 11(1) and 13 of the Money Laundering Directive should be read as precluding Member States from authorising or requiring credit institutions, such as the banks, to apply (enhanced) customer due diligence measures in circumstances that call for simplified customer due diligence, Questions 2 and 3 are no longer relevant because there could have been no lawful basis for the banks' measures.

71. If the Money Laundering Directive does not preclude Member States from authorising or requiring (enhanced) customer due diligence measures in such circumstances, Questions 2 and 3 ask the Court about the scope of such measures and the conditions under which they may be imposed. In particular: may national law foresee that credit institutions supervise the operations and the customer due diligence procedures and measures adopted by payment institutions and, if so, to what extent (Question 2(a))? Must there be a specific justification in order to exercise the right to apply (enhanced) customer due diligence measures, or is it sufficient that the customer carries out a risky activity (Question 2(b))? If a specific justification is needed, on what criteria must such an analysis be based (Question 2(c))? Finally, may such customer due diligence measures include requiring payment institutions to provide identification data for all their customers from whom the funds remitted originate and the identities of the recipients and is that in conformity with the Personal Data Directive (Question 3(a) and (b))?

19 — Namely, credit institutions or financial institutions as listed in Article 2(1)(1) and (2) of the Money Laundering Directive.

72. In interpreting the Money Laundering Directive, all parties have relied on recommendations and other materials produced by the FATF, which is an inter-governmental body that sets standards and develops and promotes policies to combat money laundering and terrorist financing. [20] The Court has already recognised that the Money Laundering Directive (like its predecessor Directive 91/308/EEC) was adopted in order to apply and make FATF recommendations binding in the European Union. [21] The Money Laundering Directive should therefore be interpreted in line with the 2003 FATF Recommendations, [22] which are in essence minimum standards in this field. I shall accordingly take them into account where relevant.

73. In some questions, the referring court has identified specific provisions of EU law. In others, it has not. However, it is well established that, in order to provide a satisfactory answer to the questions referred, this Court may deem it necessary to consider provisions of EU law to which no reference has been made. [23] I have adopted that approach in suggesting answers to the questions referred.

74. Whilst Question 3(b) does not refer to the Unfair Commercial Practices Directive, the referring court none the less expresses, elsewhere in the order for reference, doubts about the relationship between rights under that directive and the Money Laundering Directive. However, the Unfair Commercial Practices Directive does not apply here because Safe is *not* 'acting for purposes which are outside [its] trade, business, craft or profession'. [24] The Court has held that the terms 'customer' and 'trader' in this directive are diametrically opposed and that the term 'consumer' refers to 'any individual not engaged in commercial or trade activities'. [25] Thus, Safe is not a consumer within the meaning of that directive.

Scope of Article 11(1) of the Money Laundering Directive (Question 1(a) to (c))

75. Whilst the referring court has not said so explicitly, elements in the file and the written and oral observations suggest that BBVA became suspicious of money laundering or terrorist financing after it discovered irregularities in the information about the agents which transferred funds through Safe's account with BBVA.

76. BBVA closed Safe's account on the basis of Law 10/2010 which, on the one hand, authorises the application of simplified customer due diligence measures with respect to financial institutions whose compliance with customer due diligence measures is subject to surveillance and, on the other hand, requires covered entities to apply, depending on their risk assessment, enhanced customer due diligence measures in situations which, by their very nature, present a high risk of money laundering and terrorist financing, such as the transfer of funds.

77. By Question 1, the referring court asks in essence whether the Money Laundering Directive precludes a national law which regulates (simplified and enhanced) customer due diligence measures in that way.

78. The Money Laundering Directive provides for three different types of customer due diligence measure (standard, simplified and enhanced). Member States must provide for the appropriate application of these measures in order to prevent the financial system being used for money laundering and terrorist financing. Such measures may need to be applied before or after a business

20 — See 2003 FATF Recommendations, Introduction, footnote 1, and 2012 FATF Recommendations, Introduction, page 7. The Commission is listed as one of the FATF's Members.

21 — See, for example, judgment in *Jyske Bank Gibraltar*, C-212/11, EU:C:2013:270 ('judgment in *Jyske Bank Gibraltar*'), paragraphs 46 and 63.

22 — See point 7 above.

23 — See judgment in *Jyske Bank Gibraltar*, paragraph 38 and case-law cited.

24 — Article 2(a) of the Unfair Commercial Practices Directive.

25 — Judgment in *Zentrale zur Bekämpfung unlauteren Wettbewerbs*, C-59/12, EU:C:2013:634, paragraph 33.

relationship is established or a transaction is carried out. The intended degree of deterrence of each type of measure depends on the perceived degree of risk that the financial system will be used for such purposes. That degree of risk necessarily varies and thus Member States must ensure that the measures to be applied fit the situation in each case.[26] I therefore consider that the decision as to what level of customer due diligence to apply must always be based on verifiable grounds.

79. As I see it, the starting point for understanding Chapter II ('Due diligence') in the Money Laundering Directive and the relationship between Articles 5, 7, 11(1) and 13 is the obligation to apply *standard* customer due diligence measures.

80. Article 7 lays down the situations that automatically trigger the obligation to apply standard customer due diligence measures, because there are deemed to present risks of money laundering or terrorist financing which can be prevented by the measures under Articles 8 and 9.[27] These situations concern: (a) the establishment of a business relationship; (b) the carrying out of occasional transactions amounting to EUR 15 000 or more; (c) the existence of suspicion of money laundering or terrorist financing; and (d) the existence of doubts about the veracity or adequacy of previously obtained customer identification data. Thus, standard customer due diligence measures can apply before a business relationship has been formed or a transaction has taken place (Articles 7(a) and (b)), or regardless of whether or not that is the case (Article 7(c) and (d)). In particular, nothing in Article 7(c) suggests that the suspicion of money laundering or terrorist financing referred to must arise before establishing, rather than in the course of, a business relationship or transaction.

81. The Money Laundering Directive does not define 'suspicion of money laundering or terrorist financing'. Although Article 22(1)(a) (on the scope of the obligation to report to the FIU) suggests that having 'suspicion' is not the same as having 'reasonable grounds to suspect' that money laundering or terrorist financing is being (or has been) committed or attempted, I consider that that distinction cannot be read to mean that 'suspicion' in Article 7(c) is a purely subjective matter. In my opinion, suspicion must be based on some objective material that is capable of review in order to verify compliance with Article 7(c) and other provisions of the Money Laundering Directive.[28] Thus, in my opinion, 'a suspicion of money laundering or terrorist financing' within the meaning of Article 7(c) arises in particular where, taking into account the individual circumstances of a customer and his transactions (including with respect to the use and management of his account(s)), there are verifiable grounds showing a risk that money laundering or terrorist financing exists or will occur in relation to that customer.

82. Pursuant to the Money Laundering Directive, national law must provide that, where there is such suspicion (and in the other situations listed in Article 7), covered entities must apply standard customer due diligence measures, including identifying the customer and verifying his identity (Article 8(1)(a)); identifying, where applicable, the beneficial owner (Article 8(1)(b)); obtaining information on the purpose and intended nature of the business relationship (Article 8(1)(c)); and conducting ongoing monitoring of an existing business relationship and transactions already undertaken (Article 8(1)(d)). Article 8(1)(d) can only be applied *ex post*. The other three types of measure can be applied at any stage. This is consistent with Article 9(6), under which Member States must require covered entities to apply customer due diligence procedures to all new customers and, at appropriate times, to existing customers on a risk-sensitive basis. However, before a business relationship is established or a relevant transaction is carried out, Member States must require the identity of the customer and the beneficial owner to be verified (Article 9(1)).

26 — See, for example, Articles 8(2) and 34(1) of and recitals 22 and 24 in the preamble to the Money Laundering Directive.

27 — There may be other circumstances in which such a risk is found to exist.

28 — Such as Articles 22(1)(a), 24 and 27.

83. Thus, Articles 7, 8 and 9 identify the circumstances in which the EU legislator has considered that national law must provide for 'standard' preventive measures where there is a risk of money laundering and terrorist financing, and has defined the appropriate measures to prevent that risk from materialising.

84. In other circumstances (depending, for example, on the type of customer, business relationship, product or transaction [29]), the risk may be lower or higher. Articles 11 and 13 deal respectively with those situations, and require Member States to ensure that different degrees of customer due diligence measures are applied.

85. Subject to certain conditions laid down in Article 11, the customer due diligence measures in Articles 8 and 9(1) are not to be applied in circumstances where, pursuant to Article 7(a), (b) and (d), they would otherwise be required. The conditions concern situations in which the EU legislator has deemed there to be a lower risk of money laundering and terrorist financing by reason of, for example, the identity of the customer or the value and content of the transaction or product.

86. That is the case where a customer of a covered entity is itself a credit or financial institution covered by the Money Laundering Directive. In accordance with Article 11(1), Member States may not require covered entities (such as the banks) to apply customer due diligence measures under Articles 8 and 9(1) with respect to their customers (such as Safe) in the circumstances listed in Articles 7(a), (b) and (d).

87. The fact that Article 11(1) *requires* that covered entities should not be subject to standard customer due diligence measures whereas other paragraphs of Article 11 (such as Article 11(2)) *allow* Member States to authorise simplified due diligence, does not alter that conclusion. The use of a permissive form elsewhere in Article 11 indicates that Member States have the option to impose the simplified due diligence measures set out in Article 11; standard due diligence measures under Article 8; or enhanced or stricter due diligence obligations in conformity with, respectively, Articles 13 and 5. As I see it, the use of an injunctive form in Article 11(1) means that the options there are fewer: either simplified due diligence is applied or, where relevant and necessary, enhanced or stricter due diligence obligations in conformity with, respectively, Articles 13 and 5. What may not be applied is standard due diligence as such. Thus, I do not interpret Article 11(1) as prohibiting stricter provisions based on Article 5.

88. The rationale for the derogation in Article 11(1) is that the customer is itself covered by the Money Laundering Directive. That customer must comply with all relevant requirements in that directive as implemented in national law, including those as to customer due diligence measures which it must apply in relation to its own customers, and is subject to that directive's reporting, surveillance and other requirements. In such circumstances, the need to take preventive action is attenuated.

89. That rationale is also consistent with the 2012 FATF Recommendations. Point 16 of the interpretative note to recommendation 10 recognises that there may be circumstances in which the risk of money laundering or terrorist financing is lower and, subject to an adequate risk analysis, it could be reasonable to allow financial institutions to apply simplified customer due diligence measures. [30] Point 17 expressly identifies the example of financial institutions which are themselves subject to requirements to combat money laundering and terrorist financing consistent with the 2012 FATF Recommendations, have effectively implemented those requirements and are supervised for compliance with those obligations. [31]

29 — I note that, whilst the Money Laundering Directive does not appear to define the term 'product', the context in which this term is used suggests that it is intended to cover various financial and commercial offerings.

30 — See also interpretative note 9 to recommendation 5 of the 2003 FATF Recommendations.

31 — See also interpretative note 10 to recommendation 5 of the 2003 FATF Recommendations.

90. Thus, I take the view that Article 11(1) reflects the principle that customer due diligence measures should be commensurate with the risks identified. [32] Article 11(1) assumes a reduced risk because, *since the customer is a covered entity*, customer due diligence, reporting and surveillance measures are already in place to manage the risk that that covered entity and in particular that entity's own customers might present. Article 11(1) thus seeks to reconcile the interests of effective regulation, cost-efficient risk management and appropriate and proportionate prevention of the risk of money laundering and terrorist financing.

91. Article 11(1) applies to all covered entities, even if some entities may be subject to additional conditions, as is the case for payment institutions by virtue of the Payment Services Directive. Their authorisation to operate as payment institutions depends on compliance with the Money Laundering Directive and, where they intend to use registered agents, they must have an internal control mechanism in place to verify such compliance. [33]

92. However, despite the application of the Money Laundering Directive, the Payment Services Directive and other EU legislation, [34] protection under existing EU law (and national implementing laws) against the risk of money laundering and terrorist financing cannot guarantee a zero risk. [35]

93. That is why Article 11(1) does *not* derogate from Article 7(c). Regardless of any derogation, exemption or threshold and thus regardless of whether the customer is or is not a covered entity, Article 7(c) provides that customer due diligence measures are always required where there is suspicion of money laundering or terrorist financing. [36] Put differently, where such a suspicion arises, a Member State is therefore precluded from allowing or requiring simplified customer due diligence measures to be applied. Thus, if the competent national court in the present case finds that BBVA and the two other banks rightly found there to be such suspicion as regards Safe, EU law requires it to interpret national law (so far as possible) so as to mean that the banks were required under Article 7(c) to apply (at least) standard customer due diligence measures. [37]

94. Nor does the fact that the customer is itself an entity covered by the Money Laundering Directive mean that a Member State must not require enhanced customer due diligence measures within the meaning of Article 13 of that directive to be applied with respect to that customer if, despite the guarantees already provided by the Money Laundering Directive, the Payment Services Directive and other EU legislation, there exists a higher risk of money laundering and terrorist financing as foreseen by that provision. Article 11 only derogates from standard customer due diligence measures in situations of lower risk. Since it does not refer to Article 13, it has no bearing on the customer due diligence that is required where there is a higher risk.

32 — See recitals 22 and 24 in the preamble to the Money Laundering Directive. See also recommendation 1 of the 2012 FATF Recommendations.

33 — See, for example, Articles 17 and 21 of the Payment Services Directive.

34 — For example, other EU legislation relating to the combating of money laundering and terrorist financing includes: Regulation (EC) No 1781/2006 of 15 November 2006 on information on the payer accompanying transfers of funds (OJ 2006 L 345, p. 1); Regulation (EC) No 1889/2005 of 26 October 2005 on controls of cash entering or leaving the Community (OJ 2005 L 309, p. 9); Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ 2001 L 344, p. 70).

35 — The FATF has also taken the position that the risk-based approach is not a 'zero failure' approach and there might be occasions where an institution has taken all reasonable measures to identify and mitigate the risk but is still being used for money laundering and terrorist financing. See FATF, Guidance for a Risk-Based Approach – The Banking Sector (October 2014), point 10.

36 — This implication was the basis for the European Parliament's proposal to exclude (what is now) Article 7(c) from the derogation: see Report on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing (COM(2004)0448 – C6-0143/2004 – 2004/0137(COD)), p. 43.

37 — This is also consistent with the 2003 FATF Recommendations. Interpretative note 13 to recommendation 5 states that '[s]implified [customer due diligence] measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply'. See also interpretative note 2 to recommendation 1 of the 2012 FATF Recommendations.

95. Article 13 requires Member States to provide that covered entities apply, on a risk sensitive basis, enhanced customer due diligence measures in particular in situations which by their nature can present a higher risk of money laundering or terrorist financing and at least in the situations of higher risk identified in paragraphs 2 to 4 of Article 13. Sending remittances abroad is not listed in those paragraphs. Nor has the referring court suggested that any of these paragraphs applies.[38] However, Article 13 does not preclude Member States from identifying in their national laws, taking a risk-based approach, other situations which by their nature present a higher risk and therefore justify or even require the application of enhanced due diligence (in additional to standard customer due diligence).

96. Therefore, notwithstanding the derogation in Article 11(1), Articles 7 and 13 of the Money Laundering Directive require Member States to ensure that covered entities apply, in situations involving customers who are themselves covered entities under that directive (i) standard customer due diligence measures under Articles 8 and 9(1) where there is suspicion of money laundering or terrorist financing within the meaning of Article 7(c) and (ii) enhanced customer due diligence measures under Article 13 in situations foreseen under that provision.

97. Even where Member States have properly transposed Articles 7, 11 and 13 into national law,[39] Article 5 permits them to adopt or retain in force 'stricter provisions' that seek to strengthen the fight against money laundering or terrorist financing,[40] and confirms that the Money Laundering Directive merely provides for a minimum level of harmonisation.[41] Those 'stricter provisions', as I see it, might relate to situations for which the directive provides for some type of customer due diligence and also to other situations which Member States deem to present a risk.

98. Article 5 forms part of Chapter I ('Subject matter, Scope and Definitions') and applies with respect to all 'provisions in the field covered by [the Money Laundering Directive] to prevent money laundering and terrorist financing'. Its remit is thus not limited to the provisions in Chapter II ('Customer due diligence'). A Member State may therefore provide for customer due diligence measures to be applied by a credit institution in relation to a payment institution even where the conditions of Article 11(1) are satisfied (and thus even where there is no suspicion within the meaning of Article 7(c)) and in situations other than those listed in Articles 7 and 13, where this is justified and otherwise consistent with EU law.[42]

99. In summary, provisions such as Articles 8 or 13 of the Money Laundering Directive leave Member States a significant degree of freedom, in implementing that directive, in precisely how they give effect to the obligations to provide for different types of due diligence, depending on the circumstances at issue and in accordance with their overarching obligations to evaluate risk and to put into place laws that require measures to be applied which are commensurate with the identified risk and which comply with other applicable obligations under EU law. Article 5 then provides for a further margin of freedom as it permits Member States to adopt or retain 'stricter provisions' where they deem them necessary, provided that in so doing they respect their obligations under EU law.

38 — It is true that Member States must provide for similar obligations in situations other than those listed in paragraphs 2 to 4, which represent a high risk of money laundering or terrorist financing and which meet the technical criteria established in implementing measures taken by the Commission based on Article 40(1)(c). As far as I can see, such implementing measures have not yet been adopted.

39 — See point 54 above.

40 — Judgment in *Jyske Bank Gibraltar*, paragraph 61.

41 — See judgment in *Jyske Bank Gibraltar*, paragraph 61.

42 — See points 108 to 119 below.

May credit institutions supervise the customer due diligence measures adopted by payment institutions (Questions 2(a) and 2(c)(ii))?

100. In Question 2(a), the referring court seeks guidance as to the supervision powers of credit institutions, under the Money Laundering Directive and the Payment Services Directive, in relation to the operations and due diligence procedures and measures of payment institutions who are their customers. Question 2(c)(ii), which is closely related, asks whether a credit institution may assess the due diligence measures applied by a payment institution.

101. I understand these questions to be based on the assumption that Safe's accounts were closed because Safe failed to provide information requested by the banks in the context of customer due diligence measures applied by the latter. The closure should therefore be considered as a means of enforcing Safe's obligations under the Money Laundering Directive, and possibly the Payment Services Directive, for which only the competent authorities, not the banks, are competent. [43]

102. I do not see how the banks' action can be construed as being supervisory in nature. The Money Laundering Directive concerns customer due diligence requirements which apply to covered entities, not to customers *because of their status as customers*. The directive does not require customers to provide covered entities with the information which the latter must obtain and verify in order to satisfy their own customer due diligence obligations. Thus, for example, Article 8 describes elements of a business relationship about which information is to be obtained and verified. It does not specify that national law must provide that the information is to be obtained from the customer and that the latter is, pursuant to the Money Laundering Directive as properly implemented, required to respond to such requests (even if the customer has a strong interest in doing so in order to avoid the consequences described under Article 9(5)). [44]

103. As a result, action of the kinds provided for in the first subparagraph of Article 9(5) (including, where a business relationship has already been established, termination of that relationship) is the consequence of a covered entity's inability to comply with the customer due diligence obligations under Article 8(1)(a) to (c) as implemented by the Member States. That consequence is justified by the resulting risk that customers, transactions and relationships are (or may be) used for money laundering or terrorist financing purposes.

104. Article 9(5) does not depend, for its application, on *why* a covered entity cannot comply with the required customer due diligence measures under Article 8(1)(a) to (c). Thus, the fact that a covered entity's customers do not cooperate by providing information enabling it to comply with national law implementing Article 8 is neither necessary nor always sufficient to trigger the consequences set out in Article 9(5).

105. It is true that Article 37 of the Money Laundering Directive requires competent authorities to monitor effectively and to take the necessary measures to ensure that covered entities, including credit institutions and payment institutions applying customer due diligence measures to any of their customers, comply with that directive. As Advocate General Bot has put it, the effectiveness of customer due diligence and disclosure measures is assured by conferring powers of supervision and penalties on the competent national authorities. [45] I agree with him that the customer due diligence, reporting, supervision and monitoring measures together constitute preventive and dissuasive measures to combat money laundering and financing of terrorism effectively, and to safeguard the soundness and integrity of the financial system.

43 — See Article 21 of the Payment Services Directive.

44 — See also recital 10 in the preamble to the Money Laundering Directive.

45 — Opinion of Advocate General Bot in *Jyske Bank Gibraltar*, C-212/11, EU:C:2012:607, point 61.

106. However, that does not imply that covered entities, when acting on the basis of national laws implementing Articles 8 and 9 of the Money Laundering Directive, assume the supervisory role that is reserved to the competent authorities.

107. Nor does it mean that covered entities may undermine the supervision tasks which competent authorities under Article 21 of the Payment Services Directive are to exercise over payment institutions to verify compliance with the provisions of Title II ('Payment service providers') in that directive. [46] Whilst those authorities might, in appropriate circumstances, withdraw the registration of agents, the branch or the payment institution itself pursuant to that directive, [47] such powers coexist with the preventive measures to be applied by covered entities and the supervisory powers of competent authorities under the Money Laundering Directive.

Is a specific justification needed in order to exercise the right to apply (enhanced) customer due diligence measures, or is it sufficient that the customer carries out a risky activity (Question 2(b))? If specific justification is needed, what criteria apply (Question 2(c)(i) to (iii))?

108. If Member States may authorise or require credit institutions to apply customer due diligence measures to a payment institution, the referring court asks, by Questions 2(b) and 2(c)(i) to (iii), in essence whether such measures can be based merely on the general type of activity pursued by that payment institution or whether individual acts of that institution must be analysed.

109. I recall that the questions arise in the context of a dispute involving covered entities which claim to have based their customer due diligence measures on national law applicable to situations that the legislator has deemed to present high risk (such as the provision of services to send money) and that are not listed in Article 13. Moreover, I have already addressed what is required in case of suspicion of money laundering within the meaning of Article 7(c). [48]

110. I therefore understand Questions 2(b) and 2(c)(i) to (iii) to relate to circumstances in which a Member State is acting within the freedom left to it by the Money Laundering Directive.

111. When a Member State acts within that freedom, it must nevertheless exercise that competence in accordance with EU law, in particular the basic freedoms guaranteed by the Treaties. [49] The Court has accepted that the objective of combating the use of the financial system for money laundering or terrorist financing, which underlies the Money Laundering Directive, is to be balanced against the protection of other interests, including the freedom to provide services. Thus, in *Jyske Bank Gibraltar*, the Court in essence found that restrictions on the freedom to provide services resulting from an information requirement 'in so far as such legislation seeks to strengthen, in compliance with [EU] law, the effectiveness of the fight against money laundering and terrorist financing' were permissible. [50] Where (as here) EU law has not been completely harmonised, national legislation which restricts basic freedoms may be justified because it meets an overriding requirement relating to the public interest, if that interest is not already safeguarded by the rules to which the service provider is subject in the Member State in which he is established, in so far as it is appropriate to secure the attainment of the aim which it pursues and does not go beyond what is necessary in order to attain it. [51]

46 — That title includes Article 17(1) of the Payment Services Directive.

47 — See Article 17(6) of the Payment Services Directive.

48 — See points 81 and 82 above.

49 — See, for example, judgment in *Commission* v *Portugal*, C-438/08, EU:C:2009:651, paragraph 27 and case-law cited.

50 — Judgment in *Jyske Bank Gibraltar*, paragraph 49, read together with paragraphs 59 and 60.

51 — Judgment in *Jyske Bank Gibraltar*, paragraphs 57 to 60 (and, in particular, case-law cited at paragraph 60).

112. The Court has already accepted that preventing and combating money laundering and terrorist financing are legitimate objectives which concern the protection of public order and can justify a barrier to the freedom to provide services. [52]

113. Is national law such as that at issue appropriate to secure the attainment of that objective because it helps to reduce the risk and, more generally, genuinely reflects a concern to attain the objective in a consistent and systematic manner? [53] A national law that identifies, following an appropriate risk assessment (including in relation to customers which are payment institutions), a high risk with respect to a type of (for example) customer, country, product or transaction and that on that basis authorises or even requires covered entities to apply, following their own individualised risk assessment, appropriate customer due diligence measures seems to me to satisfy that requirement.

114. Assessing whether the national law is proportionate involves determining the level of protection desired by the Member State with respect to the identified level of risk of money laundering and terrorist financing. I read the Money Laundering Directive as confirming that Member States may set, for example, a level of protection that is higher than that chosen by the EU legislator, identify other situations of (high) risk and authorise or require customer due diligence measures other than those foreseen by that directive.

115. Where they do so, Member States may, for example, identify the specific measures to be applied in certain specified situations or give covered entities discretion to apply, based on an appropriate risk assessment, the measures deemed to be commensurate with the risk at issue in a specified situation. In either event, Member States must guarantee that the enhanced customer due diligence measures applied are based on assessing the existence and level of a risk of money laundering or terrorist financing with respect to a customer, business relationship, account, product or transaction, as the case may be. Without such assessment, it is not possible for either the Member State or, where relevant, a covered entity to decide in an individual case what measures to apply. And, where there is no risk of money laundering or terrorist financing, preventive action cannot be taken on those (legitimate) grounds.

116. That risk assessment must take into account, at least, all relevant facts capable of showing the (level of) risk of one of the types of conduct that are to be considered as money laundering or terrorist financing. Such risks (and their level) can depend on, inter alia, customers, countries or geographic areas, products, services, transactions or delivery channels. Thus, it may be necessary to ascertain, based on any information already available, (for example) who is involved in a transfer of property, the origin of that property, the rights transferred, whether there was knowledge of criminal activity, the degree of involvement of particular persons and entities in the acquisition, possession, use or transfer of property, the purpose of any transaction or relationship, the geographic scope of any operation involving the property, the value of the property or a transaction involving that property, or the regularity or duration of the business relationship.

117. Such an assessment makes it possible in general and in individual cases to decide how to manage the risk by adopting appropriate measures. In choosing such measures, it is necessary (for both Member States and, where relevant, covered entities) to assess how far the perceived risk is already managed and the desired level of protection already secured by other measures, including those based on the Money Laundering Directive, the Payment Services Directive and other EU (or national) legislation. It is probably unlikely that a single customer due diligence or other measure can eliminate any risk of money laundering or terrorist financing. Rather, EU legislation suggests that Member States must adopt many different types of response to such risks.

52 — Judgment in *Jyske Bank Gibraltar*, paragraphs 62 to 64 and 85 and case-law cited.

53 — Judgment in *Jyske Bank Gibraltar*, paragraph 66 and case-law cited.

118. Moreover, whether a national law is proportionate will also depend on the degree to which the customer due diligence measures for which it provides may intrude upon other protected rights and interests under EU law, such as the protection of personal data (Article 8 of the Charter) and the principle of free competition between entities operating in the same market. Their objectives must be balanced against such other legitimate interests.

119. Finally, whether a national law is proportionate will depend on whether there are alternative, less restrictive means to achieve the same level of protection. Thus, for example, rather than a blanket law that assumes that sending funds abroad will always be high risk,[54] a law that differentiates between transferee countries (based on the risk which sending money there presents) or requires covered entities so to differentiate may be less restrictive and yet still achieve the Member State's desired level of protection.

Customer due diligence measures and the protection of personal data (Question 3(a) and (b))

120. By Question 3(b), the referring court in essence asks whether the Personal Data Directive precludes Member States from requiring payment institutions to provide data regarding the identity of their customers to credit institutions, which are in direct competition with them, in the context of enhanced customer due diligence measures applied by the latter. Question 3(a) is similar, though it refers neither to any specific provision of EU law nor to the competitive relationship between the payment institution and the credit institutions (but, conversely, does refer to data pertaining to recipients of funds transmitted through Safe's accounts).

121. Some doubts have arisen as to whether Question 3 is admissible, because BBVA insists that it has never asked for personal data regarding Safe's customers or recipients of the transmitted funds; it sought only information regarding the agents who acted on behalf of Safe and used Safe's accounts.

122. If BBVA's presentation of the facts is correct and corresponds also with what happened in the dispute between the two other banks and Safe, Question 3 would indeed appear not to be relevant to the resolution of the dispute in the main proceedings. However, it is well established that it is not for the Court to ascertain and assess the facts which have given rise to the dispute. That task is the prerogative of national courts[55] and their jurisdiction in that regard is a matter of national law. I shall therefore answer Question 3 in so far as possible.

123. Covered entities, such as credit institutions and payment institutions, may need to collect and verify data pertaining to at least their own customers either in accordance with the Money Laundering Directive or, if subject to stricter provisions as permitted by Article 5 of that directive, under other rules of national law that are consistent with EU law. Where this involves treatment of personal data falling within the scope of the Personal Data Directive (the Money Laundering Directive is not very specific in this regard), the requirements under both directives apply in principle. Recital 33 in the preamble to the Money Laundering Directive confirms this with respect to the disclosure of information under Article 28. So does recital 48, which refers to respecting fundamental rights, thus including the protection of personal data under Article 8 of the Charter.

54 — Interpretative note 15, read together with interpretative note 14, to the 2012 FATF Recommendations contains examples that offer guidance on what are helpful indicators of a high risk. However, the text of note 14 expressly states that these examples may not be relevant in all circumstances. Under item (c) are listed: private banking, anonymous transactions, non-face-to-face business relations or transactions, payment received from unknown or un-associated third parties.

55 — See, for example, the judgments in *Accor*, C-310/09, EU:C:2011:581, paragraph 37 and case-law cited, and *ProRail*, C-332/11, EU:C:2013:87, paragraph 30 and case-law cited.

124. I see no basis for reading 'the customer' in either Article 8(1)(a) [56] or Article 13 so as to refer also to the customer(s) of the customer of the covered entity. These provisions essentially concern the relationship between a covered entity and its customer(s) and transactions undertaken in the context of that relationship. It is of course true that Article 13(4)(c) lists measures to establish the source of wealth and funds involved in a business relationship or transaction with politically exposed persons residing in another Member State or a third country. However, nothing in the request for a preliminary ruling suggests that that is the situation here.

125. That said, I think that the Money Laundering Directive does not necessarily preclude national laws which require or authorise a covered entity, where justified, to obtain information about the customers of its customer. Information about those customers might be relevant to assessing whether the customer of the covered entity, its transactions and business relationships present risks of money laundering or terrorist financing.

126. I do not therefore accept that a covered entity under the Money Laundering Directive may never be authorised or required under national law to seek information about the customers of its own customers in order to prevent money laundering or terrorist financing. Nor does the Personal Data Directive, in particular Article 7, appear to preclude processing of personal data in such circumstances.

127. However, such national laws must also be consistent with that Member State's other obligations under EU law, including the requirements of the Personal Data Directive and Articles 8 and 52(1) of the Charter.

Conclusion

128. In the light of all the above considerations, I suggest that the Court should answer the Audiencia Provincial de Barcelona (Spain) to the effect that:

— Notwithstanding the derogation in Article 11(1), Articles 7 and 13 of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing require Member States to ensure that covered entities apply, in situations involving customers who are themselves covered entities under that directive, (i) standard customer due diligence measures under Articles 8 and 9(1) where there is suspicion of money laundering or terrorist financing within the meaning of Article 7(c); and (ii) enhanced customer due diligence measures under Article 13 in situations foreseen under that provision.

— 'A suspicion of money laundering or terrorist financing' within the meaning of Article 7(c) of Directive 2005/60 arises in particular where, taking into account the individual circumstances of a customer and his transactions (including with respect to the use and management of his account(s)), there are some verifiable grounds showing a risk that money laundering or terrorist financing exists or will occur in relation to that customer. Article 11(1) does not derogate from Article 7(c). Regardless of any derogation, exemption or threshold and thus regardless of whether the customer is or is not a covered entity, Article 7(c) provides that customer due diligence

56 — That being so, I do accept that that provision must be interpreted as covering also all those whose conduct, when acting in the capacity of agent, engages the responsibility of the entity for which they act. Article 9(4), which refers to transactions being carried out by 'the customer or on its behalf', confirms this reading of Article 8(1)(a). That interpretation is also in conformity with recommendation 5 of the 2003 FATF Recommendations and its interpretative note 4 according to which, where the customer is a legal person, the customer due diligence measure of identifying it and verifying its identity includes the obligation to '[v]erify that any person purporting to act on behalf of the customer is so authorised, and identify that person'. See also interpretative note 4 to recommendation 10 of the 2012 FATF Recommendations.

measures are always required where there is suspicion of money laundering or terrorist financing. Where such a suspicion arises, a Member State is therefore precluded from allowing or requiring simplified customer due diligence measures to be applied.

— The fact that the customer is itself an entity covered by Directive 2005/60 does not mean that a Member State must not require enhanced customer due diligence measures within the meaning of Article 13 of that directive to be applied with respect to that customer if, despite the guarantees already provided by Directive 2005/60 and other EU legislation, there exists a higher risk of money laundering and terrorist financing as foreseen by that provision. Article 11 only derogates from standard customer due diligence measures in situations of lower risk. Since it does not refer to Article 13, it has no bearing on the customer due diligence that is required where there is a higher risk.

— Even where Member States have properly transposed Articles 7, 11 and 13 of Directive 2005/60 into national law, Article 5 permits them to adopt or retain in force stricter provisions that seek to strengthen the fight against money laundering or terrorist financing, and confirms that Directive 2005/60 merely provides for a minimum level of harmonisation. The remit of Article 5 of Directive 2005/60 is not limited to the provisions in Chapter II ('Customer due diligence') of that directive. A Member State may therefore provide for customer due diligence measures to be applied by a credit institution in relation to a payment institution even where the conditions of Article 11(1) are satisfied and in situations other than those listed in Articles 7 and 13, where this is justified and otherwise consistent with EU law.

— When Member States act within the freedom left them by Article 5 of Directive 2005/60, they must nevertheless exercise that competence in accordance with EU law, in particular the basic freedoms guaranteed by the Treaties. Where (as here) EU law has not been completely harmonised, national legislation which restricts basic freedoms may be justified because it meets an overriding requirement relating to the public interest, in so far as it is appropriate to secure the attainment of the aim which it pursues and does not go beyond what is necessary in order to attain it.

— Assessing whether the national law is proportionate involves determining the level of protection desired by the Member State with respect to the identified level of risk of money laundering and terrorist financing. Member States may set a level of protection that is higher than that chosen by the EU legislator, identify other situations of (high) risk and authorise or require other customer due diligence measures. Member States must guarantee that the enhanced customer due diligence measures applied are based on assessing the existence and level of a risk of money laundering or terrorist financing with respect to a customer, business relationship, account, product or transaction, as the case may be. In choosing what measures to apply, it is necessary (for both Member States and, where relevant, covered entities) to assess how far the perceived risk is already managed and the desired level of protection already secured by other measures, including those based on Directive 2005/60, Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market and other EU (or national) legislation. Whether a national law is proportionate will also depend on the degree to which the customer due diligence measures for which it provides may intrude upon other protected rights and interests under EU law, such as the protection of personal data (Article 8 of the Charter of Fundamental Rights of the European Union) and the principle of free competition between entities operating in the same market. Finally, whether a national law is proportionate will depend on whether there are alternative, less restrictive means to achieve the same level of protection.

— Covered entities under Directive 2005/60 may not undermine the supervision tasks which competent authorities under Article 21 of Directive 2007/64 are to exercise over payment institutions to verify compliance with the provisions of Title II ('Payment service providers') of the latter directive. Whilst those authorities might, in appropriate circumstances, withdraw the

registration of agents, the branch or the payment institution itself pursuant to that directive, such powers coexist with the preventive measures to be applied by covered entities and the supervisory powers of competent authorities under Directive 2005/60.

— Directive 2005/60 does not necessarily preclude national laws which require or authorise a covered entity, where justified, to obtain information about the customers of its customer. However, such national law must also be consistent with that Member State's other obligations under EU law, including the requirements of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Articles 8 and 52(1) of the Charter of Fundamental Rights of the European Union.