

Guidance for implementation of the  
revised Payment Services Directive

## **PSD2 guidance**



## About the EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.5 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

## General disclaimer

This document (EBF\_020819) constitutes a very preliminary version of the guidance. There are in fact some open questions, concerns and possible alternative interpretations that will hopefully be clarified in the requirements for Regulatory Technical Standards that will be issued by the European Banking Authority before the end of 2016.

© EBF - September 2016

# General Introduction

## About this document

This document offers guidance and is intended to provide high-level assistance to banks in relation to both the interpretation and practical application of the revised Payment Services Directive (PSD2). The document does not aim to be exhaustive in the list of topics it addresses, but rather focuses on specific issues that have been the subject of discussion within the payment industry and/or relate to frequently asked questions from the market.

It should be stressed that this is a living document which will be updated from time to time as necessary. For further information on the PSD EG and for any queries in relation to this document, please contact Pascale-Marie Brien at the European Banking Federation: [p.brien@ebf.eu](mailto:p.brien@ebf.eu).

Finally, it should be noted that no individual who has helped develop this document can accept responsibility whatsoever for any loss or damage caused or suffered by any person who relies upon this document and the guidance contained in it. This document is not intended to constitute legal advice and has no legal status: ultimately, the implementation and interpretation of the PSD2 is a matter for the European Court of Justice, and questions of compliance with the PSD2 as transposed into national law are matters for the relevant national competent authorities and courts. Banks will need to determine for themselves how this guidance applies to their individual circumstances and their particular products and services.

# Contents

I.	STRUCTURE AND OVERVIEW OF THE REVISED PSD.....	5
II.	SCOPE AND DEFINITIONS .....	6
A.	INTRODUCTION.....	6
B.	SCOPE – GUIDANCE AND INTERPRETATION .....	7
C.	KEY DEFINITIONS – GUIDANCE AND INTERPRETATION .....	23
III.	STRONG CUSTOMER AUTHENTICATION .....	26
IV.	AUTHORISATION .....	28
V.	INFORMATION AND CONDITIONS .....	33
VI.	CONSENT .....	42
VII.	SERVICES OFFERED BY PIPS .....	44
VIII.	ACCESS TO PAYMENT ACCOUNTS AND USE OF CREDENTIALS .....	47
IX.	AS PSP LIABILITY .....	50
X.	VALUE DATE AND AVAILABILITY OF FUNDS .....	54
XI.	OPERATIONAL AND SECURITY RISKS .....	58
XII.	TRANSPOSITION .....	63
XIII.	ANNEX A .....	65

# Figures

<i>Figure 1 – Geographical scope of PSD2.....</i>	<i>7</i>
<i>Figure 2 – Scope of PSD2 .....</i>	<i>9</i>
<i>Figure 3 – Scope of PSD2 in Correspondent Banking.....</i>	<i>10</i>
<i>Figure 4 – PSD2 extension of the scope in Title III .....</i>	<i>15</i>
<i>Figure 5 – PSD2 extension of the scope in Title IV.....</i>	<i>17</i>
<i>Figure 6 – PSD2 description of CISP.....</i>	<i>45</i>
<i>Figure 7 – PSD2 transposition and EBA mandates timeline .....</i>	<i>64</i>
<i>Figure 8 – Member States exemptions and derogations.....</i>	<i>65</i>

## I. STRUCTURE AND OVERVIEW OF THE REVISED PSD

The revised PSD2 has preserved the structure of PSD1 in terms of the split into sections (Titles) and subdivision into consistent content areas: subject matter, scope and definitions (Title I), payment service providers and specifically the regulation of payment institutions (Title II), conditions for transparency and information requirements for payment services (Title III) and rights and obligations in relation to the provision and use of payment services (Title IV), followed by the power conferred on the European Commission to adopt delegated acts and regulatory technical standards (Title V) and final provisions (Title VI).

The revision of the PSD text has led to a retention of much of the original text, although some wording has been partially amended, and new provisions have been inserted. The PSD2 fully repeals and replaces the 2007 PSD (Directive/64/EC). Member States are required to adopt the majority of the measures necessary to comply with the Directive by 13 January 2018 and apply them starting from the same date.

It is also important to note that under PSD2 the Level 2 legislative process applies, in which the European Banking Authority (EBA) has been given the mandate to develop Regulatory Technical Standards (RTS) and guidelines across a number of provisions, which will come into place in the coming years.

PSD2 widens the scope of the PSD by covering new services and players by extending the scope of existing services (payment instruments issued by payment service providers that do not manage the account of the payment service user), enabling third parties to be able to initiate payments and access payment account data based on explicit customer consent.

PSD2 also updates the telecom exemption by limiting it mainly to micro-payments for digital services. In addition, PSD2 extends the scope to all currencies -not just Member States'- and includes transactions with third countries when only one of the payment service providers is located within the European Economic Area ("one-leg transactions"). It also enhances cooperation and information exchange between authorities in the context of authorisation and supervision of payment institutions. The European Banking Authority (EBA) will develop a central register of authorized and registered payment institutions.

To make electronic payments safer and more secure, PSD2 introduces enhanced security measures to be implemented by all payment service providers, including banks. To that end, the EBA will develop Regulatory Technical Standards, covering strong customer authentication and secure communication.

## II. SCOPE AND DEFINITIONS

### A. INTRODUCTION

This Directive continues to apply to “payment services provided within the Union”. It will be transposed in all Member States of the European Union and the European Economic Area (EEA), this currently consists of 28 EU Member States plus three Member States of the European Economic Area (Norway, Iceland and Liechtenstein). Please note that the overseas territories of EU Member States are not shown on the map.

## Geographical Scope of PSD2

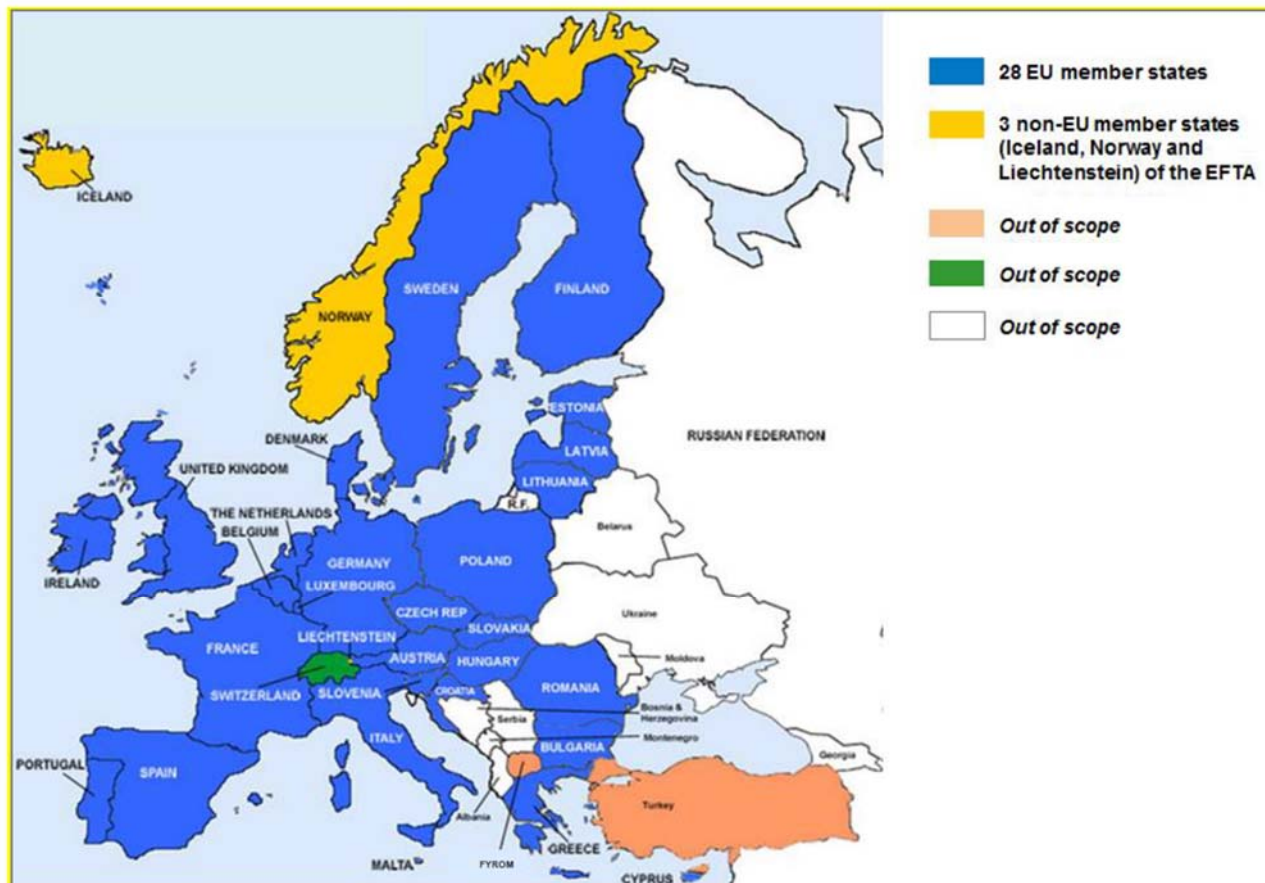


Figure 1 – Geographical scope of PSD2

## B. SCOPE – GUIDANCE AND INTERPRETATION

### Article Reference

### Articles 2(2), Article 2(3) and Article 2(4) – Scope

2. Titles III and IV apply to payment transactions in the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, within the Union.

3. Title III, except for point (b) of Article 45(1), point (2) of Article 52 and point (a) of Article 56, and Title IV except for Articles 81 to 86, apply to payment transactions in a currency that is not the currency of Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transactions, located within the Union, in respect of those parts of the payments transaction which are carried out in the Union.

4. Title III, except for point (b) of Article 45 (1), point (2)(e) of Article 52, point (5)(g) of Article 52 and point (a) of Article 56, and Title IV, except for Article 62(2) and (4), Articles 76, 77, 81, 83(1), 89 and 92, apply to payment transactions in all currencies where only one of the payment service providers is located within the Union, in respect of those parts of the payments transaction which are carried out in the Union.

## Guidance and interpretation

As for PSD1, PSD2 applies to intra-EEA payments in EEA currencies. However, although retaining the same basic structure of the text, the reach of PSD2 is broader than PSD1 due to the extension of the scope to:

1. Intra-EEA payments (two-legs in) in non-EEA currencies
2. Payments to and from non-EEA countries (one-leg in or out) in any currency

It is important to be aware of the difference between the Single Euro Payments Area (SEPA) and the scope of PSD2 as the jurisdictional scope of the SEPA Schemes extends beyond the European Economic Area (EEA) countries. Our understanding is that payments made in accordance with the SEPA Regulation (Regulation (EU) No 260/2012) and the SEPA Schemes, to or from countries and territories outside the EEA (e.g. Switzerland, Monaco, San Marino and the British Crown Dependencies), or which might be seen as 'domestic' (e.g. GBP from the UK to Jersey) – even if those countries or territories pass equivalent legislation – should be treated as one-leg transactions under PSD2.



## Extension of the scope of PSD2

### Article 2: Scope

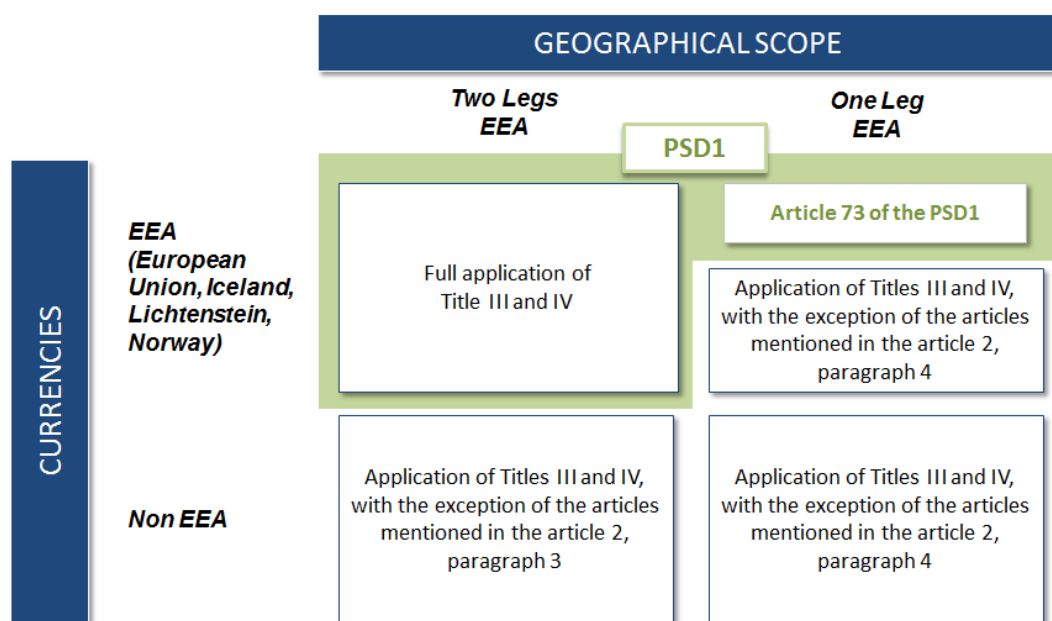


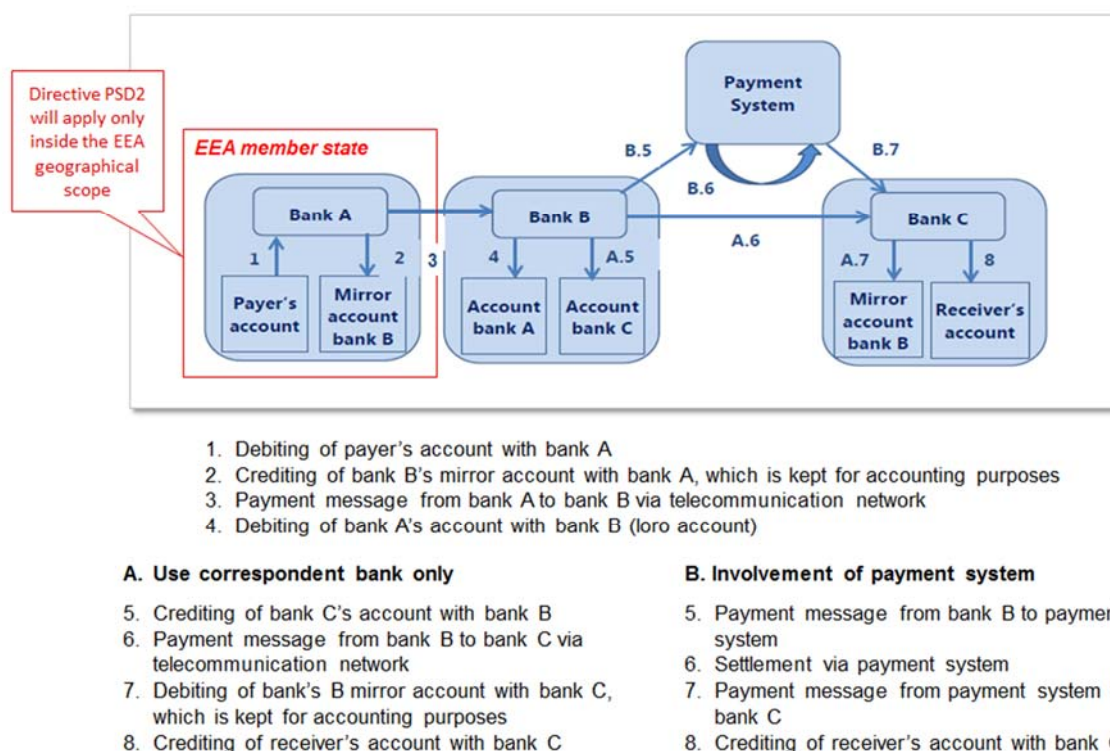
Figure 2 – Scope of PSD2

These extensions, under PSD2, apply only to those parts of the transaction that are carried out within the EEA. The wording “in respect of those parts of the payment transaction which are carried out in the Union” operates as a limit to the reach of PSD2 and seeks to clarify that Payment Service Providers (PSPs) cannot be in a position to fulfil their obligations in respect of transactions (or components thereof) taking place outside of the EEA over which they do not have any control. Parts of Title III and IV are extended to one-leg transactions and non-EEA currencies as long as it is feasible for PSPs to comply. Specifically, where a conversion between a currency different from the one of the payee's/payer's account is needed, it is important to remember that **conversions between an EEA currency and a non EEA currency or two non EEA currencies fall outside the scope of PSD2**. In addition, as with PSD1, PSD2 does not apply to the inter-PSP space, but to the customer to PSP relationship. In summary, PSD2 applies only to the part of the transaction that is taking place within the EU.

The below figure illustrates at a high level the process of international correspondent banking and helps to identify where PSD2 rules and geographical scope apply. It depicts a cross-border transaction initiated in the EEA, Bank A is the payer's PSP located in the EEA, Bank B is the correspondent bank or intermediary PSP – in this example located outside the EEA – and Bank C is the beneficiary PSP, located outside the EEA. The payment system is the system that is clearing the specific foreign currency at a domestic level, e.g. US dollar in the US.

There are various methods of making an international payment and further detail in relation to the application of PSD2 articles can be found below.

## Payments settlement via Correspondent Banking



Source: ECB, Ninth survey on correspondent banking in euro, 2015, adapted from Danmarks National bank, Payment systems in Denmark, 2005.

NB: Bank A is the payer's PSP, Bank B is the intermediary PSP or correspondent bank, and Bank C is the payee's PSP or beneficiary bank.

Figure 3 – Scope of PSD2 in Correspondent Banking

The following section provides a more detailed overview of how the various provisions of the PSD2 scope under Article 2 apply in practice.

### 1) Article 2(1): This Directive applies to payment services provided within the Union.

This provision relates to “payment services” as defined in Article 4(3) and the business activities listed in Annex 1 of PSD2. We understand the term “Union” to mean EEA Member States – i.e. the EU Member States and Norway, Iceland and Liechtenstein, in line with the application of PSD1.

**2) Article 2(2):** *Titles III and IV apply to payment transactions in the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union.*

Article 2(2) in summary:

Title III and Title IV apply to intra-EEA payments in EEA currencies (as per PSD1)

- The payer's PSP and the payee's PSP are both located in the EEA.
- The Payment Services User (PSU) has asked for the payment to be made in an EEA currency.
- Titles III & IV i.e. all transparency and information requirements and rights and obligations, covering e.g. charges payable, where applicable an actual or reference exchange rate, value date and maximum execution time) apply.
- Art 62(2) – whereby the payee pays the charges levied by his PSP, and the payer pays the charges levied by his PSP - applies to intra-EEA payments in EEA currencies whether or not there is a currency conversion. Share (SHA) option applies.
- In line with Article 81, no deductions of charges are allowed from the full amount of a payment transaction, except by the payee's PSP where agreed with the payee. In which case the full amount and charges must be shown separately in the information given to the payee.
- For payments within the scope of Article 82(1) the default maximum execution time is D+1, otherwise a longer execution time of up to a maximum of D+4 can be agreed between the PSU and the PSP.

Article 2(2) example scenarios:

- GBP payment within the UK between GBP denominated accounts a/cs (no currency conversion)
- DKK payment from Denmark to UK between DKK denominated account and GBP denominated account (with currency conversion)
- SEPA payment<sup>1</sup> from France to UK between EUR denominated account and a GBP denominated account (with currency conversion)

**3) Article 2(3):** *Title III, except for point (b) of Article 45(1), point (e) of Article 52(2) and point (a) of Article 56, and Title IV, except for Articles 81 to 86, apply to payment transactions in a currency that is not the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.*

---

<sup>1</sup> In the EPC SCT and SDD Clarification Paper (EPC348-12 v2.1, page 11): reference is made to Section 2.4 of the SCT Rulebook which states that: "all transactions are in euro in all process stages". In other words the amount of the transaction must remain unchanged and expressed in euro until it reaches the Beneficiary Bank. This also means that currency conversion of an SCT to be debited from a non-euro account can only be carried out by the Originator Bank".

### Article 2(3) in summary:

Title III and Title IV, subject to certain exceptions, apply to intra-EEA payments in non-EEA currencies in terms of the parts of the transaction carried out in the Union.

- The payer's PSP and the payee's PSP are both located in the EEA.
- The PSU has asked for the payment to be made in a non-EEA currency.
- As it is the location of the payer's PSP and the payee's PSP which is relevant, intra-EEA payments in non-EEA currencies should be treated as a "single" payment transaction even though part of the transaction is outside the EEA for foreign currency clearing purposes, and therefore those parts are not under PSD2.
- All transparency and information requirements apply except for those dealing with maximum execution time as such information cannot be guaranteed in advance of the payment being made by the PSP in the EEA.
- Article 62(2) - whereby the payee pays the charges levied by his PSP, and the payer pays the charges levied by his PSP - applies to intra-EEA payments in non-EEA currencies whether or not there is a currency conversion. SHA option applies.
- While Articles 76 and 77 concerning direct debit refunds and requests for refund do, in theory, apply, in practice no non-EEA currency direct debit scheme or process currently operates in the EEA.
- Article 81 does not apply as the full amount principle cannot be guaranteed end-to-end. Any processes associated with foreign (non-EEA) currency clearing are outside the scope of PSD2.
- Articles 82 to 86 do not apply.

### Article 2(3) example scenarios:

- USD payment within the EEA (no currency conversion) e.g. from UK USD a/c to France USD a/c
- USD payment within the EEA (with currency conversion) e.g. from France USD a/c to UK GBP a/c using the "serial method" (see figure X below).
- AUD payment within the EEA from France to the UK using the "direct plus cover" method (see figure Y below).

Figure X

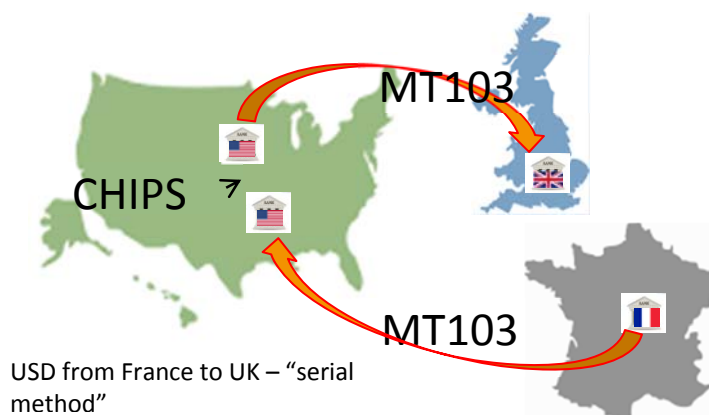
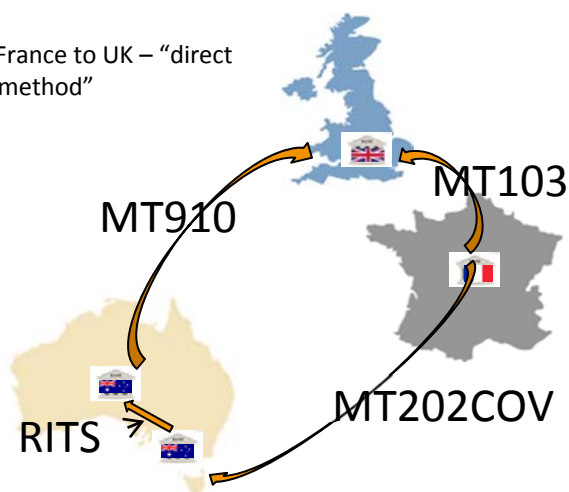


Figure Y

AUD from France to UK – “direct plus cover method”



**4) Article 2(4):** Title III, except for point (b) of Article 45(1), point (e) of Article 52(2), point (g) of Article 52(5) and point (a) of Article 56, and Title IV, except for Article 62(2) and (4), Articles 76, 77, 81, 83(1), 89 and 92, apply to payment transactions in all currencies where only one of the PSPs is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.

#### Article 2(4) in summary:

Title III and Title IV, with certain exceptions, apply to one-leg payments in all currencies in terms of the parts of the transaction carried out in the Union.

- In the context of one-leg **out** payments, the payer's PSP is located in the EEA but the payee's PSP is located outside the EEA.
- In the context of one-leg **in** payments, the payer's PSP is located outside the EEA but the payee's PSP is located in the EEA.
- All transparency and information requirements apply except for those dealing with maximum execution time and conditions for Direct Debit refund.
- Article 62(2) - whereby the payee pays the charges levied by his PSP, and the payer pays the charges levied by his PSP - does not apply to one leg payments in EEA or non-EEA currencies. OUR, SHA and BEN options can be used.
- Article 71(1) i.e. the 13 month timeframe, in which the PSU can obtain rectification from his PSP upon notification of unauthorised or incorrectly executed payment transactions, applies. This period of 13 months does not necessarily apply in all markets outside the EEA. In some countries the record keeping timeframes can be as short as 6 months, which would mean that if a claim was made after this time, the merchant may no longer be in possession of the necessary records.
- Articles 76 and 77 regarding direct debit refunds and refund requests do not apply as refunds of authorised payment transactions may only be managed within the EEA. Please note that, in case of non-EU/EEA currency direct debit refunds, there is currently no non-EEA currency direct debit process operating in Europe.

- Article 81 does not apply. The full amount principle (and sharing of charges principle as per Article 62(2)) is not applicable if one of the PSPs involved is outside the EEA.
- Article 82(2) applies to one-leg payments with the exceptions of execution times (see below) the PSP and the PSU may agree on a longer period than the one set in Article 83 for intra-Union payment transactions.
- Article 83(1) does not apply as time limits cannot be guaranteed by the PSP in the EEA.
- Article 83(2) and 83(3) do apply as these provisions are based on the scope of Article 87.
- While Article 86 does in theory apply, its scope is limited to national payments made in Member State currency (unchanged from PSD1).
- Article 87 (1) and (2) apply, meaning that the credit value date for one-leg in payments should be not later than the business day on which the amount is credited to the payee's PSP account (and the PSP is in a position to acknowledge receipt of the funds, also in consideration of different time zones and different banking calendars). If the credit to the payee's PSP's account was on a non-business day, the funds should be credited and made available to the payee no later than the following business day. Once the payee's PSP account has been credited and the PSP has all the information necessary to credit the amount on the payee's account, the payee's PSP should make the funds immediately available to the payee - including payments within the same PSP- **where there is no currency conversion** or where there is a currency conversion between the euro and a Member State currency or between two Member States currencies. Any extension of scope in relation to non-EEA currencies is limited to instances where the conversion takes place before the payee's PSP has received the funds see for example Article 82(2).
- Article 89 liability provisions do not apply.
- Article 92 right of recourse provisions do not apply.

#### Example Scenarios:

- One-leg Out – in EEA currency: EEA currency sent from the EEA to a non-EEA country (with or without currency conversion) e.g. EUR payment from France to Japan or CHF<sup>2</sup> from Liechtenstein to Switzerland.
- One-leg Out – in non-EEA currency: Non-EEA currency sent from the EEA to a non-EEA country (with or without currency conversion) e.g. USD payment from UK to USA.
- One-leg in – in EEA currency: EEA currency payment sent from a non-EEA country to an EEA country (with or without currency conversion) e.g. EUR payment from Japan to France.
- One-leg in – in non-EEA currency: Non-EEA currency sent from a non-EEA country to an EEA country (with or without currency conversion) e.g. USD payment from USA to UK.

#### ***Articles excluded by the scope extension***

Titles III and IV are not considered entirely applicable to all payment transactions in non-EEA currencies and/or partially executed inside the EEA. Some articles have therefore been specifically excluded and do not apply to the extended PSD2 scope.

---

<sup>2</sup> Liechtenstein is an EEA country whereas Switzerland is not. However, the Swiss Franc (CHF) is the official currency of Liechtenstein and thus counts as an EEA currency.



### Key

**A:** Applicable to intra-EEA payments in EEA currencies (Article 2.2)

**B:** Applicable to intra-EEA payments in non-EEA currencies (Article 2.3)

**C:** Applicable to one Leg payments in all (EEA and non-EEA) currencies (Article 2.4)

### **Title III: Application in light of the extension of the scope of PSD2 and related specific articles**

Title & Articles	Description	PSD1	PSD2 and comments
<b>Title III (from art. 38 to 60 with the exception of the articles mentioned below)</b>	<b>Transparency</b> of conditions and information requirements for payment services	<b>A</b>	<b>A, B, C</b> In addition to applying in full to intra-EEA payments in EEA currencies, PSD2 extends the application of Title III - with certain exceptions – to intra-EEA payments in non-EEA currencies and to one-leg payments in all currencies
<b>Article 45 par 1 point b)</b>	<i>Information and conditions (Single payment transactions):</i> Member States shall ensure that the following information and conditions are provided or made available by the PSP to the PSU: <b>b) the maximum execution time for the payment service to be provided;</b>	<b>A</b>	<b>A</b>
<b>Article 52 par 2 point e)</b>	<i>Information and conditions (Framework contracts):</i> Member States shall ensure that the following information and conditions are provided to the PSU: on use of the payment service: <b>e) maximum execution time for the payment services to be provided;</b>	<b>A</b>	<b>A</b>
<b>Article 52 par 5 point g)</b>	<i>Information and conditions (Framework contracts):</i> Member States shall ensure that the following information and conditions are provided to	<b>A</b>	<b>A, B</b>

	the PSU: on safeguards and corrective measures: <b>g) the conditions for refund in accordance with Articles 76 and 77;</b>		
<b>Article 56 point a)</b>	<i>Information before execution of individual payment transactions:</i> In the case of an individual payment transaction under a framework contract initiated by the payer, a payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on all of the following: <b>a) maximum execution time;</b>	<b>A</b>	<b>A</b>

Figure 4 – PSD2 extension of the scope in Title III



## Title IV: Application in light of the extension of the scope of PSD2 and related specific articles

Title & Articles	Description	PSD1	PSD2 and Comments
<b>Title IV</b> <b>(with the exception of the articles mentioned below)</b>	<b>Rights and obligations</b> in relation to the provision and use of payment services	<b>A</b>	<b>A, B, C</b>  PSD2 extends the application of Title IV - with certain exceptions – to intra-EEA payments in non-EEA currencies and to one-leg payments in all currencies.
<b>Article 62 par 2 and 4</b>	<i>Charges applicable</i>  (2) Member States shall require that for payment transactions provided within the Union, where both the payer's and the payee's PSPs are, or the sole PSP in the payment transaction is, located therein, the payee pays the charges levied by his PSP, and the payer pays the charges levied by his PSP ( <b>SHA option</b> ).  (4) In any case, Member States shall ensure that the <b>payee shall not request charges</b> for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751] and for those payment services to which Regulation (EU) No 260/2012 applies.	<b>A</b>	<b>A, B</b>
<b>Article 71</b>	<b>The payment service user shall obtain rectification of an unauthorised or incorrectly executed transaction from the PSP only if the payment service user notified the PSP without undue delay of becoming aware of any such transaction giving rise to a claim, including that under Article 89, and no</b>	<b>A</b>	<b>A, B, C</b>

	<b>later than 13 months after the debit date....</b>		
<b>Article 76</b>	<i>Refunds for payment transactions initiated by or through a payee:</i> (..) The payer has an unconditional right to a refund within the time limits laid down in Article 77 of this Directive. (..)	<b>A</b>	<b>A, B</b>
<b>Article 77</b>	<i>Requests for refunds for payment transactions initiated by or through a payee:</i> (1) Member States shall ensure that <b>the payer can request the refund</b> referred to in Article 76 of an authorized payment transaction initiated by or through a payee <b>for a period of eight weeks from the date on which the funds were debited.</b> (2) Within 10 business days of receiving a request for a refund, <b>the PSP shall either refund the full amount</b> of the payment transaction <b>or provide a justification for refusing the refund</b> and indicate the bodies to which the payer may refer the matter in accordance with Articles 99 to 102 if the payer does not accept the reasons provided. (..)	<b>A</b>	<b>A, B</b>
<b>Article 81</b>	<i>Amounts transferred and amounts received (Execution of payment transactions):</i> Member States shall require the PSPs of the payer, the PSPs of the payee and any intermediaries of the PSP to <b>transfer the full amount of the payment transaction and refrain from deducting charges</b> from the amount transferred. (..)	<b>A</b>	<b>A</b>
<b>Article 82</b>	<i>Scope ( Section 2 – Execution time and value date):</i> (1) a) payment transactions <b>in euro</b> ; b) national payment transactions in the currency of the Member State <b>outside the euro area</b> ; c) payment transactions involving only <b>one currency conversion</b> between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member	<b>A</b>	<b>A, C</b>

	State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro. (2) To <b>payment transactions not referred to in the paragraph 1</b> , unless otherwise agreed between the PSU and the PSP, with the exception of Article 87 (...)		
<b>Article 83 par 1</b>	<i>Payment transactions to a payment account (Execution time &amp; value date):</i> the payer's PSP shall ensure that after the time of receipt as referred to in Article 78, the <b>amount of the payment transaction will be credited to the payee's PSP's account by the end of the following business day</b> . That time limit may be <b>extended by a further business day for paper-initiated payment transactions</b> .	<b>A</b>	<b>A</b>
<b>Article 83 par 2 and 3</b>	<i>Payment transactions to a payment account (Execution time &amp; value date):</i> the PSP of the payee shall <b>value date and make available the amount</b> of the payment transaction <b>to the payee's payment account</b> after the PSP has received the funds in accordance with Article 87; the payee's PSP shall <b>transmit a payment order</b> initiated by or through the payee to the payer's PSP <b>within the time limits agreed between the payee and the PSP (..)</b>	<b>A</b>	<b>A, C</b>
<b>Article 84</b>	<i>Absence of payee's payment account with the PSP (Execution time &amp; value date):</i> Where the payee does not have a payment account with the PSP, the <b>funds shall be made available to the payee by the PSP</b> who receives the funds for the payee <b>within the time limit laid down in Article 83</b> .	<b>A</b>	<b>A, C</b>
<b>Article 85</b>	<i>Cash placed on a payment account (Execution time &amp; value date):</i> Where a consumer places cash on a payment account with that PSP in the currency of that payment account, the PSP shall ensure that <b>the amount is made</b>	<b>A</b>	<b>A, C</b>

	<b>available and value dated immediately after receipt of the funds.</b> Where the PSU is not a consumer, the amount shall be made available and value dated at the latest on the following business day after receipt of the funds.		
<b>Article 86</b>	<i>National payment transactions (Execution time &amp; value date):</i> For national payment transactions, Member States may provide for <b>shorter maximum execution times</b> than those provided for in this Section.	<b>A</b>	<b>A, C</b>
<b>Article 87</b>	<i>Value date and availability of funds:</i> the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's PSP's account where, on the part of the payee's PSP, there is: (a) <b>no currency conversion</b> ; or (b) a <b>currency conversion</b> between the euro and a Member State currency or between two Member State currencies.	<b>A, C</b>  Under PSD1, C only applied to EEA currencies	<b>A, B, C</b>  Please note the link to Article 83 (part 2 and 3). Any expansion of scope in relation to non-EU/EEA currencies is limited to instances where the conversion takes place before the payee's PSP has received the funds.
<b>Article 89</b>	<i>PSPs' liability for non-execution, defective or late execution of payment transactions</i>	<b>A</b>	<b>A, B</b>
<b>Article 92</b>	<i>Right of recourse (Section 3 - Liability)</i>	<b>A</b>	<b>A, B</b>

Figure 5 – PSD2 extension of the scope in Title IV

It is important to remember that in the national transposition of PSD1 some Member States implemented all or parts of Titles III and IV of the Directive to one-leg payments and/or to all currencies. Therefore, the present guideline identifies the differences between the scope of PSD1 and PSD2, while the exact identification of the implementation gaps between the current rules and the ones that will be in force once PSD2 will be implemented can only be made at the level of each Member State where the PSP provides services.

Furthermore, PSD2 has maintained some options for the Member States about a number of exemptions and derogations. For the complete list of 'opt in/out' made available in the Member State see ANNEX A.

## Article Reference

### Article 3 - Exclusions

The Directive does not apply to the following preserved exclusions of the scope:

- Cash payments from the payer to the payee (though any cash transaction involving movement to or from a payment account will be caught)
- Cheques and paper instruments
- Cash transportation (e.g. cash deliveries by commercial security companies)
- Payment services associated with securities asset servicing (e.g. dividend payments)
- Technical services
- independent ATM deployers (adding an obligation to provide information to the customer on any withdrawal charges before carrying out the withdrawal and on receipt of the cash at the end of the transaction)
- Commercial agents (on behalf of the payee or of the payer, but not for both parties);

The exclusions were revised in two cases by limiting more precisely the scope and by adding the obligation to supply information to the competent Authority.

### Article 3(k)

*k) services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions:*

- (i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer;*
- (ii) instruments which can be used only to acquire a very limited range of goods or services;*
- (iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;*

## Guidance and interpretation

This exclusion provides a more precise definition of “limited instrument/network” than PSD1. This new definition is in line with the definition of limited networks set out in Directive 2009/110/EC. Recitals 13 and 14 set this exclusion in a broader context (e.g. “*it should not be possible to use the same instrument to make payment transactions to acquire goods and services within more than one limited network or to acquire an unlimited range of goods and services*”) that further helps understanding that the provision is intended to avoid specific-purpose instruments developing into general purpose ones.

In order to prevent any circumvention of the rule, the service providers carrying out the activities mentioned in the exclusion and whose total value of payment transactions executed exceeds the amount of EUR 1 million per year, are required according to Article 37(2) to send a notification to the competent authority with reference to the exclusion under which they provide the services. On the basis of that notification, the competent authority shall inform the PSP whether the activity perimeter falls into a “limited network” or not.

## Article 3(I)

*l) payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service:*

- (i) for purchase of digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or*
- (ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;*

*provided that the value of any single payment transaction referred to in points (i) and (ii) does not exceed EUR 50 and:*

- the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or*
- where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month;*

## Guidance and interpretation

The exclusion of payments offered by telecom operators has been further specified and narrowed down. The exclusion now covers only payments made through telecom operators for the purchase of digital services such as music and digital newspapers that are downloaded on a digital device or of electronic tickets or donations to charities.

These provisions have changed significantly from the PSD1 telecom exemption. The intention is to ease the purchasing of tickets for an event or for transport through an electronic device as part of the provision of electronic communication services. Context is provided by Recital 15, which refers to services such as entertainment (chat, downloads, news and sport updates, directory enquiries, radio and TV participation such as voting) and Recital 16, which gives examples of electronic tickets such as transport, entertainment, car parking, and entry to venues. There are new definitions in Article 4(41) (“electronic communication network”), Article 4(42) (“electronic communication service”) and Article 4(43) (“digital content”). Such ticketing services would typically be offered and charged by a telecommunication company as part of its product offering. The law applicable to the contract between the client and the company applies to the purchasing of e-tickets via the provider of telecommunication services.

Concerning the reference to charitable activity, Recital 16 states that “*Member States should, in accordance with national law, be free to limit the exclusions to donations collected in favour of*

*registered charitable organisations". The specified threshold aims to limit the exclusion clearly to payments with a low risk profile.*

Providers that leverage on the exclusion shall yearly inform the competent authority of the results of a specific audit, testifying that the activity complies with the limits of the transactions amount limit set out in art. 3.

### Article 3 (n)

*(n) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group;*

### Guidance and interpretation

The application of Article 3(n) under PSD1 has led to differences in interpretation at a Member State level. In this context it is worth noting that Recital 17 provides additional clarification, stating that *"The Single Euro Payments Area (SEPA) has facilitated the creation of Union wide - 'payment factories' and 'collection factories', allowing for the centralisation of payment transactions of the same group. In that respect payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking provided by a payment service provider belonging to the same group should be excluded from the scope of this Directive. The collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to a payment service provider should not be considered to be a payment service for the purposes of this Directive"*.

Practical examples would include cases where collections are made on behalf of subsidiaries of a payment factory.

## C. KEY DEFINITIONS – GUIDANCE AND INTERPRETATION

Some key definitions (for example: 'payment account', 'business day', 'framework contract') remain the same, while some others, not previously included in the PSD1, were added (for example: "acquiring" of payment transactions), thus solving previous interpretative difficulties. Moreover, definitions contained in the relevant Regulations adopted after 2007 were considered as a point of reference for the new definitions and included in PSD2 (for example: 'credit transfer' taken from Regulation (EU) No. 260/2012).

The main new items in the definitions are related to the new services listed in Annex I of the Directive (e.g. "payment initiation service", "account information service", "account servicing payment service provider", "payment initiation service provider" and "account information service provider"), as well as to the provisions regarding security measures and management (e.g.: "authentication", "strong customer authentication", "personalised security credentials" and "sensitive payment data").



## Article Reference

### Article 4 (15) Definitions

15. *“‘payment initiation service’ means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.”*

## Guidance and interpretation

Instead of a generic ‘initiation of a payment transaction’, Recitals 27 and 29 outline some scenarios where the definition of Payment Initiation Service would apply to help avoid confusion with other definitions (e.g. direct debits). In fact, Recital 27 describes payment initiation services playing *“a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer’s bank in order to initiate payments on the basis of a credit transfer”*. Recital 29 refers to such services as enabling *“the PISP to provide comfort to a payee that the payment has been initiated in order to provide an incentive to the payee to release goods or to deliver the service without undue delay. Such services offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards”*.

Therefore, the definition of Payment Initiation Services (PIS) shall be considered in the context of an online scenario where, often, the PISP’s contractual relationship is with the merchant. Payers could use a payment initiation service to initiate a transaction (on a one-off or ad-hoc basis) via the merchant’s web site leveraging online banking services made available by the AS PSP (“accessible on line”) and for which the user needs to be registered. There may also be situations where PIS take place as an add-on service alongside Account Information Services (where the provider has the necessary authorisation), for example to move funds from one payment account to another.

## Article Reference

### Article 4(16)

16. *“‘account information service’ means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.”*



## Guidance and interpretation

The aggregation of information on payment accounts is offered to PSUs in some European countries and it allows clients to obtain a consolidated view on their payment accounts. For that purpose, clients allow a provider to access information from their payment accounts and to provide services based upon the account information related to their payment accounts.

There are many features and information around a payment account (terms, conditions, fees) that can also be connected to services (mortgages, loans, deposits) that differ from the payment services ones. The definition does not specify which type of information the Account Information Services Provider (AISP) shall make available to the user. However, Recital 28 states that, through AIS, the payment service user is able to have an “overall view of its financial situation” from many payment accounts and article 67(2) (d) provides that the AIS providers “access only the information from designated payment accounts and associated payment transactions”.

By combining the two above mentioned criteria it appears that the information the payer’s AS PSP shall make available concerns the updated account balances of the payment accounts (e.g. current account, credit card accounts etc.) and payment account debit / credit entries related to the payment transactions as within the scope in the Directive (only if the payment account is accessible on line, i.e. online banking). In all circumstances, the PSU has chosen to use online banking.

### III. STRONG CUSTOMER AUTHENTICATION

This chapter has been put on hold until further clarification is provided by the European Commission and the forthcoming European Banking Authority Regulatory Technical Standard on strong customer authentication and secure communication.

#### Article Reference

##### Article 4(6) - Definitions

6. *“‘remote payment transaction’ means a payment transaction initiated via internet or through a device that can be used for distance communication;”*

#### Guidance and interpretation

A remote payment is made when the PSU is not physically present at the point of sale: the interaction between the merchant and the client is ensured via internet through an electronic communication device such as computers, tablets and mobile phones.

As a consequence, mobile contactless NFC payments are not considered remote as the PSU is physically present at the point of interaction when initiating a payment.

#### Article Reference

##### Article 4(30) - Strong customer authentication

30. *“‘strong customer authentication’ means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;”*

##### Article 97(1) and (2) - Authentication

1. *“Member States shall ensure that a payment service provider applies strong customer authentication where the payer:*

- (a) accesses its payment account online;*
- (b) initiates an electronic payment transaction;*
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*

*2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee."*

## **Article 98(1) and (3) - Regulatory technical standards on authentication and communication**

*1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:*

*(a) the requirements of the strong customer authentication referred to in Article 97(1) and (2);*  
*(b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article;*

*(c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and*

*(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.*

*3. The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria:*

- (a) the level of risk involved in the service provided;*
- (b) the amount, the recurrence of the transaction, or both;*
- (c) the payment channel used for the execution of the transaction.*

## **Guidance and interpretation**

The scope of the strong customer authentication requirements in the PSD2 are wider than under the EBA guidelines since the PSD2 requirements apply to all "electronic payments" (including e.g. card-present transactions), whereas the requirements in the EBA guidelines only apply to "Internet payments". The EBA Guidelines will be superseded by the EBA regulatory technical standards on strong customer authentication and secure communication.

Further clarification will be provided at a later stage.

## IV. AUTHORISATION

### Article Reference

#### Article 5 – Applications for authorisation

*1. For authorisation as a payment institution, an application shall be submitted to the competent authorities of the home Member State, together with the following:*

- (a) a programme of operations setting out in particular the type of payment services envisaged;*
- (b) a business plan including a forecast budget calculation for the first 3 financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;*
- (c) evidence that the payment institution holds initial capital as provided for in Article 7;*
- (d) for the payment institutions referred to in Article 10(1), a description of the measures taken for safeguarding payment service users' funds in accordance with Article 10;*
- (e) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, which demonstrates that those governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;*

#### Guidance and Interpretation

Under PSD2, Payment Institutions (PIs) are required to fulfil a variety of requirements in order to obtain an authorisation to provide payment services. These requirements are largely the same as under PSD1. The main changes relate to the enhanced levels of payment security under PSD2. Entities that wish to be authorized as a payment institution shall provide a security policy document together with their application, as well as a description of security incident management procedure, contingency procedures etc. Capital requirements which aim to ensure financial stability have largely remained the same under PSD2 as they were set out in PSD1.

Payment Initiation Service Providers (PISPs) will have to be authorized and AISPs registered with the competent authority in their home Member State, setting out the business plan and operating model, demonstrating appropriate levels of initial and working capital, setting out risk management, financial controls, fraud and security monitoring, and business continuity arrangements. PISPs and AISPs must hold a professional indemnity insurance or comparable guarantee to cover their liabilities in this respect. The EBA will provide guidance on how much this should be.

## Article Reference

### Article 14 - Registration in the home Member State

*1. Member States shall establish a public register in which the following are entered:*

*(a) Authorised payment institutions and their agents;*

*(b) Natural and legal persons benefiting from an exemption pursuant to Article 32 or 33, and their agents; and*

*(c) the institutions referred to in Article 2(5) that are entitled under national law to provide payment services.*

*Branches of payment institutions shall be entered in the register of the home Member State if those branches provide services in a Member State other than their home Member State.*

*2. The public register shall identify the payment services for which the payment institution is authorised or for which the natural or legal person has been registered. Authorised payment institutions shall be listed in the register separately from natural and legal persons benefiting from an exemption pursuant to Article 32 or 33. The register shall be publicly available for consultation, accessible online, and updated without delay.*

*3. Competent authorities shall enter in the public register any withdrawal of authorisation and any withdrawal of an exemption pursuant to Article 32 or 33.*

*4. Competent authorities shall notify EBA of the reasons for the withdrawal of any authorisation and of any exemption pursuant to Article 32 or 33.*

### Article 15(1) - EBA register

*1. EBA shall develop, operate and maintain an electronic, central register that contains the information as notified by the competent authorities in accordance with paragraph 2. EBA shall be responsible for the accurate presentation of that information.*

*EBA shall make the register publicly available on its website, and shall allow for easy access to and easy search for the information listed, free of charge.*

## Guidance and interpretation

The EBA register of PIs, persons and institutions referred to under Article 14(1), points b) and c) could perform the functionality of a secure PISP / AISP on line authentication. This is essential to allow the PSP to check the authorisation / registration status of the PISP / AISP and Card-Based Payment Instrument Issuer. It should however be noted that the only legally binding registers will be managed by each respective Member State.

The Discussion Paper from the EBA (dated December 2015) does not clarify whether as part of the RTS on strong customer authentication and secure communication the register will satisfy

this requirement, i.e. if it will be available 24/7/365 and promptly modified in case of change of the PISP/AISP status. This is particularly important due to the consequences on the payment transaction's chain and the related liabilities among the PSPs involved in the specific payment transaction, given that only registers held at national level will be legally binding.

## Article Reference

### Article 33 (1) Account information service providers

1. Natural or legal persons **providing only the payment service as referred to in point (8) of Annex 1** shall be exempt from the application of the procedure and conditions set out in Sections 1 and 2, with the exception of points (a), (b), (e) to (h), (j), (l), (n), (p) and (q) of Article 5(1), **Article 5(3)** and Articles 14 and 15. **Section 3 shall apply**, with the exception of Article 23(3).

## Guidance and interpretation

Article 5(3) states that AISPs do not need to be authorised by the competent authority but they have to apply in order to be registered. After the registration, they are subject to the prudential supervision by the competent authority and they can exercise the right of establishment or the freedom to provide service in a Member State other than their home Member State (*passporting right*).

Recital 48 explains the rationale: "*In view of the specific nature of the activity performed and the risks connected to the provision of account information services, it is appropriate to provide for a specific prudential regime for AISPs. AISPs should be allowed to provide services on a cross-border basis, benefiting from the "passporting" rules.*"

## Article Reference

### Article 35(1) and (2) - Access to Payment Systems-

1. "Member States shall ensure that the rules on access of authorised or registered payment service providers that are legal persons to payment systems are objective, non-discriminatory and proportionate and that they do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system.

Payment systems shall not impose on payment service providers, on payment service users or on other payment systems any of the following requirements:

(a) restrictive rule on effective participation in other payment systems;

*(b) rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants;*

*(c) restriction on the basis of institutional status.*

*2. Paragraph 1 shall not apply to:*

*(a) payment systems designated under Directive 98/26/EC;*

*(b) payment systems composed exclusively of payment service providers belonging to a group. For the purposes of point (a) of the first subparagraph, Member States shall ensure that where a participant in a designated system allows an authorised or registered payment service provider that is not a participant in the system to pass transfer orders through the system that participant shall, when requested, give the same opportunity in an objective, proportionate and non-discriminatory manner to other authorised or registered payment service providers in line with paragraph 1.*

*The participant shall provide the requesting payment service provider with full reasons for any rejection.*

## **Guidance and interpretation**

The criteria applicable to the direct or indirect access to payment systems (non-discriminatory and proportionate) allow payment systems owners to make informed decisions about access of direct and indirect participants provided that access criteria are compliant with Article 35 of PSD2. Payment systems designated under the Settlement Finality Directive (Directive 98/26/EC) continue to be exempted from the requirements of Article 35 (1). One major change brought about by PSD2 compared to PSD1 is that the exemption for three-party card schemes from the access requirements has been removed – meaning that PSPs may have access to such three party card schemes (e.g. to acquire transactions under that three-party card scheme).

## **Article Reference**

### **Article 36 – Access to accounts maintained with a credit institution-**

*“Member States shall ensure that payment institutions have access to credit institutions’ payment accounts services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive as to allow payment institutions to provide payment services in an unhindered and efficient manner.*

*The credit institution shall provide the competent authority with duly motivated reasons for any rejection.”*

## Guidance and interpretation

Recital 39 gives additional context, explaining that PSPs engaging in one or more of the services covered by PSD2 “should always hold payment accounts used exclusively for payment transactions”. Thus, Member States “should ensure that access to such accounts be provided in a manner that is not discriminatory and that is proportionate to the legitimate aim it intends to serve. While access can be basic, it should always be sufficiently extensive for the payment institution to be able to provide its services in an unobstructed and efficient way”.

PSPs must base their decisions about opening payment accounts for payment institutions, on an objective, non-discriminatory and proportionate assessment taking into account other legal and regulatory obligations and apply due diligence. In other words, a credit institution has the right to reject account applications of payment institutions on, for example, evidence of anti-money laundering concerns. However, credit institutions that decline a payment institution with access to a payment account will have to explain the rejection to the competent authority.

Furthermore, access that is “sufficiently extensive as to allow payment institutions to provide payment services” does not include any improper use of accounts held by payment institutions with the credit institutions, whose main purpose remains to allow payment institutions to clear and settle payments. For this reason, such accounts should never be referenced in the payment instruction as if they were accounts directly held by a payee or payer.



## V. INFORMATION AND CONDITIONS

Generally speaking, information requirements are not greatly changed compared to PSD1. However, it must be noted that the impact of concomitant EU legislation on transparency requirements (namely stemming from Directive 92/2014 and the ensuing Level 2 rules such as the EBA standardised Union level terms and definitions) will have to be duly considered when reviewing the current terms and conditions of framework contracts to ensure that the contractual content is aligned with the new provisions.

Coming back to PSD2, the introduction of PISPs has a number of consequences in Title III. The overall aim of the information requirement, as set out in recitals 54-56, are also largely unchanged, although information now needs not only to be necessary and sufficient but also, comprehensible (recital 54), while information needs to be presented in a standard format (previously referred to as “manner”, recital 56).

From the perspective of AS PSPs, the review of the information requirements should aim to make the payment service user (PSU) aware about the separate roles and services of the AS PSP as distinct from PISPs and AISPs.

It is nevertheless interesting to refer to recitals 63 and 64 as they seem to introduce new restrictions on the (changes to) terms and conditions of the framework contract. Recital 63 states that Member States should, in the interest of the consumer, “be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change”. Finally, recital 64 clarifies the fact that all PSPs listed in PSD2 are subject to Article 15 of the Payment Accounts Directive (2014/92/EU).

### Article 33(2): Account information service providers

*2. “The persons referred to in paragraph 1 of this Article shall be treated as payment institutions, save that Titles III and IV shall not apply to them, with the exception of Articles 41, 45 and 52 where applicable, and of Articles 67, 69 and 95 to 98.”*

### Guidance and interpretation

While PISPs will need to comply with the general requirements for PSPs offering payment initiation services, AISPs are generally “treated” as Payment Institutions as stated in Article 33 (2). AISPs have to provide service information and conditions to their clients and the applicable part of the framework contract if the service is provided on a permanent basis. Like any other PSPs, they also have to comply with security rules (strong customer authentication [SCA]) and secure communication standards as set by the EBA in the draft RTS to be developed in accordance with Article 98.

## Articles References

### Article 41: Burden of proof on information requirements

*Member States shall stipulate that the burden of proof lies with the payment service provider to prove that it has complied with the information requirements set out in this Title.*

#### Guidance and interpretation

Whilst Member States previously had the option to put the burden of proof regarding compliance with Title III on PSPs, this is now a requirement. According to article 33(2), this also applies to AISPs.

### Article 42: Derogation from information requirements for low-value payment instruments and electronic money

*In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time.*

#### Guidance and interpretation

Compared to PSD1, the thresholds - below which information requirements are lighter - remain unchanged.

## Article Reference

### Article 44(1): Prior general information

*Member States require that before the payment service user is bound by a single payment service contract or offer, the payment service provider makes available to the payment service user, in an easily accessible manner, the information and conditions specified in Article 45 with regard to its own services,...*

#### Guidance and interpretation

Article 44(1) has been amended to highlight that the PSP only needs to provide information and conditions pertaining to its own services. Hence, apart from providing general information about the fact that the PSD2 regulates two new types of payment services (PIS and AIS) as mentioned above, and sets out provisions regarding confirmation on availability of funds in connection with card-based payment instruments (see Article 65) AS PSPs do not need to describe the specific services that Third Party Providers (TPPs) might offer. The information now needs to be provided in an easily accessible manner.

## Article Reference

### Article 45: Information and condition

*Article 45(1): Member States shall ensure that the following information and conditions are provided or made available by the payment service provider to the payment service user:*

- (a) A specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly initiated or executed;*
- (b) The maximum execution time for the payment service to be provided*
- (c) all charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges*
- (d) Where applicable, the actual or reference exchange rate to be applied to the payment transaction.*

*Article 45(2): In addition, Member States shall ensure that PISPs, prior to initiation, provide the payer with,..., the name of the payment initiation service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch, ..., and any other contact details, including electronic mail address,...and the contact details of the competent authority.*

### Guidance and interpretation

Article 45 has been amended to take into account the introduction of PISPs into the scope of the Directive. Article 45 (1), point e) makes clear that a payment order can indeed be *initiated* or executed. Hence, the requirements in Article 45(1) also apply to PISPs. As per Article 44, information on charges and exchange rates refer to those that the PSP itself levies on the PSU. In line with Article 45 (1) (c), charges should be clearly stated, with a clear distinction and separation of the different amounts corresponding to each transaction or service which gives rise to the specific charges.

Article 45(2) specifies the additional information that PISPs must provide to the payer, including its name and contact details of the competent authority. Since PISPs will most likely have a framework contract with the payee but possibly a one-off or very ad hoc relationship with the payer, this is a key information requirement for PISPs.

AISPs are, according to article 33(2) also subject to this article. While the chapter covers single payment transactions, the logic must be that AISPs are subject to the information requirements regarding one-off interactions with PSUs. However, AISPs will most likely enter into a framework contract with the PSU.

As with PSD1, PSD2 (Article 45 (1c)) does not specify what is exactly meant with all charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges. The objective of this article is to allow PSUs to be offered a maximum level of transparency on the charges they will have to pay in line with Directive 2014/92/EU of 23<sup>rd</sup> July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

## Articles References

### Article 46: Information to the payer and payee after the initiation of a payment order

*“where a payment order is initiated through a payment initiation service provider, the payment initiation service provider shall.. immediately after initiation, provide or make available all of the following data to the payer and, where applicable, to the payee...”*

### Guidance and interpretation

PISPs need to make available to the payer and, when applicable, to the payee information beyond that is specified in Article 45, which includes confirmation of the initiation, a reference and the amount of the transaction and the amount and breakdown of any charges payable to the PISP.

A PISP can, on a PSU's behalf, instruct the AS PSP to send a payment from the PSU's account. The payment must be processed with the same service level as if the user had initiated the payment directly (Article 66, (4c)).

## Article Reference

### Article 47: Information for payer's account service payment service provider in the event of a payment initiation service

*Where a payment order is initiated through a payment initiation service provider, it shall make available to the payer's account servicing payment service provider the reference of the payment transaction.*

### Guidance and interpretation

The requirement to provide the reference of the payment transaction needs to be seen in the context of the wider communication between AS PSPs and PISPs (see article 66). We assume that the reference of the transaction, as mentioned in articles 46 and 47, is one and the same reference. It should nevertheless be noted that compliance with article 47 and similar articles will be required before the measures in Article 65, 66, 67 and 97 (which are governed by the RTS timeline) are applied.

## Article Reference

### Article 48: Information for the payer after receipt of the payment order

### Article 49: Information for the payee after execution

*Immediately after receipt of the payment order (48) and the execution of the payment transaction (49), the payer's (48) and payee's (49) payment service provider shall provide the following data with regard to its own services.*

## Guidance and interpretation

Both articles have been amended to clarify that each respective PSPs are obliged to provide information on its own services only.

## Article Reference

### Article 52 Information and conditions

*Par. (2)(b) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly **initiated or** executed*

*Par. (2)(c) the form of and procedure for giving consent **to initiate a payment order or** execute a payment transaction and withdrawal of such consent in accordance with Articles 64 and 80;*

*Par. (2)(g) **in the case of co-badged, card-based payment instruments, the payment service user's rights under Article 8 of Regulation (EU) 2015/751.***

*Par. (3)(a) All charges payable by the PSU to the **PSP including these connected to the manner in and frequency with which information under this Directive is provided or made available and**, where applicable, the breakdown of the amounts of such charges*

*Par. (4)(a) where applicable, the means of communication, including the technical requirements for the payment service user's equipment **and software**, agreed between the parties for the transmission of information or notifications under this Directive;*

*Par. (5)(b) **the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;***

*Par. (5)(e) how and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly **initiated or** executed payment transaction in accordance with Article 71 as well as the payment service provider's liability for unauthorised payment transactions in accordance with Article 73;*

*Par. (5)(f) the liability of the payment service provider for the **initiation or** execution of payment transactions in accordance with Article 89.*

## Guidance and interpretation

Compared to PSD1 the content of the framework contract as listed in article 52 has been both **modified** in order to align with the new initiation services (through which the order could be initiated) and **extended** with new provisions (see bold above).

The PSP will have to check the current terms and conditions of their framework contracts to ensure that the contractual content is aligned with the new provisions.

AISPs are, according to article 33 (2), also subject to this article. While AISPs do not initiate or execute transactions (and hence are not covered by e.g. 52(2) (d) and 52 (2)(e)), AISPs will most likely enter into a framework contract with the PSU and should provide the relevant information to the PSU, including name and contacts details, relevant competent authority, a description of the relevant service, relevant charges, conditions for changing or terminating the framework contract, security measures and communication channels etc.

Article 52 introduces a number of obligations to provide information, which PSPs need to incorporate into the framework contract:

- o 52(2)(g): In case of co-badged card-based payment instruments, the payment service user's right under article 8 of the Interchange Fees Regulation.
- o 52(3)(a): An additional requirement to include information on charges related to "the manner in and frequency with which information under this Directive is provided or made available". It is unclear how this relates to the obligation on PSPs under article 40(2) and (3) to "not charge the PSU for providing information".
- o 52(5b): A requirement has been added that the framework contract should provide for information on the secure procedure (to prevent phishing/ social engineering, for example) for notification of the customer by the PSP in case of suspected or actual fraud or security threats. As a result, the AS PSPs will need to update all framework contracts to add this new procedure.

## Article Reference

### Article 54: Changes in conditions of the framework contract

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

## Guidance and interpretation

The principle is that the PSU is deemed to have accepted changes unless he notifies the PSP that he does not before the date of their entry into force is retained, provided that the changes are related to areas specified in the framework contract as per article 52(6)(a). However, the PSU now has the right to terminate the contract free of charge and effect at any time until the date when the changes would have applied. Hence, the PSU is given the right to decide when to terminate the contract (before the changes take effect).

## Article Reference

### Article 55: Termination

*Termination of the framework contract shall be free of charge for the payment service user except where the contract has been in force for less than 6 months. Charges, if any, for termination of the framework contract shall be appropriate and in line with costs.*

## Guidance and interpretation

The rules on the termination of the framework contract are largely unchanged. However, the period after which termination of the framework contract is free of charge has been reduced from 12 to 6 months.

## Article Reference

### Article 57: Information for the payer on individual payment transactions

*2. "A framework contract shall **include a condition** that the **payer may** require the information referred to in paragraph 1 to be provided or made available periodically, at least once a month, free of charge and in an agreed manner which allows the payer to store and reproduce information unchanged."*

In both article 57 (3) and 58 (3) the Member State options have been amended in a way that Member States may require the PSPs of the payer and payee to provide information on another durable medium (instead of only on paper) at least once a month and free of charge.

## Guidance and interpretation

While the content of the information to be provided after the receipt of the order is unchanged, there is a new mandatory provision to be inserted in the framework contract. This provision allows the user (when he/she plays the payer's role) to opt for a monthly report of the payment transactions or, alternatively, to have information on individual transactions under article 57(1).

## Article Reference

### Article 59: Currency and currency conversion

*59(2): Where a currency conversion service is offered prior to the initiation of the payment transaction and where that currency conversion service is offered at an ATM, at the point of sale by the payee, the party offering the currency conversion service to the payer shall disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction.*



## Guidance and interpretation

This article includes an additional reference to currency conversion offered at an ATM as well as to payment transactions through a payee or at the point of sale. This means that the party offering the currency conversion service on an ATM to the payer shall disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction. The same should apply to currency conversion at the Point of Sale.

## Article Reference

### Article 60 (2) and (3): Information on additional charges or reductions

*Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction.*

*Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof prior to the initiation of the payment transaction.*

## Guidance and interpretation

The PSD1 reference to a third party has been changed to “another party involved in the payment transaction”, presumably to allow for the fact that a payment initiation service provider may be involved in the transaction.

Article 60(3) contains a new provision that the payer only has to pay the charges levied by the payee or a PSP or another party involved in a transaction if their full amount was made known prior to the initiation of the payment transaction. As such charges are often calculated as a percentage of the payment amount, this provision should also be considered fulfilled if the prior information refers to such percentages rather than to the absolute amount.

## Article Reference

### Article 61: Scope

Art. 61 is not significantly changed from PSD1 beyond updating the cross-references to the relevant articles and related legislation. Thus PSUs and PSPs can agree that articles 62(1), 64(3), 72, 74, 76, 77, 80 and 89 “shall not apply in whole or in part” and “may also agree on a time period different from that laid down in Article 71” but solely when the PSU is not a consumer.



## Article Reference

### Article 62(2), (3) and (4) – charges applicable -

2. *"Member States shall require that for payment transactions provided within the Union, where both the payer's and the payee's payment service providers are, or the sole payment service provider in the payment transaction is, located therein, the payee pays the charges levied by his payment service provider, and the payer pays the charges levied by his payment service provider."*

3. *The payment service provider shall not prevent the payee from requesting from the payer a charge, offering him a reduction or otherwise steering him towards the use of a given payment instrument. Any charges applied shall not exceed the direct costs borne by the payee for the use of the specific payment instrument.*

4. *In any case, Member States shall ensure that the payee shall not request charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751 and for those payment services to which Regulation (EU) No 260/2012 applies."*

## Guidance and interpretation

Article 62(2) now applies to **all** intra-EEA transactions in **all** currencies, whether or not there is a currency conversion. This is a change compared to PSD1, reflecting the extension of scope under PSD2 (see Article 2 (3)). Under PSD1, the PSP was obliged to apply the sharing of charges principle to intra-EEA payments in EEA currencies only *"where a payment transaction does not involve any currency conversion"*.

According to Article 2(4), this article does however not apply to one-leg transactions, irrespective of the currency: SHA, OUR and BEN options can be used.

In practice, for intra-EEA payment transactions in Euro and non-Euro Member State currencies, the charge code 'SHA' is applied, in combination with the full amount principle under Article 81. However, for intra-EEA payment transactions in non-EEA currencies with SHA option, the full amount principle of Article 81 does not apply and in practice indeed cannot be guaranteed, because intermediary institutions (some of which are necessarily located outside the EEA) may deduct charges from the amount transferred.

Article 62(3) should be read as an exception to Article 62(2) as, in case of surcharge, the payer pays the charges levied by the payee (e.g. the merchant) for accepting a given payment method. Payees are therefore allowed to apply surcharges or offer discounts or otherwise steer use of a given payment instrument, except for those capped under the Interchange Fees Regulation (as per Article 62(4)) but these charges cannot exceed the direct costs borne by the payee for the use of the specific payment instrument.

Surcharging is also forbidden for the payee in case of payment services to which the SEPA Regulation (Regulation (EU) No 260/2012 applies), as, for example, SEPA Direct Debit.

## VI. CONSENT

### Article Reference

#### Article 64 (3) – Consent and withdrawal of consent -

3. *"Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Article 80. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised".*

### Guidance and interpretation

There is a risk that in case a payment is initiated by a PISP, the AS PSP may be unaware that the PSU has withdrawn his or her consent to initiate a payment or a series of payment transactions, because PSD2 does not specifically require PSUs to communicate their consent in relation to payment initiation services also to the AS PSP.

In that particular case, it would be advisable to add a specific provision in the contract between an AS PSP and his PSU stating that the latter must inform his AS PSP that he or she has withdrawn his or her consent in relation to PISPs or a card-based payment instrument issuer (in the context of Article 65) in a form to be agreed between them. It is indeed essential to make the PSU aware of the risk of further data sharing in case his AS PSP is not informed of the withdrawal of his consent. **This will be clarified by the forthcoming EBA RTS.**

### Article Reference

#### Article 78(2) – Receipt of payment orders

2. *"If the payment service user initiating a payment order and the payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has put funds at the payment service provider's disposal, the time of receipt for the purposes of Article 83 is deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day."*

#### Article 80 (2) (4) – Irrevocability of a payment order

2. *"Where the payment transaction is initiated by a payment initiation service provider or by or through the payee, the payer shall not revoke the payment order after giving consent to the payment initiation service provider to initiate the payment transaction or after giving consent to execute the payment transaction to the payee."*

4. *"In the case referred to in Article 78(2) the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day."*

## Guidance and interpretation

In general the principles governing irrevocability have not changed from PSD to PSD2. However, the introduction of PIS has some consequences in this respect. In an online/e-commerce context the payment order initiated through a PISP requires execution from ASPSP. That explains why the order is not revocable under article 80(2).

Since PISPs are PSPs, article 78(2) on receipt on an agreed (future) day or on the following business day, and article 80(4) on the PSU's right to revoke at latest "by the end of the business day preceding the agreed day", also apply to PISPs unless they do not offer future transaction dates.

## VII. SERVICES OFFERED BY CARD BASED PAYMENT INSTRUMENTS ISSUERS

### Article Reference

#### Article 65 (1) – Confirmation on the availability of funds

*1. “Member States shall ensure that an account servicing payment service provider shall, upon the request of a payment service provider issuing card-based payment instruments, immediately confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, provided that all of the following conditions are met:*

- (a) the payment account of the payer is accessible online at the time of the request;*
- (b) the payer has given explicit consent to the account servicing payment service provider to respond to requests from a specific payment service provider to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer’s payment account;*
- (c) the consent referred to in point (b) has been given before the first request for confirmation is made.”*

### Guidance and interpretation

PSD2 refers to PSPs issuing card-based payment instruments but does not separately define these Card-Based Payment Instrument Issuers (CISPs). Recital 67 provides some context: *“The issuing of a card-based payment instrument by a payment service provider whether a credit institution or a payment institution, other than the servicing the account of the customer, would provide increased competition in the market and thus more choice and a better offer for consumers”*.

Consequently, we understand the term Card Based Payment Instrument Issuer therefore to mean *PSPs licensed either as credit institutions or as payment institutions offering services under Annex 1 for the execution of payment transactions, including transfers of funds on a payment account with the user’s PSP or with another PSP (point 3), the execution of payment transactions where the funds are covered by a credit line...(point 4) or the issuing of payment instruments and/or acquiring of payment transactions (point 5)*.

There should be a clear distinction between the provisions related to PISPs and AISPs and Card-Based Payment Instrument Issuers as there are different communication and process requirements.

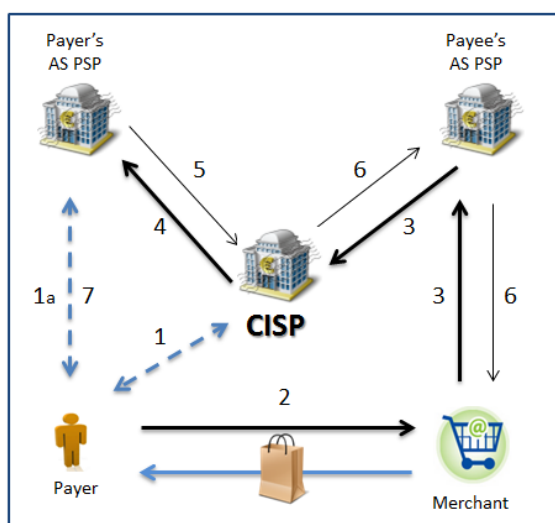
Recitals 67 and 68 describe the use of a card or card-based payment instrument issued by a credit institution or payment institution other than the customer’s Account Servicing Payment

Service Provider which allows the card-based payment instrument issuer to seek confirmation from the Account Servicing Payment Service Provider (AS PSP) as to whether sufficient funds are on the account in the form of a simple “yes” or “no” answer at the time of the request. This information is subject to the PSU’s consent. PSPs issuing such card-based payment instruments must ensure that the PSUs has been duly informed their AS PSP before the initial payment transaction. PSUs must inform their AS PSPs accordingly when consent has been given, and ideally amended or withdrawn. The AS PSP will also need to ensure it has processes in place to track when a PSU has given its consent, which appropriately authorised PSP (card-based payment instrument issuer) is involved and whether consent has subsequently been withdrawn.

As stated in Article 65 (6), “*This Article does not apply to payment transactions initiated through card-based instruments on which electronic money as defined by Directive 2009/110/EC is stored*”. This is also reflected in Recital 68, which argues that “*Given the specific nature of electronic money, it should not be possible to apply that mechanism to payment transactions initiation through card-based payment instruments on which electronic money is stored*”.

## Card-Based Payment Instrument Issuer (CISP)

*Payment transactions through a card-based payment instrument issuer  
Operating model and principal features*



1. **The payer signs an agreement with another PSP/CISP** that offers the alternative payment card and issues the new card with specific credentials (PIN code = strong authentication). The Payer gives consent to his AS PSP, identifying the PSP/CISP to whom, if addressed, the AS PSP should give the answer on the availability of funds;
2. At POS, the payer initiates the card payment transaction by entering his PIN code (SCA);
3. The merchant's PSP requests the confirmation on the availability of funds to the PSP/CISP who issued the payment card;
4. The PSP/CISP requests the confirmation on availability of funds to the payer's AS PSP where the payer's account is;
5. The Payer's AS PSP gives a simple Yes/No answer on the availability of funds;
6. The PSP/CISP sends the answer to the Merchant via the merchant's PSP and the card transaction at the POS can be concluded or denied in case of insufficient funds;
7. Meanwhile, if requested by the payer, his AS PSP sends him information that there has been a request for confirmation on the availability of funds from a specific PSP/CISP and the answer that was given.

Recital 67 and 68 plus article 65 of the PSD2 refer to the CISP operating features as described in the figure and summarized as follows:

- The payment account of the payer is accessible online at the time of the request;
- Before the first confirmation is made, the payer gives explicit consent to the ASPSP to respond to confirmation requests from the CISP;
- The confirmation shall not allow the ASPSP to block the funds on the payer's payment account
- The funds are settled for example through a direct debit transaction between the payer's ASPSP and the issuer (article 68)
- Payment transactions initiated through card-based payment instruments on which electronic money is stored are excluded.

*Figure 6 – PSD2 description of CISP*

It should be noted that it is only steps 1, 1a, 4, 5 and 7, that are prescribed by article 65 PSD2 in the above figure. The payment in itself is not covered by the article. Steps 2, 3 and 6 are just included to illustrate how the availability of funds question prescribed in Article 65 could be utilised by a third-party card-based payment instrument issuer. In this example it is assumed that the card issuer would be issuing cards under a general purpose four party scheme.

Article 65 could be utilised by issuers with different business models and product setups:

- Issuers of general purpose cards in four party schemes, such as Visa, MasterCard.
- Three-party schemes issuing and acquiring cards, such as American Express
- Issuers of store cards, chain cards and other limited networks.

It should be noted that the operations of customer authentication, authorisations, clearing and settlement of the card transaction, as well as the liabilities between the third-party card-based payment instrument issuer and the acquirer, are governed entirely by the rules of a scheme. In the last two bullets above, the scheme is the issuer. None of this is governed by Article 65.

Afterwards, to settle the transaction the PSP pays the amount to the merchant's bank upon request (payment card scheme usually debits the card issuer's account). This part is directed by the card scheme rules, and is also not governed either by Article 65.

Therefore a clear distinction needs to be made between the confirmation process and the handling of any subsequent settlement transaction. Our current understanding is that settlement i.e. the debiting of the PSU's account with its AS PSP may involve either a credit transfer (initiated by the PSU) or a direct debit (originated by the card-based payment instrument issuer). This part of the process will be subject to the normal PSD2 provisions governing payment transactions between PSPs, including authorisation, authentication and liability.

The PSD2 provisions – see article 66(5) and Article 67(4) - relating to PIS and AIS explicitly state that such services shall not be "*dependent on the existence of a contractual relationship*". There is no equivalent wording used in article 65. We take this as an acknowledgement that a contract could be negotiated between a Card-based Payment Instrument Issuer (the PSP) and the AS PSP. A form of agreement between Card-based Payment Instrument Issuer and AS PSP may be an option, the card-based payment instrument issuer will have to receive the amount, which it has paid in advance to the merchant, by e.g. using a direct debit (to transfer the amount from the PSUs bank account held at the AS PSP to the account of the Card Based Payment Instrument Issuer), as mentioned in recital 68. It is less clear whether also the other aspects of the relationship between the card-based payment instrument issuer and the ASPSP could also be governed by a contract (e.g. regulating the response to confirmation requests).

## VIII. ACCESS TO PAYMENT ACCOUNTS AND USE OF CREDENTIALS

### Articles References

#### Article 66 (3b) - Rules on access to payment account in the case of payment initiation services

3. *"The payment initiation service provider shall:*

*b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels".*

#### Article 67(2b) - Rules on access to and use of payment account information in the case of account information service

2. *"The account information service provider shall:*

*b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels."*

#### Article 69 (1a) and (2) - Obligations of the payment service user in relation to payment instruments and personalised security credentials

1. *"The payment service user entitled to use a payment instrument shall:*

*(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate"*

2. *For the purposes of point (a) of paragraph 1, the payment service user shall, in particular, as soon as in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe".*

#### Article 70(1) (a) – Obligations of the payment service provider in relation to payment instruments

1. *"The payment service provider issuing a payment instrument shall:*

*a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligation on the payment service user set out in Article 69".*

#### Article 97 (3) – Authentication

3. *"With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service user's personalised security credentials".*



## Article 98 (1d) - Regulatory technical standards on authentication and communication

1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:

d) “the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.”

### Guidance and interpretation

Articles 66 and 67 require AS PSPs to provide facilities to communicate securely with authorised and registered Payment Initiation Service Providers (PISPs) and Account Servicing Payment Service Provider (AISPs) and allow them to provide services to all payment accounts that are accessible online. We note that these provisions are not specifically limited to consumers (for example, they also apply to online corporate accounts) as detailed under articles 65, 66 and 67. See the definitions of “payer” (article. 4 (8)) and Payment Service User “PSU” (article 4 (10)), which can be a natural or legal person, in combination with the scope of title III (article 38) and title IV (article 61).

The use of personalised security credentials needs to be considered in conjunction with the subjects of consent, security, confidentiality/data protection, bank secrecy and fraud prevention. The AS PSP has the responsibility to protect its customers’ account information and funds. The provisions of Article 66 (3)(b) and 67 (2)(b) have to read in connection with both Articles 69, 70 and 97.

There are currently various business models and practices in the TPP space, some relying on the re-use of PSU’s personalised security credentials and others not requiring the access to these credentials, but rather operating based on information flows between AS PSPs and the TPP. There are various degrees of security risk and complexity associated with these different operating models. It is expected that the EBA’s regulatory technical standards (as referred to in Article 98) which will specify the requirements for “common and secure open standards of communication” will provide i) the parameters within which PISP and AISP-related models will be expected to operate in the future and ii) the level of standardisation required in the PSP implementation to allow any EEA AS PSP to exchange information with any EEA PISP/AISP for the services provided.

Article 69 (2) states, just as in PSD1, that the PSU shall take all reasonable steps to keep its personal security credentials safe. Whilst this provision remains in PSD2, the text does not prohibit the re-use of the PSU’s personalised security credentials by PISPs and AISPs. Recital 69 provides context: “The obligation to keep personalised credentials safe is of the utmost importance to protect the funds of the PSU and to limit the risks relating to fraud and unauthorised access to the payment account. However, terms and conditions or other obligations imposed by PSPs on the PSUs in relation to keeping personalised security credentials safe should not be drafted in a way that prevents PSUs from taking advantage of services offered by other PSPs, including PIS and AIS. Furthermore, such terms and conditions should not contain any



*provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to this Directive".*

## Articles References

### **Article 68 (5) and (6) - Limits of the use of the payment instrument and of the access to payment accounts by payment service providers**

*5. An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction. In such cases the account servicing payment service provider shall inform the payer that access to the payment account is denied and the reasons therefore in the form agreed. That information shall, where possible, be given to the payer before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law. The account servicing payment service provider shall allow access to the payment account once the reasons for denying access no longer exist.*

*6. In the cases referred to in paragraph 5, the account servicing payment service provider shall immediately report the incident relating to the account information service provider or the payment initiation service provider to the competent authority. The information shall include the relevant details of the case and the reasons for taking action. The competent authority shall assess the case and shall, if necessary, take appropriate measures.*

## Guidance and interpretation

Article 68 makes it clear that AS PSPs can block a transaction in line with Article 68(5). In addition, the AS PSP may deny an AISP or PISP access to a payment account "for objectively justified and duly evidenced reasons". For example, if the PISP has not correctly authenticated itself to the AS PSP, the latter can refuse to initiate the payment order and can contact the PSU to confirm the payment order. In the event that the AS PSP denies a PISP or AISP access, the AS PSP, in accordance with article 68(6), has to inform the competent authority about the incident.

## IX. AS PSP LIABILITY

### Articles References

#### **Article 71 - Notification and rectification of unauthorised or incorrectly executed payment transactions.**

*1. "The payment service user shall obtain rectification of an unauthorised or incorrectly executed payment transaction from the payment service provider only if the payment service user notifies the payment service provider without undue delay on becoming aware of any such transaction giving rise to a claim, including that under Article 89, and no later than 13 months after the debit date.*

*The time limits for notification laid down in the first subparagraph do not apply where the payment service provider has failed to provide or make available the information on the payment transaction in accordance with Title III.*

*2. Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to paragraph 1 of this Article, without prejudice to Article 73(2) and Article 89(1)."*

#### **Article 72 – Evidence on authentication and execution of payment transactions**

*1. "Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.*

*If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge".*

*2." Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user."*

## Article 73 (1) and (2) – Payment service provider’s liability for unauthorised payment transactions

1. *“Member States shall ensure that, without prejudice to Article 71, in the case of an unauthorised payment transaction, the payer’s payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer’s payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer’s payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer’s payment account shall be no later than the date the amount had been debited.*

2. *Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.”*

### Guidance and interpretation

The liability of AS PSPs has been altered due to the intermediation of PISPs. PSD2 makes it clear that the PSU can obtain rectification from the AS PSP in the event of an unauthorised or incorrectly executed payment. Thus, an AS PSP will be obliged to reimburse the PSU even if the transaction has been initiated by a PISP. It will then be up to the PISP to prove, within its sphere of competence, that the transaction was authenticated, accurately recorded, and not affected by a technical breakdown. The PSD2 does not specify to whom the PISP will have to hand-over this proof. We assume this is to the AS PSP. However, in the absence of a contract between a PISP and an AS PSP, and in light of the fact that in the interest of consumer protection, a PSU is entitled to claim a refund from the AS PSP, it remains to be seen how the allocation of liability provisions will operate in practice. For this reason it is desirable that Member States transpositions provide that the AS PSP – which has already refunded the PSU –whenever the liable PISP or AISP does not comply with its obligation to immediately compensate the AS PSP when the PISP or AISP was at fault. In this case, AS PSPs should immediately refer the case to their supervisory authorities or Courts. There is currently some uncertainty as to what insurance will be available to the TPPs to enable them to comply with this requirement. What appears to be clear is that TPPs will not receive authorisation to operate in the market without having the professional indemnity insurance or comparable guarantee.

No clarification is offered by the PSD2 on the recourse available to the AS PSP in cases where the PISP (or AISP) denies any wrong doing. It is therefore assumed that AS PSPs will have to refer the case(s) to their supervisory authorities.

## Article 74(1) and (2) - Payer's liability for unauthorised payment transactions

*1. "By way of derogation from Article 73, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.*

*The first subparagraph shall not apply if:*

*(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or*

*(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.*

*The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence.*

*In such cases, the maximum amount referred to in the first subparagraph shall not apply.*

*Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 69, Member States may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.*

*2. Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.".... "Member States may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated".*

## Guidance and interpretation

Paragraph 1 states that, except in cases of fraud or gross negligence by the payer, for any unauthorised payment transactions, a payer could pay up to EUR 50. This maximum amount has been decreased from the previous EUR 150 PSD1 threshold.

Paragraph 2 introduces the liability shift principle in the context of the application of strong customer authentication. Except in the case of the payer's fraud, the party in the payment chain, which does not support strong customer authentication, bears the financial loss. Member States have the option to further reduce this liability depending on the circumstances listed under Article 74.2 last sub paragraph.

## Article reference

### **Article 75: Payment transactions where the transaction amount is not known in advance**

This new article (supported by Recital 75) has been introduced to address 'card pre-authorisations' in response to issues identified in some Member States where it can take up to several weeks for pre-authorisations to be cancelled or balances to be released.

When a purchase is made, a customer's card details are checked and the purchase transaction is authorised as normal, but the transaction is set to a 'pre-authorised' status. Funds are placed on hold, and the money is not debited to the card holder's account at this point, but held until final payment is processed. This is, for example, the case when filling up with petrol at an unmanned gas station, in car rental contracts or hotel reservations. Article 75 states that the payee will only be allowed to block funds on the account of the payer if the payer has approved the exact amount that can be blocked. The payer's bank must release the blocked amount without undue delay after receipt of the exact amount and immediately after receipt of the order.

## **X. VALUE DATE AND AVAILABILITY OF FUNDS**

### **Article reference**

#### **Section 2 EXECUTION TIME AND VALUE DATE**

##### **Articles 82 to 87**

The issue is the extent to which PSD2 regulates the time taken to conduct a currency exchange which takes place at one or both ends of a payment transaction – such as where a payment service user wishes to make a payment in a currency which is different from the currency of the account which he wishes to have debited, or to have a payment arriving in one currency credited to an account in another currency.

Article 82 defines the scope of application of the execution time and value dating articles (Articles 83 - 87). Throughout Article 82, reference is made to the types of 'payment transactions' to which Articles 83 to 87 apply.

At the time PSD1 was being implemented, the EU Commission indicated that payments involving a currency conversion between two EEA currencies are regarded as 'other' transactions and hence governed by Article 82(2), except in the specific case foreseen in Article 82(1)(c). Hence an execution time period longer than that set out in Article 83 may be agreed between the PSU and his PSP, so long as this is no longer than D+4. Non-EEA currencies would be deemed to fall under the category of 'other' payments, which would also fall into the scope of Article 82(2) where this applies.

Where funds arrive with a payee's PSP in a currency different to that of the payee's account, the payee's PSP may sometimes need to seek explicit instructions from the payee, which could take time, or may simply not be able to perform the specific currency conversion requested on a same day basis due to the conventions of the foreign exchange markets.

Articles 82 to 87 need to be read in conjunction with Article 2. Thus, according to:

- Article 2(2) – Articles 82 to 87 apply to intra-EEA payments in EEA currencies
- Article 2(3) – Articles 82 to 86 do not apply to intra-EEA payments in non-EEA currencies, however, Article 87 applies.
- Article 2(4) – Articles 82 to 87, except for 83(1) concerning the D+1 execution time rule, do apply to one-leg payments in any currency. However, from the perspective of the PSP in the EEA while provisions relating to making incoming funds available and value dating do apply without exception, Article 82(2) allows for specific agreements with PSUs beyond the scope of Article 82 (1) for the purpose of articles 84 and 85

## Article 87 – Value date and availability of funds

1. *“Member States shall ensure that the credit value date for the payee’s payment account is no later than the business day on which the amount of the payment transaction is credited to the payee’s payment service provider’s account.*

2. *The payment service provider of the payee shall ensure that the amount of the payment transaction is at the payee’s disposal immediately after that amount is credited to the payee’s payment service provider’s account where, on the part of the payee’s payment service provider, there is:*

*(a) no currency conversion or*

*(b) a currency conversion between the euro and a Member State currency or between two Member State currencies.*

*The obligation laid down in this paragraph shall also apply to payments within one payment service provider.*

3. *Member States shall ensure that the debit value date for the payer’s payment account is no earlier than the time at which the amount of the payment transaction is debited to that payment account.*

## Guidance and interpretation

Article 87 applies to all payment transactions (i.e. intra-EEA payments in both EEA and non-EEA currencies and to one-leg transactions in any currency).

For the purposes of credit and debit value dating, articles 87(1) and (3) already applied under PSD1 to one leg transactions in EEA currencies. The application of the debit/credit value dating rule has now been extended also to transactions in non EEA currencies but only in the absence of currency conversion and to intra-EEA transactions in non-EEA currencies, but only in the absence of currency conversions and to one-leg transactions in non EEA currencies.

Credit value date: The credit value date should not be later than the business day on which the amount is credited to the payee’s PSP’s account. If the credit to the payee’s PSP’s account was on a non-business day, the funds should be credited and made available to the payee no later than the following business day. Once the payee’s PSP’s account has been credited and the PSP has all the information necessary to credit the amount on the payee’s account, the payee’s PSP should make funds immediately available to the payee – including payments within the same PSP – where there is no currency conversion or where there is a currency conversion between the euro and a Member State currency or between two Member State currencies. For any currency conversion that has to take place on the beneficiary PSP side, it should be noted however that currency exchange transactions are subject to international standards, which execute over a T+2 horizon. Nevertheless, the PSD2 requires that any currency conversion between the euro and a Member State currency or between two Member State currencies applied on the side of the beneficiary PSP have to be immediate. Therefore the beneficiary PSP will have to ensure that the amount of the payment transaction is at the payee’s disposal without delay.



Given that this article also applies to non-EEA currency payments made between or to EEA PSPs, where there is no currency conversion the following has to be considered: For these types of foreign currency payments there may be time zone restrictions, which may not allow for an immediate availability of funds on the PSUs account following fund receipt by the beneficiary PSP (e.g. credit of US dollar to beneficiary PSP before bank systems open) as it closely depends on the PSP business day in which it is operational.

Debit value date: The debit value date should in all cases be not earlier than the time the payment transaction is debited to the payer's payment account. In case a currency conversion has to be applied on the sending side – because the currency of the payment account is different from the currency of the payment transaction - the payment transaction process only begins once the required currency has been obtained (e.g. a SEPA payment from a UK sterling account will only be initiated once the required Euro amount is available).

## Article reference

### **Article 89: Payment service providers' liability for non-execution, defective or late execution of payment transactions**

This article now also includes PSP's liability in case of 'late execution' of payment transactions, as compared to PSD1 which only dealt with 'non-execution' or 'defective execution' of payment transactions.

## Article reference

### **Article 90: Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions**

*"1. Where a payment order is initiated by the payer through a payment initiation service provider, the account servicing payment service provider shall, without prejudice to Article 71 and Article 88(2) and (3), refund to the payer the amount of the non- executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.*

*The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 78 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.*

*2. If the payment initiation service provider is liable for the non-execution, defective or late execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer".*

This new article is included to describe the liability of PISPs in case of non-execution, defective or late execution of payment transactions. The AS PSP must refund the payer with the amount of the unauthorised payment transaction. The PISP is obliged to compensate the AS PSP for the cost incurred in connection with the reimbursement of the payer, as well as the amount of the unauthorised payment transaction, immediately at the request of the AS PSP, unless the PISP is able to prove that it was not responsible for the unauthorised payment transaction. The burden of proof thus lies with the PISP.

## XI. OPERATIONAL AND SECURITY RISKS

### Article reference

#### Article 95 – Management of operational and security risks

1. *“Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.*

2. *Member States shall ensure that payment service providers provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.*

3. *By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.*

*EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years.*

4. *Taking into account experience acquired in the application of the guidelines referred to in paragraph 3, EBA shall, where requested to do so by the Commission as appropriate, develop draft regulatory technical standards on the criteria and on the conditions for establishment, and monitoring, of security measures.*

*Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.*

5. *EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security.”*

#### Article 96 – Incident reporting

1. *“In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment*

*service provider. Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident."*

*2. Upon receipt of the notification referred to in paragraph 1, the competent authority of the home Member State shall, without undue delay, provide the relevant details of the incident to EBA and to the ECB. That competent authority shall, after assessing the relevance of the incident to relevant authorities of that Member State, notify them accordingly. EBA and the ECB shall, in cooperation with the competent authority of the home Member State, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system.*

*On the basis of that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.*

*3. By 13 January 2018, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 addressed to each of the following:*

*(a) payment service providers, on the classification of major incidents referred to in paragraph 1, and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;*

*(b) competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities*

*4. EBA shall, in close cooperation with the ECB, review the guidelines referred to in paragraph 3 on a regular basis and in any event at least every 2 years.*

*5. While issuing and reviewing the guidelines referred to in paragraph 3, EBA shall take into account standards and/or specifications developed and published by the European Union Agency for Network and Information Security for sectors pursuing activities other than payment service provision.*

*6. Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form."*

## **Guidance and interpretation**

The EBA will draft guidelines, where ideally any redundancy with other incident notification requirements (i.e. the NIS Directive and possibly any local regulation) should be avoided. The impact for the AS PSP could be a multitude of notifications related to the same incident, to be sent without undue delay to different authorities at both national and European levels, probably

using different formats based on different criteria. It is therefore considered necessary that in its guidelines, EBA sets common, clear and homogeneous criteria to understand the level of significance and severity of a security incident, and harmonise the different formats and procedures for incident notification. More specifically, the definition of common processes and templates for security incident notification that could be used to comply with different Directives (NIS and PSD2 for example) could reduce the PSP's efforts and costs in relation to the notification obligations.

Moreover, it would be valuable to develop proper mechanisms able to extract and distribute to PSPs lessons learned deriving from incident reporting, in order to support incident and fraud prevention and early warning.

Article 95 addresses security risks and aspects of authentication in line with the Directive on Network and Information Security (NIS Directive). All PSPs will need to prove that they have certain security measures in place ensuring safe and secure payments. The PSP will have to carry out an assessment of the operational and security risks at stake and the measures taken on a yearly basis. The content of this article overlaps with the EBA Guidelines on the security of internet payments.

## Article reference

### Article 101 – Dispute resolution

*"1. Member States shall ensure that payment service providers put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints of payment service users concerning the rights and obligations arising under Titles III and IV of this Directive and shall monitor their performance in that regard.*

*Those procedures shall be applied in every Member State where the payment service provider offers the payment services and shall be available in an official language of the relevant Member State or in another language if agreed between the payment service provider and the payment service user.*

*2. Member States shall require that payment service providers make every possible effort to reply, on paper or, if agreed between payment service provider and payment service user, on another durable medium, to the payment service users' complaints. Such a reply shall address all points raised, within an adequate timeframe and at the latest within 15 business days of receipt of the complaint. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond the control of the payment service provider, it shall be required to send a holding reply, clearly indicating the reasons for a delay in answering to the complaint and specifying the deadline by which the payment service user will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.*

*Member States may introduce or maintain rules on dispute resolution procedures that are more advantageous to the payment service user than that referred to in the first subparagraph. Where they do so, those rules shall apply.*

*3. The payment service provider shall inform the payment service user about at least one ADR entity which is competent to deal with disputes concerning the rights and obligations arising under Titles III and IV.*

*4. The information referred to in paragraph 3 shall be mentioned in a clear, comprehensive and easily accessible way on the website of the payment service provider, where one exists, at the branch, and in the general terms and conditions of the contract between the payment service provider and the payment service user. It shall specify how further information on the ADR entity concerned and on the conditions for using it can be accessed.*

## **Guidance and interpretation**

This new article explains that PSPs must have complaints' resolution procedures in place, that apply in every Member State where the PSP offers payment services, in the official language of the relevant Member State (or any one official language where there are several) or in another language if agreed between PSP and PSU.

The overall deadline for a PSP to resolve a complaint is 15 business days (or, up to a total of 35 business days if there is a delay for reasons beyond the control of the PSP, and the PSP indicates the reasons for delay and the date for a final reply). Member States can provide for faster redress (Member State option).

The PSP shall inform the PSU about at least one out-of-court redress entity which is competent to deal with disputes concerning the rights and obligations arising under Titles III and IV. PSPs will have to make this information available in an easily accessible manner on their websites and on paper at their branches (if present), and in the general terms and conditions of the contract between PSP and PSU.

## **Article reference**

### **Article 109 – Transitional provision**

Companies operating under a waiver (under article 32) would have an extra 12 months (13 January 2019) to either become authorised or obtain a fresh waiver, unless the regulator has enough evidence to grant the waiver automatically where that power is given to them. Failure to satisfy the regulator of the conditions for authorisation or a waiver would mean the firm is no longer authorised, or the waiver is lost, as the case may be.

PSD2 foresees transitional provisions for PIs that are already authorised to provide services under PSD1. These PIs are allowed to continue providing payment services for 30 months - 13 July 2018 - (authorised institutions) or 36 months - 13 Jan. 2019- ("small" institutions that benefited from the waiver under art. 26 of PSD1) after the entry into force of PSD2.

In order to provide payment services beyond that transitional period, the existing PIs would need to submit all relevant information required under PSD2 to the competent authorities that have granted them their existing licences and fully comply with the relevant PSD2 requirements.

In addition, Member States may provide for the existing PIs to be automatically granted PSD2 authorisation if the competent authority already possesses evidence that the PI complies with the PSD2 requirements. Competent authorities shall make such an assessment on a case-by-case basis. They should inform the PI concerned before the authorisation is granted.



## XII. TRANSPOSITION

### Article reference

#### Article 115 – Transposition

*1. By 13 January 2018 Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.*

*2. They shall apply those measures from 13 January 2018.  
When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. Member States shall determine how such reference is to be made.*

*3. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.*

*4. By way of derogation from paragraph 2, Member States shall ensure the application of the security measures referred to in Articles 65, 66, 67 and 97 from 18 months after the date of entry into force of the regulatory technical standards referred to in Article 98.*

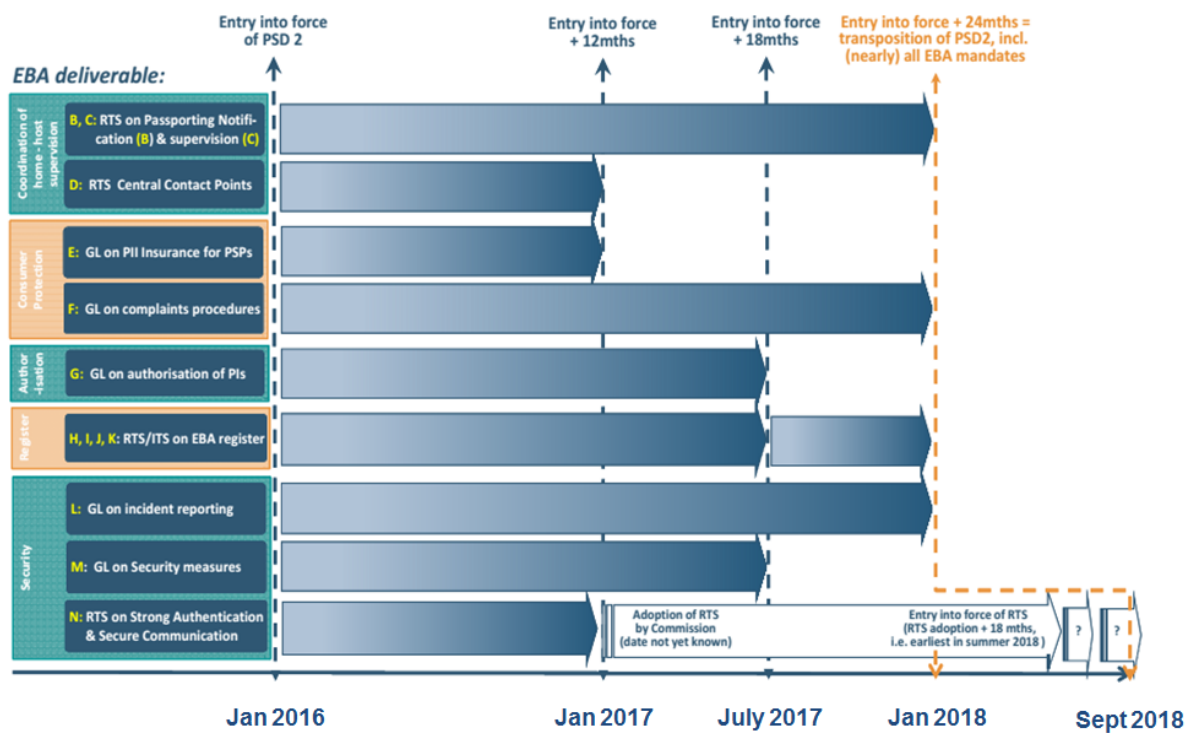
*5. Member States shall not forbid legal persons that have performed in their territories, before 12 January 2016, activities of payment initiation service providers and account information service providers within the meaning of this Directive, to continue to perform the same activities in their territories during the transitional period referred to in paragraphs 2 and 4 in accordance with the currently applicable regulatory framework.*

*6. Member States shall ensure that until individual account servicing payment service providers comply with the regulatory technical standards referred to in paragraph 4, account servicing payment service providers do not abuse their non-compliance to block or obstruct the use of payment initiation and account information services for the accounts that they are servicing.*

### Guidance and interpretation

The timeline illustrates the distinction between the different deadlines for transposition in Member States and for the application of the regulatory technical standards to be developed by the EBA in accordance with Article 98.

## PSD2 and EBA timeline



Source: EBA

Figure 7 – PSD2 transposition and EBA mandates timeline

## XIII. ANNEX A

### ARTICLES ALLOWING FOR MEMBER STATES EXEMPTIONS AND DEROGATIONS

PSD2 is a maximum harmonisation Directive, in which flexibility given to Member States in how they transpose the provisions into national law is minimal. However, it still offers some options for Member States about a certain number of dispositions. The number of available options has changed from the PSD1, but has not actually reduced in total; therefore, there is still room for fragmentation in the EU, given the amount of derogations. For this reason, the industry will have to monitor implementation; updates to this guidance will try to provide the most accurate representation of all derogations as implemented by Member States.

PSD1	PSD2	
Article reference	Article reference	Description
2 (3)	2 (5)	MS may exempt institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU from the application of all or part of the provisions of this Directive.
7 (3)	8 (3)	Derogation for MS not to apply Article 9 to PIs which are included in the consolidated supervision of the parent credit institution.
9 (2) and (3) and (4)	<b>CANCELLED</b>	Calculation of safeguarding requirements when funds can be used for future payment transactions and for non-payment services. Application of safeguarding requirements to genuine (non hybrid activities) PIs. Threshold of EUR 600 for applying safeguarding requirement.
8 (1 Method A)	9 (1 Method A)	Competent authorities may adjust the own fund requirement in the event of a material change in a PI's business since the preceding year.
8 (3)	9 (3)	The competent authorities may, based on an evaluation of the risk management processes, risk loss data base and internal control mechanisms of the PI, require the PI to hold an amount of own funds which is up to 20% higher than the amount which would result from the application of the method chosen in accordance with paragraph 1, or permit the payment institution to hold an amount of own funds which is up to 20% lower than the amount which would result from the application of the method chosen in accordance with paragraph 1.

22 (3)	24 (3)	MS may apply this Article taking into account, mutatis mutandis, Article 53 to 61 of Directive 2013/36/EU.
	29 (2) NEW	The competent authorities of the host MS may require that PI having agents or branches within their territories shall report to them periodically on the activities carried out in their territories.
	29 (4) NEW	MS may require PI that operate on their territory through agents under the right of establishment and the head office of which is situated in another MS, to appoint a central contact point in their territory to ensure adequate communication and information reporting on compliance with Titles III and IV...
26 (1)	32 (1)	MS may exempt or allow their competent authorities to exempt from the application of all or part of the procedure and conditions set out in Sections 1 to 3, with the exception of Articles 14,15,22,24,25 and 26, natural or legal persons providing payment services listed in points 1 to 6 of Annex I,...
26 (4)	32 (4)	MS may also provide that any natural or legal person registered in accordance with paragraph 1 of this Article may engage only in certain activities listed in Article 18.
30 (2)	38 (2)	MS may apply the provisions in Title III to micro enterprises in the same way as to consumers
33 (optional)	<b>Mandatory</b>	Burden of proof on the provision of information requirements lies with the PSP.
34 (1) and (2)	42 (2)	For national payment transactions, MS or their competent authorities may reduce or double the amounts referred to in par. 1. For prepaid payment instruments, MS may increase those amounts up to EUR 500.
45 (6)	Article 55 (6)	MS may provide for more favourable conditions for PSUs.
47 (3)	Article 57 (3)	However, MS may require PSPs to provide information on paper or another durable medium as least once a month free of charge.
48 (3)	Article 58 (3)	Same as under 57 (3)
51 (2) and (3)	Article 61 (2) and (3)	MS may provide that Article 102 does not apply where the PSU is not a consumer. MS may provide

		that provisions in this Title [i.e. Title IV] are applied to micro enterprises in the same way as to consumers
52 (3)	Article 62 (5)	MS may prohibit or limit the right of the payee to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments.
53 (2) and (3)	Article 63 (2) and (3)	For national payment transactions, MS or their competent authorities may reduce or double the amounts referred to in par. 1. They may increase them for prepaid payment instruments up to EUR 500. Ms may limit that derogation to payment accounts on which the electronic money is stored or payment instruments of a certain value.
61 (3)	Article 74 (1b)	Where the payer has neither acted fraudulently nor with intent failed to fulfil its obligations under Article 69, MS may reduce the liability referred to in the first subparagraph, taking into account, in particular, the nature of the personalised security credentials of the payment instrument and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.
	Article 76 (4) NEW	For direct debits in currencies other than euro, MS may require their PSPs to offer more favourable refund rights in accordance with direct debit schemes providing that they are more advantageous to the payer.
72	Article 86	For national payment transactions, MS pay provide for shorter maximum execution times than those provided for in this section.
	Article 101 (2) 3rd par NEW	MS may introduce or maintain rules on dispute resolution procedures that are more advantageous to the PSU than the one outlined in the first subparagraph. Where they do so, those rules shall apply.
88 (3)	Article 109 (2) and (4)	MS may provide that legal persons referred to in the first subparagraph or paragraph 1 of this Article shall be automatically granted authorisation and entered in registers referred to in Articles 14 and 15 if the competent authorities already have evidence that the requirements laid down in Articles 5 and 11 are complied with. The competent authorities shall inform

		the legal persons concerned before the authorisation is granted.
88 (4)	<b>CANCELLED</b>	Transitional provision for natural or legal persons eligible for the waiver under article 26.

*Figure 8 – Member States exemptions and derogations*

### PREG<sup>3</sup> members

Ruth Wandhöfer-Mosca, Citi	Chair of the Payment Regulatory Experts Group (PREG)
Pascale-Marie Brien	European Banking Federation
Ingo Beyritz	Bundesverband deutscher Banken - Germany
Wulf Hartmann	Bundesverband deutscher Banken - Germany
Gijs Boudewijn	Dutch Payments Association and Chair of the PSC
Marc van de Maarel	Dutch Payments Association – The Netherlands
Rita Camporeale	Associazione Bancaria Italiana (ABI) - Italy
Pilar Clavería	Spanish Banking Association (AEB) - Spain
Tobias Nicholas Thygesen	Danish Bankers Association - Denmark
Louise Fjord	Danish Bankers Association - Denmark
Tamas Földi	Hungarian Banking Association - Hungary
Elizabeth Fraser	Payments UK – United Kingdom
Martin Kadorik	Komerční banka (KB) – Czech Republic
Robert Macho	UniCredit Bank Austria AG - Austria
Aline Mottet	Fédération Bancaire Française (FBF) - France
Jean Petry	BGL BNP Paribas - Luxembourg
Essi Ruokanen	Federation of Finnish Financial Services - Finland
Lars Rutberg	Svenska Bankföreningen - Sweden
Veca Kovacevic-Jalisi	Electronic Money Association
Anne Willems	BNP Paribas Fortis - Belgium
Christophe Baert	MasterCard
Scott Mc Innes	
Peter Moller-Jensen	Visa
Adrian Calvo	Visa

---

<sup>3</sup> The PREG reports to the EBF Payment Systems Committee (PSC)