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, bringing together national banking associations from 45 countries, that together represent some 3,500 banks - large and small, wholesale and retail, local and international - employing about 2 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. The EBF is committed to a thriving European economy that is underpinned by a stable, secure and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere. Website: www.ebf.eu Twitter: @EBFeu.

General disclaimer

This document constitutes the second version of the guidance. In comparison to the version published in September 2016, this second edition contains guidance on the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication and other related acts, as well as guidance on the interaction between the Payment Services Directive and the General Data Protection Regulation (GDPR).
However, there are still some open questions, concerns and clarifications that could be provided of the Payment Services Directive and related acts (Regulatory Technical Standards - RTS and Guidelines issued by the European Banking Authority). For this reason, in the future EBF might further change and update contents of the Guidance.

Date of Publication 20 December 2019

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 2015/2366 (PSD2) and the related Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. Other Regulatory Technical standards, Guidelines, Compliance Tables or Opinions issued by the European Banking Authority (EBA) and the European Commission (EC) are also referred to in this document to the extent deemed necessary to clarify the issues addressed. In section XI ("*Transposition and EBA/EC mandates*"), we provide a table listing all level 2 documents adopted by the EC and the EBA pursuant to PSD2.

The document does not aim to be exhaustive in the list of topics it addresses, but rather focuses on specific issues that introduce differences with respect to the first Directive and 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 PSD2 EG and for any other queries in relation to this document, please contact Anni Mykkänen at the European Banking Federation: a.mykkanen@ebf.eu

Finally, it should be noted that no individual, banking federation or organisation who has helped develop this document can accept responsibility whatsoever for any loss or damage caused or suffered by any legal or natural 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.

This document is focused on the PSD2 text as such, the level 2 and 3 documents produced by the EC and/or the EBA as well as on the EBA Single Rulebook Q&A[1] for specific clarification needs (even if it is meant purely as a documentation tool) – and generally does not deal with the implementation and enforcement of PSD2 at the national Member State level. As an exception to the above, the document sometimes refers in footnotes to particularly noteworthy national interpretations and enforcement.

[1] https://eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/5402

Contents

Figures

I. GLOSSARY

- **Payment Initiation Service (PIS)**– "*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*" (Article 4(15) of PSD2);
- **Payment Initiation Service Provider (PISP)** – "*payment service provider pursuing business activities as referred to in point (7) of Annex I*" (Article 4(18) of PSD2);
- **Account Information Services (AIS)** "*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" (Article 4(16) of PSD2);*
- **Account Information Service Provider (AISP)** – *"payment service provider pursuing business activities as referred to in point (8) of Annex I*" ((Article 4(19) of PSD2);
- **Card-based payment instrument issuer (CISP)** is not defined as such in PSD2. However 'issuing of payment instruments' is defined as "*a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions*" (Article 4(45) of PSD2). Payment instrument means "*a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order*" (Article 4(14) of PSD2); what is relevant is that this PSP issuing the card-based payment instrument is different from the PSP servicing the account of the customer (see Recital (67)). Indeed, PSPs issuing card-based payment instrument do not manage the account of the payment service user to issue card-based payment instruments to that account and to execute card-based payments from that account.
- **Account Servicing Payment Service Provider (ASPSP)** – "*payment service provider providing and maintaining a payment account for a payer*" (Article 4(17) of PSD2);
- **Payment account** – "*account held in the name of one or more payment service users which is used for the execution of payment transactions*" (Article 4(12) of PSD2);
- **Strong customer authentication (SCA)** – "*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 4(30) of PSD2);
- **Remote payment transaction** – "*payment transaction initiated via internet or through a device that can be used for distance communication*" (Article 4(6) of PSD2);
- **Sensitive payment data** – "*data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data*" (Article 4(32) of PSD2);

II. STRUCTURE AND OVERVIEW OF THE REVISED PSD

PSD2 has preserved the structure of directive 2007/64 (**PSD** or **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).

On 23 April 2018, a corrigendum to PSD2 was published in the OJ of the EU. This corrigendum amends Recital 47 and Articles 5(2), 52, 61(1), 76(1), 89(2), 92(1), 99(1), 102(1) and 107(1) of the PSD2. On 23 May 2018 a second corrigendum to PSD2 was published in the OJ of the EU to amend Article 89(2). The changes mainly relate to liabilities and making sure the right cross-references to relevant Articles or subparagraphs are accurately shown in PSD2.

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 PSD1. Member States were 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, though some Member States have not yet transposed PSD2. Additional provisions necessary to ensure the full compliance to PSD2 are subject to different adoption times depending on the level 2 legislative process, in which the European Banking Authority **(EBA)** has been given the mandate to develop Regulatory Technical Standards **(RTS)** and Guidelines **(GL)** (for specific adoption timeline on level 2 legislation please refer to section X – *Transposition and EBA Mandates*).

PSD2 widens the scope of PSD1 by covering new services and players by extending the scope of existing services, enabling third parties (so-called Third Party Providers **-TPPs**) to be able to initiate payments and access payment account data based on explicit customer (payment service user - **PSU**) consent.

PSD2 also updates the telecom exemption by limiting it mainly to micro-payments for digital content and voiced-based services. In addition, PSD2 extends the scope to all currencies - not just those of the Member States' - and includes transactions with third countries when only one of the payment service providers is located within the European Economic Area **(EEA)** ("*one-leg transactions*"). It also enhances cooperation and information exchange between authorities in the context of authorisation and supervision of payment institutions (and electronic money institutions). The EBA has developed a central electronic register of authorised/registered payment institutions (PIs) and electronic money institutions (EMIs), which is based on information from the national registers in the 28 EU Member States and includes the payment services for which these PIs and EMIs are authorised/registered, including account information and payment initiation services

To make electronic payments safer and more secure, PSD2 also introduces enhanced security measures to be implemented by all payment service providers (PSPs). To that end, the EBA has

developed RTS, covering strong customer authentication and common and secure open standards of communication **(RTS on SCA & CSC)**[2].

[2] COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ 13 March 2018, L 69/23.

III. SCOPE AND DEFINITIONS

A. INTRODUCTION

This Directive continues to apply to "payment services provided within the Union". The scope of PSD2 currently includes the 28 EU Member States plus three Member States of the European Economic Area (EEA, i.e. Norway, Iceland and Liechtenstein). Please note that the overseas territories of EU Member States are not shown on the below map.

At time of writing (December 2019), the UK remains and must be treated as an EU Member State. Should the UK leave the EU and enter the transitional period (as determined by the Withdrawal Agreement[3]) EU law will also continue to apply, meaning the UK should be treated as an EEA state under PSD2 until the end of such a transitional period[4]. As the future relationship between the UK-EU is still under negotiation, it is not possible at time of writing to provide guidance on how PSD2 should be applied post-transitional period.

Geographical Scope of PSD2

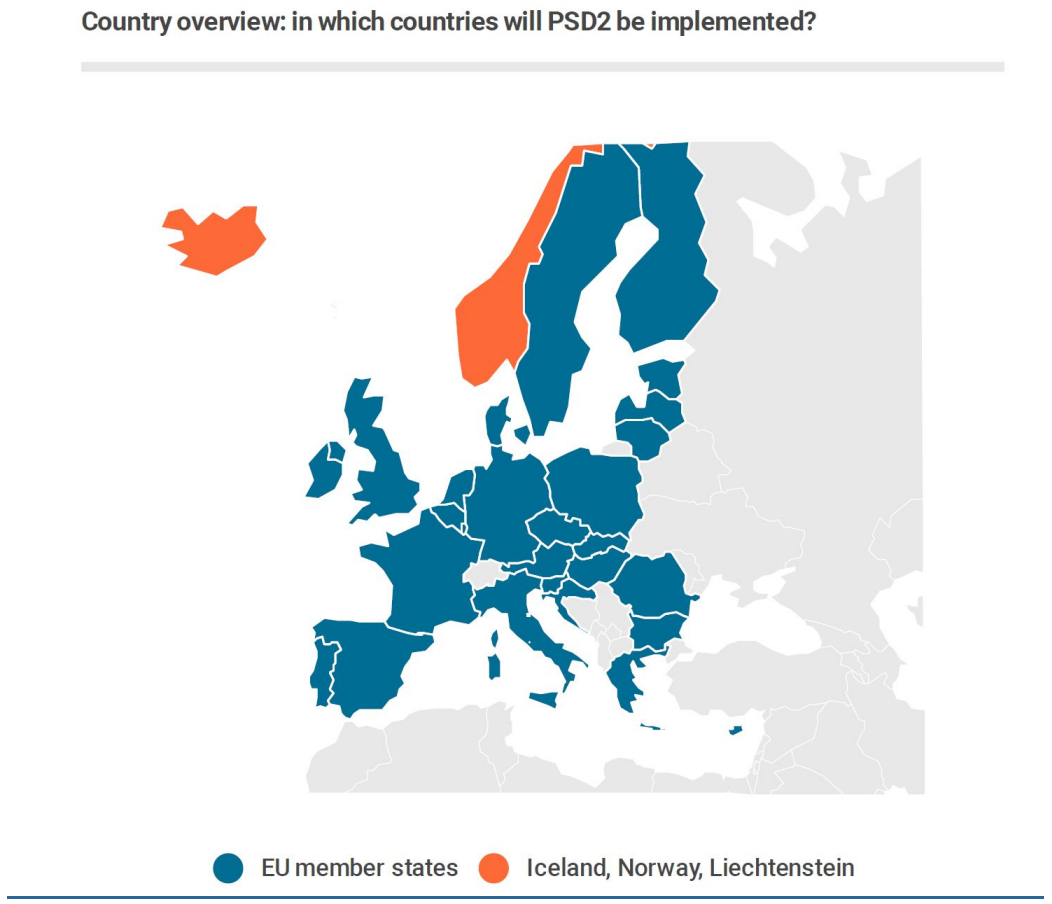


Figure 1 – Geographical scope of PSD2

[3] Full text of the WA
[4] Further details of the impact of the WA on EU law in the UK

B. SCOPE – GUIDANCE

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, located within the Union.

3. Title III, except for point (b) of Article 45(1), point (2)(e) 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 is, located within the Union, in respect to 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

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 – both the payer's PSP and the payee's PSP are located within the Union) 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. 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' – even if those countries or territories pass equivalent legislation – are one-leg transactions under PSD2.

Extension of the scope of PSD2

Article 2: Scope

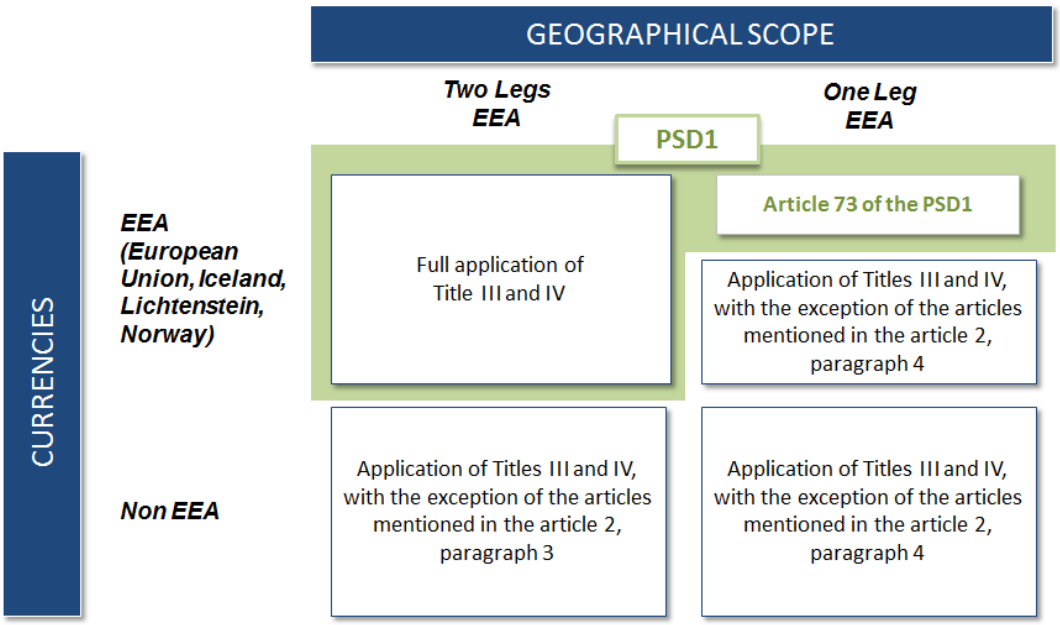


Figure 2 – Scope of PSD2

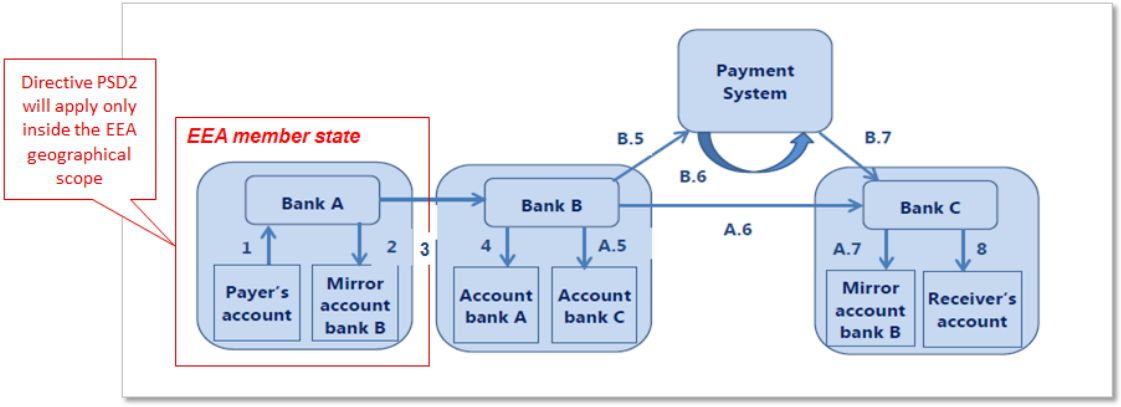
These extensions, under PSD2, apply only to those parts of the transaction that are carried out within the EEA. The wording "*in respect of those parts of the payment transaction which are carried out in the Union*" operates as a limit to the reach of PSD2 and seeks to clarify that PSPs cannot be in 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 underline that **conversions between an EEA currency and a non-EEA currency or two non-EEA currencies fall outside the scope of PSD2 as explained below**. In addition, as with PSD1, PSD2 does not apply to the inter-PSP space, but to the PSU 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



1. Debiting of payer's account with bank A
2. Crediting of bank B's mirror account with bank A, which is kept for accounting purposes
3. Payment message from bank A to bank B via telecommunication network
4. Debiting of bank A's account with bank B (loro account)

A. Use correspondent bank only

5. Crediting of bank C's account with bank B
6. Payment message from bank B to bank C via telecommunication network
7. Debiting of bank's B mirror account with bank C, which is kept for accounting purposes
8. Crediting of receiver's account with bank C

B. Involvement of payment system

5. Payment message from bank B to payment system
6. Settlement via payment system
7. Payment message from payment system to bank C
8. Crediting of receiver's account with bank C

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[5].

2) Article 2(2): Titles III and IV apply to payment transactions in the currency of a Member State where both the payer's PSP and the payee's PSP are, or the sole PSP 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 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.
- 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:

- PLN payment within Poland between Polish Zloty denominated accounts (no conversion)
- DKK payment from Denmark to Germany between DKK denominated account and EUR denominated account (with currency conversion)
- SEPA payment[6] from France to Denmark between EUR denominated account and DKK 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.

[5] Cf. https://www.efta.int/sites/default/files/documents/legal-texts/eea/the-eea-agreement/Annexes%20to%20the%20Agreement/annex9.pdf

[6] 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.
- 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 Belgium USD account to France USD account
- USD payment within the EEA (with currency conversion) e.g. from France USD account to Belgium GBP account using the "*serial method*" (see figure 4 below).
- AUD payment within the EEA from France to Belgium using the "*direct plus cover*" method (see figure 5 below).

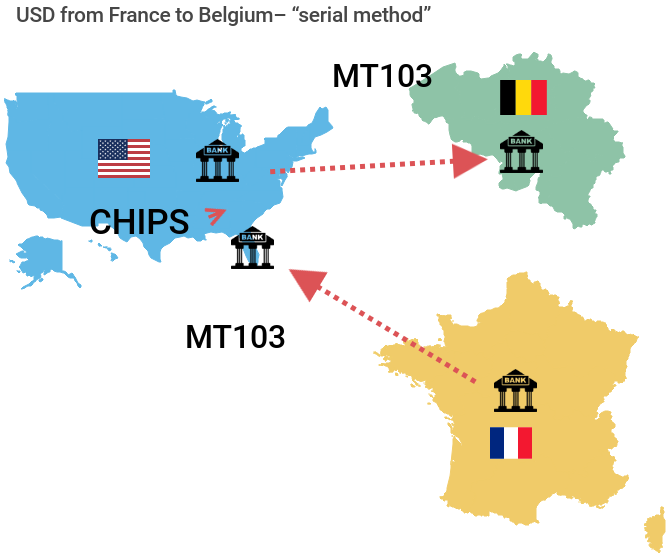


Figure 4 – USD from France to Belgium with serial method

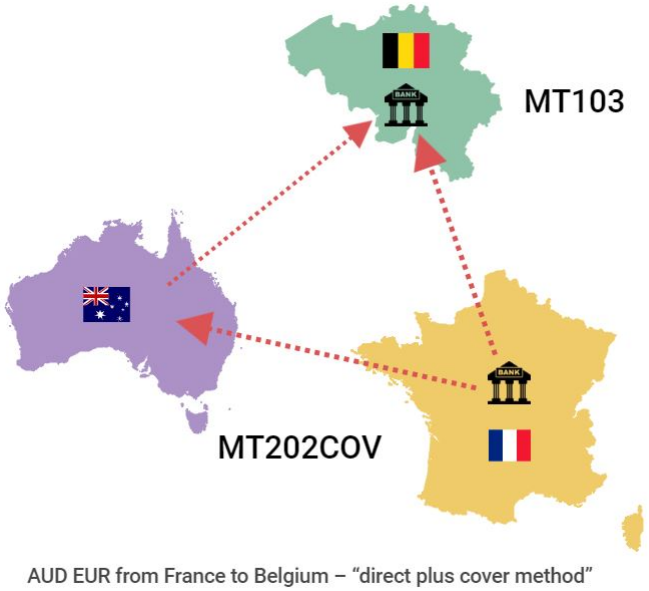


Figure 5 – AUD from France to Belgium with direct plus cover method

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.
- Although Article 97 on strong customer authentication in principle applies to one-leg in and one leg-out transactions, the EBA indicated in the final report on the RTS on SCA and CSC dated 23 February 2017 that "*In the case of cross-border transactions where payment instruments issued under a national legal framework that does not require the use of SCA (such as magnetic stripe cards) are used within the EU or when the PSP of the acquirer is established in a jurisdiction where it is not legally required to support the strong customer authentication procedure designed by the European issuing PSP, the European PSPs shall make every reasonable effort to determine the legitimate use of the payment instrument. …*". Although this was not replicated in further iterations of the draft RTS and does not appear in the final version of the RTS published in the OJ on 13 March 2018, it has been recently recalled at point 32 of the EBA Opinion issued on 13 June 2018, where EBA states that "*as explained in the final report on the draft RTS published in February 2017, the EBA's view, after discussing it with the European Commission, is that* ***SCA applies*** *to all payment transactions initiated by a payer, including to card payment transactions that are initiated through the payee within the EEA and apply* ***only on a best-effort basis for cross-border transactions with one leg out of the EEA****. In such a case, the liability regime stated by Article 74(2) PSD2 applies*", meaning that EEA-based PSPs on one-leg transactions are not expected to comply with the PSD2 requirements on SCA, but only to "*make reasonable effort to determine the legitimate use of the payment instrument*". However, this is without prejudice to the allocation of liabilities between the PSPs stated by article 74.2 of PSD2.

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[7] 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 Belgium 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 Belgium.

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.

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)

[7] 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.

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

Title & Articles	Description	PSD1	PSD2 and comments
Title III (from art. 38 to 60 with the exception of the articles mentioned below)	**Transparency** of conditions and information requirements for payment services	**A**	**A, B, C** 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
Article 45 par 1 point b)	Information and conditions (Single payment transactions): Member States shall ensure that the following information and conditions are provided or made available by the PSP to the PSU: **b) the maximum execution time for the payment service to be provided;**	**A**	**A**
Article 52 par 2 point e)	Information and conditions (Framework contracts): Member States shall ensure that the following information and conditions are provided to the PSU: on use of the payment service: **e) maximum execution time for the payment services to be provided;**	**A**	**A**
Article 52 par 5 point g)	Information and conditions (Framework contracts): Member States shall ensure that the following information and conditions are provided to the PSU: on safeguards and corrective measures: **g) the conditions for refund in accordance with Articles 76 and 77**;	**A**	**A, B**

Article 56 point a)	Information before execution of individual payment transactions: 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: **a) maximum execution time**;	**A**	**A**

Figure 6 – 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
Title IV (with the exception of the articles mentioned below)	**Rights and obligations** in relation to the provision and use of payment services	**A**	**A, B, C** 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.
Article 62 par 2 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 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.	**A**	**A, B**

	(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 (Interchange Fee Regulation - IFR) and for those payment services to which Regulation (EU) No 260/2012 applies.		
Article 71	**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 later than 13 months after the debit date….**	**A**	**A, B, C**
Article 76	Refunds for payment transactions initiated by or through a payee: (..) The payer has an unconditional right to a refund within the time limits laid down in Article 77 of this Directive. (..)	**A**	**A, B**
Article 77	Requests for refunds for payment transactions initiated by or through a payee: (1) Member States shall ensure that **the payer can request the refund** referred to in Article 76 of an authorized payment transaction initiated by or through a payee **for a period of eight weeks from the date on which the funds were debited**. (2) Within 10 business days of receiving a request for a refund, **the PSP shall either refund the full amount** of the payment transaction **or provide a justification for refusing the refund** 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. (..)	**A**	**A, B**
Article 81	Amounts transferred and amounts received (Execution of payment transactions): Member States shall require the PSPs of the payer, the PSPs of the payee and any intermediaries of the PSP to **transfer the full amount of the payment transaction and refrain from deducting charges** from the amount transferred. (..)	**A**	**A**

Article 82	Scope (Section 2 – Execution time and value date): (1) a) payment transactions **in euro**; b) national payment transactions in the currency of the Member State **outside the euro area**; c) payment transactions involving only **one currency conversion** 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 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 **payment transactions not referred to in the paragraph 1**, unless otherwise agreed between the PSU and the PSP, with the exception of Article 87 (...)	**A**	**A, C**
Article 83 par 1	Payment transactions to a payment account (Execution time & value date): the payer's PSP shall ensure that after the time of receipt as referred to in Article 78, the **amount** of the payment transaction **will be credited to the payee's PSP's account by the end of the following business day**. That time limit may be **extended by a further business day for paper-initiated payment transactions**.	**A**	**A**
Article 83 par 2 and 3	Payment transactions to a payment account (Execution time & value date): the PSP of the payee shall **value date and make available the amount** of the payment transaction **to the payee's payment account** after the PSP has received the funds in accordance with Article 87; the payee's PSP shall **transmit a payment order** initiated by or through the payee to the payer's PSP **within the time limits agreed between the payee and the PSP (..)**	**A**	**A, C**
Article 84	Absence of payee's payment account with the PSP (Execution time & value date): Where the payee does not have a payment account with the PSP, the **funds shall be made available to the payee by the PSP** who receives the funds for the payee **within the time limit laid down in Article 83**.	**A**	**A, C**

Article 85	Cash placed on a payment account (Execution time & value date): Where a consumer places cash on a payment account with that PSP in the currency of that payment account, the PSP shall ensure that **the amount is made available and value dated immediately after receipt of the funds**. 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.	**A**	**A, C**
Article 86	National payment transactions (Execution time & value date): For national payment transactions, Member States may provide for **shorter maximum execution times** than those provided for in this Section.	**A**	**A, C**
Article 87	Value date and availability of funds: 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) **no currency conversion**; or (b) a **currency conversion** between the euro and a Member State currency or between two Member State currencies.	**A, C** Under PSD1, C only applied to EEA currencies	**A, B, C** 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.
Article 89	PSPs' liability for non-execution, defective or late execution of payment transactions	**A**	**A, B**
Article 92	Right of recourse (Section 3 - Liability)	**A**	**A, B**

Figure 7 – 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 service providers
- 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)

Compared to PSD1, some exclusions from the scope have been revised and narrowed down. These include the commercial agent exclusion (Article 3(b)), the limited nertwork exclusion (Article 3(k)) and the telecom exclusion (Article 3(l)). For the two latter exclusions, an obligation to supply information to the competent authority has been added in Article 37 (2) and 37(3) respectively.

Article 3(b)

(b) payment transactions from the payer to the payee through a commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee;

Guidance

Commercial agents (on behalf of the payee or of the payer, but not for both parties): the exemption was narrowed down by PSD2 compared to PSD1. Under PSD1 the commercial agent exemption was applied very differently across the Member States; in particular in some Member States e-commerce platforms that act as an intermediary on behalf of both individual buyers and sellers without a real margin to negotiate or conclude the sale or purchase of goods or services were allowed to benefit from the exemption. Under PSD2 the commercial agent exemption should apply when agents act only on behalf of the payer or only on behalf of the payee, regardless of whether or not they are in possession of client funds. Where agents act on behalf of both the payer and the payee, they should be excluded only if they do not, at any time enter into possession or control of client funds. PSD2 also further amends the exemption by stating that the agent needs to be authorised to negotiate or conclude the sale/purchase via an agreement.

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

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 the 2nd e-money directive (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[8].

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(l)

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;

[8] For example, BaFin published a guidance to the PSD2 according to which the exclusion for premises is applicable for department stores as well as for shop-in-shop solutions "under one roof" (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html?nn=9450978#doc7846622bodyText24).
The UK FCA has also published guidance on the use of the limited network exclusion for payment cards (https://www.handbook.fca.org.uk/handbook/PERG/15/5.html).

Guidance

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

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*".

B. KEY DEFINITIONS – GUIDANCE

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 includedin PSD2 (for example: 'credit transfer' taken the SEPA Regulation (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
Articles 4(12) - Definitions

12. "'*payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions*".

Guidance

The definition of payment account in PSD2 is identical to the definition "*payment account*" in PSD1. The following statements made by the EC in its PSD1 Q&A[9] in relation to the concept of payment account under PSD1 are therefore relevant to understanding what constitutes a payment account under PSD2:

- Question 11: "*Mortgage accounts established by the mortgage lender (e.g. a credit institution) in conjunction with a mortgage loan on a residence, into which the borrower is required to make regular periodic payments, are not to be considered as 'payment accounts' within the meaning of the PSD as the holder of the debt is the lender: in case of early repayments, the lender (e.g. the credit institution) is to be considered as 'the payee' (and not only as a payment service provider). However, when one account combines e.g. mortgage, saving and payment facilities in order to reduce the overall mortgage balance, this should be considered as 'payment account' within the meaning of the PSD as far as it is used for making payment transactions*". See also question 31.
- Question 25: "*… savings accounts where the holder can place and withdraw funds without any additional intervention or agreement of his payment service provider should be considered as payment accounts within the meaning of the PSD. On the contrary, fixed term deposits should fall out of this category as the funds are taken and paid back by the payment service provider and the holder of the deposit does not keep any freedom to place additional funds or withdraw funds during the term of the deposit*". See also questions 150, 187, 262.

[9] https://ec.europa.eu/info/sites/info/files/faq-transposition-psd-22022011_en.pdf

- Question 325: "*Complete anonymous prepaid products used for the execution of payment transactions do not qualify as payment accounts for the purposes of the PSD, but as e-money. Only from the moment the prepaid card is registered in the name of 'one or more payment service users' and a payment account is created on their behalf, it could fall within the definition under Article 4(14).*"
- Question 371: "*Loan agreements established via a credit platform do not fall within the scope of the 'payment account' definition under Article 4(14) of the PSD.*"[10]

Articles 4(15), 4(18) and 4(12) - 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.*"

18. "'*payment initiation service provider' means a payment service provider pursuing business activities as referred to in point (7) of Annex I*"

Guidance

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) entails a contractual relationship between the PISP and the merchant. Payers could use a payment initiation service to initiate a payment (on a one-off or ad-hoc basis) via the merchant's web site, typically leveraging online banking services made available by the Account Servicing PSP (ASPSP) ("*accessible on line*"), and for which the payer has given his/her explicit consent.

The ASPSP is required to "*immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider*" (Article 66(4)(b) – see also Article 36(1)(b) of the RTS).

[10] In its judgment issued on 4 October 2018 (case C-191/17), the Court of Justice of the European Union concluded that Article 4(14) of PSD1 must be interpreted as meaning that a savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account does not come within the concept of 'payment account'. Although it was decided on the basis of PSD1, it will also apply to PSD2 since the definition of "payment account" is the same in both directives.

Article Reference

Articles 4(16) and 4(19)

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*."

19. "'*account information service provider' means a payment service provider pursuing business activities as referred to in point (8) of Annex I*"

Guidance

The aggregation of information on payment accounts is offered to PSUs in some European countries since some time and it allows clients to obtain a consolidated view on their payment accounts. Recital 28 states that, through Account Information Services (AIS), the PSU is able to have an "*overall view of its financial situation*" from payment accounts **held with one or more other payment service providers** and article 67(2)(d) limit the access of AIS providers only to "*the information from designated payment accounts and associated payment transactions*".

In accordance with Article 36(1)(a) RTS, the ASPSP is required to provide the AISP with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data. This may include account balances of the payment accounts 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).
Other features and information around a payment account (personal data of the holder, terms, conditions, fees) and non-payment services like mortgages, loans, deposit accounts are out of scope of what is generically called "*Access to account (XS2A)*" services under the PSD2.
In all circumstances, as a precondition to access to information on payment account through an AISP, the PSU must have previously chosen and agreed to use the online banking service offered by the Account Servicing PSP (ASPSP).

Sensitive payment data is defined in PSD2 as "*data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number (IBAN) do not constitute sensitive payment data*" (Article 4(32) PSD2).

It is also helpful to refer to the ECB Assessment Guide For The Security Of Internet Payments of February 2014[11], which provides an indicative list of elements that could, depending on the circumstances under which the data are used, be considered as sensitive payment data:

"- data used for authentication (when applicable and used in this context), such as:

- *customer identifiers (e.g. client number/log-in name);*
- *passwords, codes, personal identification numbers (PINs), secret questions,*

[11] Available here: https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf

reset passwords/codes;

- *phone number (mobile or landline, when applicable);*
- *certificates;*

- data used for ordering payment instruments or authentication tools to be sent to customers (offering this functionality online in the case of PSPs, otherwise those data that are not considered sensitive), e.g.

- *client's postal address;*
- *phone number, e-mail address;*

- data, parameters and software stored in the PSP's systems which, if modified, may undermine the security of the delivery of payment instruments or authentication tools to the customer or may affect the latter's ability to verify payment transactions, authorise e-mandates or control the account, e.g.

- *"black" and "white" lists, customer-defined limits, etc.*
- *data outlined in (a), (b) and (c), depending on applicability and methods used."*[12]

IV. AUTHORISATION AND REGISTRATION OF PAYMENT INSTITUTIONS

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;

[12] Page 7 of the ECB Assessment Guide.

Guidance

Under PSD2, Payment Institutions (PIs) are required to fulfil a variety of requirements in order to obtain an authorisation to provide payment services (listed in Annex I of PSD2). 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 with the exception of new capital requirements for payment institutions performing PIS activities (€ 50,000 in accordance with Art 7(b) PSD2). There are no initial capital requirements for AIS activities.

Payment Initiation Service Providers (PISPs) will have to be authorized and Account Information Service Providers (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. The EBA has provided guidance on the information to be provided for authorisation/registration of PISP and AISP (EBA/GL/2017/09). PISPs and AISPs must hold a professional indemnity insurance or comparable guarantee to cover their liabilities in this respect. The EBA has provided guidance on the criteria on how to stipulate the minimum amount of professional indemnity insurance or other comparable guarantee (EBA-GL-2017-08).
Passporting is the exercise by a business of its right to carry on activities and services regulated under EU legislation in another EEA State on the basis of authorisation or registration in its home EEA State. The activities may be carried on through an establishment in the host state (establishment passport) or on a cross-border services basis without using an establishment in the host state (cross-border service passport).

Payment Institutions, PISPs and AISPs may exercise passporting rights under PSD2 to carry on payment services in another EEA State. The Commission has adopted RTS on passporting[13] which covers the passporting application process.

The definition of PIS covers services to initiate a payment order at the request of the payer with respect to a payment account held at another PSP located in one of the EEA States. More precisely, the payer "*has the right to make use of a PISP to obtain the service referred to in point (7) of Annex I of PSD2*" if the payment service is provided within the EEA according to article 2 of PSD2.

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

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1541765198306&uri=CELEX:32017R2055

(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 Reference
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

PSD2 mandates Public Registers in the different Member States to be publicly available for consultation, accessible online, and updated without delay. PSD2 also mandates the EBA to develop a "central register". This is explained in recital 42 of PSD2 indicating that to 'ensure easy public access to the list of the entities providing payment services. EBA hastherefore developed and operate a central electronic register in which it publishes a list of the names ofpayment institutions, electronic money institutions, exempted payment insitutions, exempted electronic money institutions, AISPs exempted under Article 33 of PSD2, institutions entitled under national law to provide payment services, branches, agents and service providers as referred to in Article 3(k) and (l) of PSD2. Credit institutions (which can also provide payment services, including AIS and PIS) are included in the separate EBA register for credit institutions. Member States should ensure that the data that they provide is kept up to date. Those measures should also contribute to the enhancement of the cooperation between the competent authorities.

The requirements of the central register of the EBA are set forth in Article 15 PSD2.

On 13 December 2017, the EBA issued the final Report on the RTS and the ITS on the EBA register for adoption by the European Commission ("*Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2)*" and "*Draft Implementing Technical Standards on the details*

and structure of the information entered by competent authorities in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366"), respectively EBA-RTS-2017-10 and EBA-ITS-2017-07.

These final drafts define three main functional features of the register:

1. the content (i.e. which are the service providers listed and which is the related information)
2. the alignment of the EBA's register in case of any change in the CA's register
3. how any interested party (consumers and service providers) can access and copy the content of the register.

The EBA electronic central register[14] includes all providers authorized and/or registered in the EEA as:

- payment institutions, their branches in host Member State and their agents in home and host Member State;
- account information service providers, their branches in host Member State and their agents;
- electronic money institutions, their branches in host Member State and their agents in home and host Member State;
- natural or legal person benefiting from various exemptions (Article 32 of Directive (EU) 2015/2366 and their agents, Article 9 of Directive 2009/110/EC and their agents, service providers carrying out services under points (i) and (ii) of point (k) and point (l) of Article 3 of Directive (EU) 2015/2366);

For each of the above mentioned providers listed in the EBA register, NCAs communicate to the EBA a different set of information to be stored. For instance, a record related to a payment institution contain the name, the type of natural or legal person, the commercial name, the full address and country, the payment services for which the PI has been authorised and/or registered, the status and the dates of granting or withdrawal of authorisation/registration, and which payment services it is providing or intends to provide in which host member States.

The EBA register is directly updated by the NCAs. The NCAs opt between automatic and manual means to feed and change the information in the EBA register. In both cases NCAs are obliged to insert in the electronic central register all changes in their national registers related to the granting or withdrawal of authorisation or registration by the end of the same day. Once the data is technically and automatically validated by the EBA, it is immediately published and made available; a time stamp displays the moment of the last change/synchronisation between the EBA register and the national registers.

The EBA has made available a search engine for the public in its website through a set of criteria. In order to obtain a copy of the full content, public users will be also able to download the electronic central register into a machine-readable standardised file at least twice a day at pre-agreed intervals. The EBA shall disclose the pre-agreed intervals for such updates.

However, the EBA electronic central register does not include credit institutions. This is because the EBA's mandate, under Article 15(5) of PSD2, requires the EBA to maintain a register based on a pre-defined list of institutions in which, however, credit institutions are not included. Banks are entered into the register of credit institutions, which is also maintained by the EBA.

[14] https://eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2

Therefore, ASPSP are able to verify the valid authorisation/registration of TPPs in both registers – the EBA register maintained under PSD2 and the EBA's credit institutions register, the latter containing the indication of ASPSPs acting as TPPs.

Regarding some recurrent doubts in the market about the requirement for credit institution to acquire further authorisation/registration to provide AIS and/or PIS, the EBA confirmed that: "*all authorised credit institutions are entitled to provide the whole range of payment services, including AIS and PIS, and to do so without any need for additional authorization*"[15].

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*** *I 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

Article 5(3) states that AISPs do not need to be authorised by the NCA but they have to apply in order to be registered. After the registration, they are subject to the prudential supervision by the NCA 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) provided they comply with the passporting notification procedure.

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;

[15] Para. 26 of the *Final Report on Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2),and Draft Implementing Technical Standards on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366 (PSD2)* (EBA/RTS/2017/10 and EBA/ITS/2017/07).

(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

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 does not apply to three-party card schemes that operate as *de facto* four-party card scheme..

PSD1 subjected traditional four-party scheme (4PS) to an "*access*" requirement, meaning that those schemes had to grant licenses to PSPs to issue cards and/or acquire transactions on "*objective, non-discriminatory and proportionate" conditions*[16]*.* Three-party scheme (3PS) were not subject to this access requirement[17], meaning that a 3PS was free to decide which, if any, PSPs would be allowed to participate in any part of its scheme. For example, it allowed a 3PS to decide to operate in way which was quite similar to a 4PS in some EU countries (e.g. by working with one or more other PSPs), while operating in a purely closed manner in others.

In PSD2, 3PS are in principle still free to decide if any PSP would be allowed to participate in any part of its scheme, except where they *operate as de facto four-party card schemes, for example by relying upon licensees, agents or co-brand partners*"[18].

The above was clarified by the CJEU in Case C-643/16, where the Court concluded that *"a three party payment card scheme that has entered into a co-branding agreement with a co-branding partner does not lose the benefit of the exception provided for by that provision and, therefore, is not subject to the obligation laid down in Article 35(1) of that directive in a situation where that co-branding partner is not a payment service provider and does not provide payment services within that scheme with respect to the co-branded products. However, a three party payment card scheme that makes use of an agent for the purposes of supplying payment*

[16] Article 28 PSD1.
[17] See Article 28(2)(C) PSD1 and Recital 17 PSD1.
[18] Recital 52 PSD2

services loses the benefit of that exception and, therefore, is subject to the obligation laid down in Article 35(1).”

The PSD2 access requirement should be read in conjunction with Article 6 IFR which provides that "*Any territorial restrictions within the Union or rules with an equivalent effect in licensing agreements or in payment card scheme rules for issuing payment cards or acquiring card-based payment transactions shall be prohibited*". In other words, a PSP (e.g. an acquirer) permitted to acquire 3PS transactions in one EU Member State should also be allowed to acquire those transactions in other EU Member States.

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

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.

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 2014/92/EU of 23rd July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, the so called Payment Accounts Directive "*PAD*" - 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 ASPSPs, the review of the information requirements should aim to make the PSU aware about the separate roles and services of the ASPSP 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*".

Article Reference

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

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).

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

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(1): 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

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

Article Reference

Article 44(1): Prior general information

Member States shall 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

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) ASPSPs do not need to describe the specific services that TPPs might offer. The information now needs to be provided in an easily accessible manner.

Article Reference

Article 45: Information and condition

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.

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

Article 45 has been amended to take into account the introduction of PISPs into the scope of the Directive. Article 45 (1), point a) 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[19]. 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 PSU 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 PAD.

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

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 ASPSP 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.

[19] While the chapter covers single payment transactions and AISPs do not initiate or execute "transactions" (they just collect and aggregate data , the logic must be that AISPs are subject to the information requirements regarding one-off interactions with PSUs.

Guidance

The requirement to provide the reference of the payment transaction needs to be seen in the context of the wider communication between ASPSPs 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. provided by the PISP both to the PSU and to the ASPSP.

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

Guidance

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 and 90.*

Guidance

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:

- 52(2)(g): In case of co-badged card-based payment instruments, the PSU's right under article 8 of the Interchange Fee Regulation.
- 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*".
- 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 ASPSPs will need to update all framework contracts to add this new procedure. According to Guidelines on the security measures for operational and security risks of payment services (EBA/GL/2017/17), EBA states the following:
  - Guideline 9.2 "*the assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and* ***changes should be communicated to the PSU****"*
  - Guidelines 9.6 "***PSPs should keep PSUs informed about updates in security procedures*** *which affect PSUs regarding the provision of payment services*", and
  - Guideline 9.7 "*PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services.* ***PSUs should be appropriately informed about how such assistance can be obtained****".*

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

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). The PSP should provide the information on changes on durable medium in easily understandable words and in clear and comprehensible form, in language of the state where the services are offered or other language agreed by the parties.

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

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

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

This article includes an additional reference to currency conversion offered at an ATM (in addition to transactions 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 (1) and (2): 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

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 PISP 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

1. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 62(1), Article 64(3), and Articles 72, 74, 76, 77, 80 and 89 do not apply in whole or in part. The payment service user and the payment service provider may also agree on time limits that are different from those laid down in Article 71.

2. Member States may provide that Article 102 does not apply where the payment service user is not a consumer.

3. Member States may provide that provisions in this Title are applied to microenterprises in the same way as to consumers.

4. This Directive shall be without prejudice to Directive 2008/48/EC, other relevant Union law or national measures regarding conditions for granting credit to consumers not harmonised by this Directive that comply with Union law.

Guidance

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, 89 and 90 "*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.

VI. CHARGES APPLICABLE

Article Reference

Article 62(2) to (5): 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 (Interchange Fee Regulation) and for those payment services to which Regulation (EU) No 260/2012 applies(SEPA Regulation).

5. Member States 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.

Article 81: Amounts transferred and amounts received

1. Member States shall require the payment service provider(s) of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers to transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.

2. However, the payee and the payment service provider may agree that the relevant payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.

3. If any charges other than those referred to in paragraph 2 are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. Where the payment transaction is initiated by or through the payee, the payment service provider of the payee shall ensure that the full amount of the payment transaction is received by the payee.

Guidance

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 only to intra-EEA payments in EEA currencies and "*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 and therefore charges in this case can be applied in a discretionary manner: for example: SHA, OUR and BEN options are permitted.

Article 62(2) should also be read in joint combination with the full amount principle under Article 81. In particular:

- The sharing of charges principle applies only to two legs-transactions in all currencies
- The full amount principle applies only to two legs-transactions in EEA currencies, (according to exceptions stated in article 2(3) and 2(4)).

Therefore, 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) is subject to full PSD2 scope enlargement and therefore for all transactions in all currencies, in case of surcharge, the payer can be requested to pay the charges applied by the payee (e.g. the merchant) for accepting a given payment method, provided that these charges cannot exceed the direct costs borne by the payee for the use of the specific payment instrument. Payees are therefore allowed to apply surcharges, with the exception for those payment instruments capped under the Interchange Fee Regulation (as per Article 62(4)) in the case of two legs-transactions regardless of the currency (as per article 2(4)). Surcharging is also forbidden for the payee in case of payment services to which the SEPA Regulation (Regulation (EU) No 260/2012) applies, i.e. SEPA Direct Debit and SEPA Credit Transfers.

In general, payees are always free to offer discounts or otherwise steer use of a given payment instrument through other means than surcharging (see also Article 10 IFR as regards card-based payments).

PSD2 gives Member States the option to adopt a broader surcharging ban. The majority of Member States have decided to make use of that option and completely ban surcharging on all transactions. A few Member States however kept the partial ban provided for in PSD2, which may lead to different client experiences within the EEA.

EXECUTION OF PAYMENT TRANSACTIONS

Section 1 – PAYMENT ORDER AND AMOUNT TRANSFERRED

Article Reference

Article 78(2) – Receipt of payment orders

1. "*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

Pursuant to Article 61 PSD2, the PSP and the PSU may agree that Article 80 does not apply in whole or in part.

In general the principles governing irrevocability have not changed from PSD1 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), except in cases falling under Article 80(5), where the payment order may be revoked if agreed between the payment service user and the relevant payment service providers (including PISPs).
Specifically, 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 in case they offer future transaction dates.

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.

An execution time period longer than that set out in Article 83 may be agreed between the PSU and his/her 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 reference

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

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 in respect to those parts of the payments transaction which are carried out in the Union.

For the purposes of availability of funds, with respect to article 87(2), the rule applies i) to transactions in non EEA currencies but only in the absence of currency conversion and ii) to transactions in EEA currencies, even in case of currency conversion between such currency and Euros or between 2 EEA currencies and iii) to payments performed within one payment service provider regardless of the currency and following the same obligations at point i) and ii).

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 detailed 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 up to D+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 PSP systems open) as it closely depends on the PSP business day in which it is operational.
For one-leg transactions in non EEA currencies, the credit value date should not be later than the business day on which the exchange value of the transaction is credited to the payee's PSP's account held in the Union.

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 execution process only begins once the required currency has been obtained (e.g. a SEPA payment from a Danish DKK account will only be initiated once the required Euro amount is available). Therefore the debit value date should be not earlier than the execution date (which corresponds to the date when the payer's account is debited).

Section 3 – LIABILITY

Article reference

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

Pursuant to Article 61 PSD2, where the PSU is not a consumer, the PSP and the PSU may agree that Article 89 does not apply in whole or in part.

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".

Pursuant to Article 61 PSD2 as amended by the PSD2 Corrigendum, the PSP and the PSU may agree that Article 90 does not apply in whole or in part.

This new article is included to describe the liability of PISPs in case of non-execution, defective or late execution of payment transactions. The ASPSP must refund the payer with the amount of the unauthorised payment transaction. The PISP is obliged to compensate the ASPSP 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 ASPSP, unless the PISP is able to prove that it was not responsible for the unauthorised payment transaction. The communication and process standards for the interaction and resolution of events between ASPSPs and TPPs is not defined under PSD2. The ERPB WG has suggested that there should be common business practices on standardised processes for dispute handling between ASPSP and PISP[20].

[20] The report of the ERPB can be found here: https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf?483e4d28242cd84322850a01e549d116

VII. 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."

Guidance

Article 95 addresses operational and security risks and aspects of authentication.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.
In the final "*Guidelines on the security measures for operational and security risks of payment services*", the EBA sets out that PSPs should establish:

- an effective operational and security risk management framework which should be approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management. The framework should be properly documented;

- a sound risk assessment, identifying functions, processes and assets, classifying them in terms of criticality and continuously monitoring threats and vulnerabilities and regularly review the risk scenarios;
- preventive security measures against identified operational and security risks, by instituting multi-layered controls covering people, processes and technology.
- processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities in the provision of payment services;
- sound business continuity management to maximise their ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption. PSP should test their business cointinuity plans at least annually; plans should be updated at least annually, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes;
- testing framework that validates the robustness and effectiveness of the security measures. For systems that are critical for the provision of their payment services, tests shall be performed at least on an annual basis; non-critical systems should be tested regularly on a risk-based approach, but at least every three years;
- processes and organisational structures to identify and constantly monitor security and operational threats that could materially affect their ability to provide payment services;
- PSPs should establish a training programme for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures. PSPs should ensure that the training programme provides for training staff members at least annually, and more frequently if required;
- processes to enhance PSUs' awareness of security risks linked to the payment services by providing PSUs with assistance and guidance.

All PSPs should comply with all the provisions set out in the Guidelines according to the NCAs declaration on their intention to comply or not; the level of detail should be proportionate to the PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide.

It has to be noted that the GL on security measures for operational and security risks will be replaced by the new ones on ICT and security risk management, whichhave been finalised by the EBA[21].

Article reference

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."

[21] https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

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."

Guidance

The EBA issued guidelines on major incident reporting (EBA/GL/2017/10). The impact of the Guidelines in combination with requirements set out in GDPR and the NIS Directive is that a multitude of notifications related to the same incident under is to be sent without undue delay to different authorities at both national and European levels, using different formats based on different criteria.

The final guidelines mainly set:

- The classification as major incident, i.e. when the incident met one or more criteria at the 'Higher impact level', or three or more criteria at the 'Lower impact level'. Criteria for the classification are the transaction affected, the PSUs affected, the service downtime, the economic impact, high level of internal escalation, if other payment service providers or relevant infrastructures potentially are affected, the reputational impact. If the 'impact level' is 'higher' or 'lower' depends on different values asssigned to thresholds for each of the mentioned criterion. See the below table extracted from the EBA guidelines.

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **and** > EUR 100 000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 5 million
Payment service users affected	> 5 000 **and** > 10% of the payment service provider's payment service users	> 50 000 **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital,* EUR 200 000) **or** > EUR 5 million
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

- The notification process. After having assessed an incident as major the PSP has to produce a report using a pre-defined template and submit it to the competent authority in the home Member State. The report has to be provided to the NCA throughout the lifetime of the incident (i.e. for initial, intermediate and final reports) within defined time deadline (for instance, the initial report should be submitted to the NCA within 4 hours from the detection of the major incident)

The 'Procedure for notifying NCAs' set forth on the GL on major incident reporting (para. 3.2) overlaps with the Procedure of the EBA guidelines on the security of internet payments. The EBA in its 'Opinion on the transition from PSD1 to PSD2' clarified that the Procedure in the GL on major incident reporting superseeds the application of the 2014 GL on security of internet payments. The GL on major incident reporting are applicable as of 13 January 2018 (provided that PSD2 has been implemented in the relevant jurisdiction).

Article reference

Article 96(6) – Fraud reporting

"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

In relation to paragraph 6, the EBA published the final GL on fraud reporting under PSD2 (EBA/GL/2018/05) on 18 July 2018. According to point 34 of the Final Report, the date of application of these GL is January 2019, except for the reporting of data related to the exemption to the requirement to use SCA, for which data collection will only be applicable when the RTS on SCA & CSC are enforced (14 September 2019). For the transitional period, between the implementation of PSD2 and 1st January 2019, the EBA clarifies that, for the period between 13 January 2018 (or the date of application of the national legislation transposing PSD2 if this is later) and 31 December 2018, PSPs will not be required to report the data foreseen under the EBA GL on fraud reporting.

In addition, it is important to notice that EBA clarifies that the GL and the RTS on SCA & CSC are aligned to the extent that the same two categories included in the reporting for the purpose of the EBA GL, namely unauthorised transactions and transactions as a result of the manipulation of the payer, should be used to calculate the fraud rate (as also explained in paragraph 46 of the EBA Opinion published on 13 June 2018).

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

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 at their branches (if present), and in the general terms and conditions of the contract between PSP and PSU.

VIII. ACCESS TO PAYMENT ACCOUNTS

A. CONSENT

Article Reference

Article 64 – Consent and withdrawal of consent

"*1. Member States shall ensure that **a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction**. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction.*

*2. **Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider**.*
In the absence of consent, a payment transaction shall be considered to be unauthorised.

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.

4. The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).”

Articles 65, 66, 67 – respectively Card-Based Payment Instrument Issuers (CISPs), PISPs and AISPs

- CISP - Article 65(2)(a): "*The payment service provider may request the confirmation referred to in paragraph 1 where all of the following conditions are met: (a) the payer has given explicit consent to the payment service provider to request the confirmation referred to in paragraph 1;*" and 65(1)(c) “*the consent referred to in point (b) [of paragraph 1] has been given before the first request for confirmation is made.”*

- PISP - Article 66(2): "*When the payer gives its explicit consent for a payment to be executed in accordance with Article 64, the account servicing payment service provider shall perform the actions specified in paragraph 4 of this Article in order to ensure the payer’s right to use the payment initiation service.*"
- AISP - Article 67(2)(a): "*The account information service provider shall: (a) provide services only where based on the payment service user’s explicit consent;*"

Article 94(2) – Data Protection

“*2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user*”.

Guidance

When referring to “*consent*”, it is first of all important to distinguish the different stages of the payment service flow and therefore the specific type of consent we are talking about. In particular it is possible to identify the following types:

- **Consent for the provision of services (to the TPP):** it is the consent given by the PSU to the TPP for the provision of CISP, PISP and/or AISP services. CISPs, PISPs and AISPs need the explicit consent from the PSU before they can provide payment services and benefit from the prerogatives set out respectively in article 65, 66 and 67. More details regarding this type of consent can be found both in PSD2 and in the RTS on SCA & CSC. In particular:
    - Recital 93 of PSD2 states that “*It is necessary to set up a clear legal framework which sets out the conditions under which payment initiation service providers and account information service providers can provide their services with the consent of the account holder without being required by the account servicing payment service provider to use a particular business model, whether based on direct or indirect access, for the provision of those types of services*”. It should be noted that the provision of consent can differ from CISP, PISP and AISP perspective. For example Recital 10 of the RTS states that “***consent can be given individually for each request of information or for each payment to be initiated or, for***

account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user". This may be some agreed form, even if not the only ones. It is important that the **forms agreed are not such as to require the ASPSP to carry out "*additional checks of the consent*** *given by the PSU to the TPP*", as stated in article 32.3 of the RTS.

The TPP has to collect the explicit consent from the PSU for the provision of the specific payment services, there is a risk that, in case a payment is initiated by a PISP, the ASPSP 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/withdrawal of consent in relation to payment initiation services also to the ASPSP (although some national implementation laws may be more specific on this point). It should be noted that according to Article 32(3) of the RTS on SCA & CSC, ASPSPs should not carry out any additional checks on the consent given by the PSU as otherwise this may constitute an obstacle to TPP services.

- **Consent to execute a payment (through a TPP or not):** it refers to the authorization of the payment transaction by the PSU and with the possible involvement of a PISP. The consent for the execution of a payment may be given via the PISP, as foreseen in Article 64(2) PSD2. Considering that the consent to execute a payment "***shall be given in the form agreed between the payer and the payment service provider***" (see art. 64(2) PSD2) and "***in accordance with Article 80***" (see art. 64(3) PSD2), ASPSP may add a specific provision in the contract between an ASPSP and his PSU stating the possible forms to be agreed to as well as the procedure for giving consent (see art. 64(4) PSD2). ASPSPs are required (see Art. 66(4) PSD2) to provide or make available to the PISPs all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction.

- **Consent to access, process and retain (store) personal data**: it is the consent the PSU has to give to the PSP to process the personal data in line with article 94 on data protection. This user consent is especially important in view of the General Data Protection Regulation (GDPR), in case the ASPSP needs to provide account-related information (see section XI on interplay PSD2 / GDPR).

B. 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

PSD2 refers to PSPs issuing card-based payment instruments but does not separately define these Card-Based Payment Instrument Issuers (sometimes shortened as CISPs or also as PIISPs, CBPIIs). 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 that the servicing the account of the customer, would provide increased competition in the market and thus more choice and a better offer for consumers*".

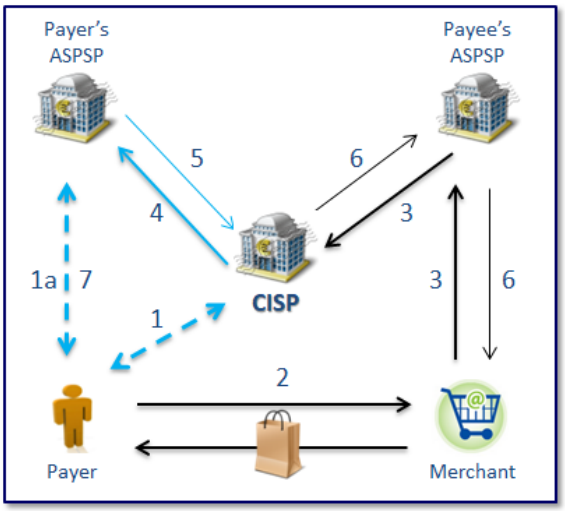
As stated in paragraph 23(d) of the EBA Opinion on the use of eIDAS certificates, a CBPII would need to be authorised for the payment services under point (5) of Annex I to PSD2 ("the issuing of payment instruments and/or acquiring of payment transactions"), but, depending on the activities it carries out, its license does not necessarily need to cover the payment services under points (3) and (4) of Annex I to PSD2.

Recitals 67 and 68 describe the use of a card or card-based payment instrument issued by a licensed PSP other than the customer's ASPSP which allows the card-based payment instrument issuer to seek confirmation from the ASPSP 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 explicit consent. The PSU needs to provide a prior consent to the ASPSPs for the ASPSP to respond to requests from a specific CBPII. If the PSU has not given such consent to the ASPSP, in accordance with Article 65(1) PSD2, the ASPSP will not be able to provide the confirmation of funds to that CBPII.PSUs must inform their ASPSPs accordingly when consent has been given, and ideally amended or 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 (retail premises use case)



1. **The payer signs an agreement with another PSP/CISP** that offers the alternative payment card and issues the new card with specific credentials (e.g. PIN code = strong authentication). (1a) The Payer gives consent to his ASPSP, identifying the PSP/CISP to whpm, if addressed, the ASPSP 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 ASPSP where the payer's account is;
5. **The Payer's ASPSP 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 ASPSP 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.

Figure 8 – PSD2 description of CISP

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 (recital 68)
- Payment transactions initiated through card-based payment instruments on which electronic money is stored are excluded.

It should be noted that it is only blue 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 (a retail premises use case) it is assumed that the card issuer would be issuing cards under a general purpose four party scheme.
According to the example in figure 6, Article 65 could be utilised by issuers with the following business models and product setups, such as:

- Issuers of general purpose cards in four party schemes.
- Issuers of cards under three-party schemes

Afterwards, to settle the transaction the PSP pays the amount to the merchant's ASPSP upon request (payment card scheme usually debits the card issuer's account). This part is directed by the card scheme rules, and is not governed by Article 65.
In general and as reported on recital 68 of PSD2 "*the use of a card or card-based payment instrument for making a payment often triggers* ***the generation of a message confirming availability of funds and two resulting payment transactions****. The first transaction takes place between the issuer and the merchant's ASPSP, while the second, usually a direct debit, takes place between the payer's ASPSP and the issuer."* Therefore a clear distinction needs to be made between the confirmation process and the handling of any subsequent settlement transaction. Settlement i.e. the debiting of the PSU's account with its ASPSP 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. In fact, recital 68 continues stating that "*Both transactions should be treated in the same way as any other equivalent transactions.* ***PSP issuing card-based payment instruments should enjoy the same rights and should be subject to the same obligations under this Directive****, regardless of whether or not they are the ASPSP of the payer,* ***in particular in terms of responsibility (e.g. authentication) and liability vis-à-vis the different actors in the payment chain***."
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, however the conclusion is the same – i.e. there is no need for a agreement between the CISP and the ASPSP (although all categories of TPPs and ASPSPs are always free to negotiate agreements if they so wish) for the performance of the CISP service to the PSU.

C. 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*".

Guidance

Articles 66 and 67 require ASPSPs to provide facilities to communicate securely with authorised Payment Initiation Service Providers (PISPs) and registered Account Servicing Payment Service Provider (AISPs) and allow them to provide services to all payment accounts that are accessible online (through the internet or via a mobile application downloaded onto the PSU's mobile device). 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 "*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/detection. The ASPSP has the responsibility to protect its customers' account information. The provisions of Article 66 (3)(b) and 67 (2)(b) have to be 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 ASPSPs and the TPP.

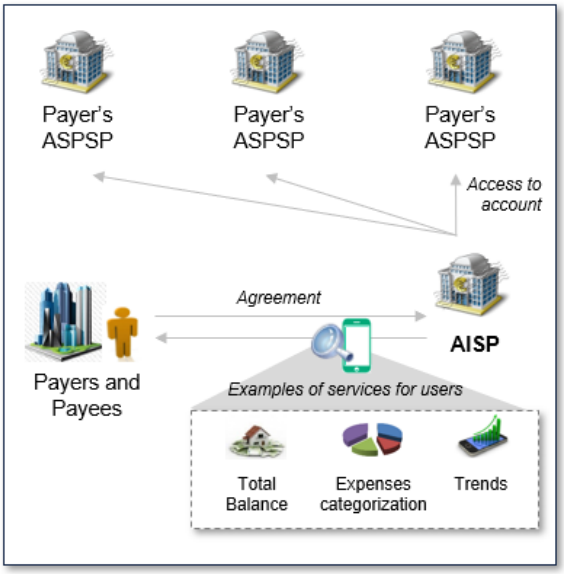
Article 69 (2) states, just as in PSD1, that the PSU shall take all reasonable steps to keep its personal security credentials safe. Whilst this provision remains in PSD2, the text does not prohibit the re-use of the PSU's personalised security credentials by PISPs and AISPs. Recital 69 provides context: "*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*".

The possibility of usage of PSU' personalised security credentials is also referred to in the RTS subject to security requirements as set out in Article 30.

Concerning the identification of TPPs towards ASPSPs when accessing payment accounts, Article 34 of the RTS on SCA & CSC and the EBA Opinion on the use of eIDAS certificates under the RTS on SCA & CSC specifies that for the purposes of identification, PSPs shall rely on qualified certificates for electronic seals or for website authentication

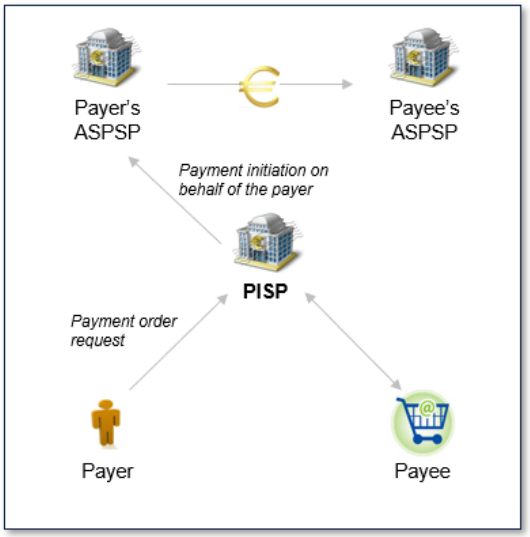
All processes must be auditable and audited by independent security experts.

Aggregation services through an Account Information Service Provider
Operating model and main features (app mobile use case)



1. The **payer signs an agreement with an AISP** that offers consolidated information (e.g. via an App) on one or more payment accounts held by the payer with one or more PSPs.
2. The **payer gives its explicit consent to the AISP** for the provision of information services.
3. For each communication session, the **AISP identifies itself towards the ASPSP(s) of the payer,** accesses to the payer's online payment account(s) by ensuring that the personalized security credentials of the payer are transmitted through safe and efficient channels.
4. The **AISP only accesses the information from designated payment account(s) and associated payment transactions**, without requesting sensitive payment data linked to those payment account(s)

Payment transactions through a Payment Initiation Service Provider Operating model and main features (e-commerce use case)



1. The **payee signs an agreement with a PISP** that offers payment initiation services on its website.
2. The **payer gives its explicit consent to the PISP**, other than its ASPSP, for the execution of the payment order.
3. Every time a payment is initiated, the **PISP identifies itself towards the ASPSP of the payer**, accesses the payer's online payment account by ensuring that the personalized security credentials of the payer are transmitted through safe and efficient channels.
4. Once the account has been accessed, the **PISP initiates a payment** (for example a SCT) to be executed from the account held by the payer at its ASPSP in favour of the payee's ASPSP.
5. The **PISP does not hold at any time the payer's funds** and does not store any sensitive payment data of the payer.

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 ASPSP 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

Article 68 makes it clear that ASPSPs can block a transaction in line with Article 68(5). In addition, the ASPSP may deny an AISP or PISP access to a payment account "*for objectively justified and duly evidenced reasons*". If the PISP cannot be identified for any reason, a process may be followed:

- In the case of electronic certificate problem, the PISP or AISP has to refer to the certificate authority for renewing/obtaining a valid certificate
- In the case of incorrect or incomplete information in the national register, the PISP or AISP has to refer to the CA for completion or updating the information
- In the case of incorrect or incomplete personal security credentials (PSC), the PISP or AISP has to refer to the PSU for completion or updating the PSC
- In the case of denied access for suspected or actual PISP or AISP fraudulent activities, the ASPSP shall inform the payer and the competent authority.

However, the possibility for an ASPSP to deny access if it cannot identify the TPP does not fully apply during the 'transition period'. In its opinion on transition from PSD1 to PSD2, EBA clarified that "*in accordance with Article 115(2), (4) and (6) PSD2 AISPs and PISPs may access customer account information without being blocked (unless there are reasonably justified and duly evidenced reasons for doing so) using existing methods, for instance 'web scraping' or 'screen scraping' (where the PSP logs in to an account as if it were the user) unless national law prevented such access before PSD2 came into force on 12 January 2016*".

In the event that the ASPSP denies a PISP or AISP access, the ASPSP, in accordance with article 68(6), has to inform the competent authority about the incident.

D. ASPSP 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."*

Pursuant to Article 61 PSD2, the PSP and the PSU may agree that Article 72 does not apply in whole or in part.

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. If the payment initiation service provider is liable for the unauthorised payment transaction, it shall immediatelycompensate 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, including the amount of the unauthorised payment transaction. In accordance with Article 72(1), 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."

Guidance

The liability of ASPSPs has not been altered due to the intermediation of PISPs. PSD2 makes it clear that the PSU can obtain rectification from the ASPSP as "sole port of call". Thus, an ASPSP shall reimburse the PSU whenever a transaction has not been executed or has been defectively executed, even when initiated by a PISP even if the latter is at fault (Article 90 PSD2). However, the PISP must then prove, within its sphere of competence, that the transaction was authenticated, accurately recorded, and not affected by a technical breakdown. Otherwise, the PISP is obliged to refund the ASPSP since the PISP initiated the payment transaction.

When a PSU denies having authorised an executed payment transaction, Article 72.2 establishes a presumption of unauthorised payment transactions as the use of a payment instrument recorded by the PSP is not sufficient to prove either the authorisation, the fraud or the failure or gross negligence of the payment service payer[22].

Therefore the PSP, including, where appropriate, thePISP, shall rebut the presumption by providing supporting evidence to prove that the transaction was an authorised transaction, correctly executed transaction or that there was fraud or gross negligence on part of the PSU. The PISP will handover this evidence to the ASPSP.

The PSD2 does not specify to whom the PISP will have to hand-over this proof. We assume this is to the ASPSP. However, in the absence of a contract between a PISP and an ASPSP, and in light of the fact that in the interest of consumer protection, a PSU is entitled to claim a refund from the ASPSP, it remains to be seen how the allocation of liability provisions will operate in practice. In any case, Recital 74 states that the allocation of liability should compel ASPSPs and PISPs to take responsibility of their respective parts of the transaction that are under their control.
In this case, ASPSPs should immediately refer the case to their supervisory authorities or Courts. 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. For more information on this, please refer to the EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/08).

No clarification is offered by the PSD2 on the recourse available to the ASPSP in cases where the PISP denies any wrong doing. It is therefore assumed that ASPSPs will have to refer the case(s) to the supervisory authorities or national courts in the absence of any authority being granted to the NCA.

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:*

[22] Pursuant to Article 61 PSD2, the PSP and the PSU may agree that Article 72 does not apply in whole or in part if the PSU is not a consumer.

(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."….

Pursuant to Article 61 PSD2, the PSP and the PSU may agree that Article 74 does not apply in whole or in part.

Guidance

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. Member States have the option to reduce this maximum amount depending on the circumstances listed under 74.1 last sentence.

Paragraph 2 states that where the payer's PSP does not require SCAand the payer has not acted fraudulently, the payer shall not bear any financial losses and introduces the liability shift principle in the context of the application of SCA

Specifically in relation to card-based payments, the party in the payment chain, which does not supportSCA, bears the financial loss in case of unauthorised payment transactions. In the case of card-based payments, this means that if the acquirer invoked the benefit of one of the exemptions to SCA set out in the RTS and sent the transaction to the issuer without a request for SCA (and assuming of course that the issuer, who has the last say, allows that transaction to go through), the acquirer will be liable in case that transaction happens to be fraudulent. Conversely, if an acquirer supported SCA by requesting the issuer to perform the SCA, the issuer will be liable for the fraud on that transactions irrespective of whether the issuer actually stepped up to request the cardholder to perform SCA or not, unless the payer has acted fraudulently.

Article reference

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

Article reference

"Payment transactions where the transaction amount is not known in advance

1. Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact amount is not known at the moment when the payer gives consent to execute the payment transaction, the payer's payment service provider may block funds on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked.

2. The payer's payment service provider shall release the funds blocked on the payer's payment account under paragraph 1 without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order."

Guidance

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 by card issuers.

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 may be placed on hold, and the money may not be debited to the card holder's account at this point, but held until final payment is processed. Whether the amount is blocked or not depends on the agreement between issuers and cardholders. This, for example, may be the case when filling up with petrol at an unmanned gas station, in car rental contracts or when checking into a hotel. Article 75(1) states that the issuer can only block an amount on the card if the cardholder has given his/her consent to the exact amount that can be blocked. Since it is the payee that has to inform the payer of the amount that he wishes to block on the card, the payer's ASPSP can only rely on the consent given by the customer to execute the transaction and therefore better specify customer's rights within the contract.

In particular, the following could be considered in line with Article 75(1):

- If the amount to be blocked is displayed on the terminal screen (it is up to the terminal provider to provide for this) and the consumer types his/her PIN to consent to the blocked amount
- If the amount to be blocked on the card is communicated by the merchant to the cardholder in the form of a POS receipt (both physical and virtual POS) and the customer signs it/enter PIN to give his/her consent to the amount to be blocked.

The practical reality is that the issuer, in most cases, will not have complete certainty that the amount was communicated by the payee to the payer (e.g. the issuer will not know for sure that the merchant operating a petrol station has placed a stick on the pump informing the

cardholder of how much will be blocked on the card). The issuer is reliant on the merchant communication –.

Pursuant to Article 75(2), the card issuer must release the blocked amount without undue delay after receipt of the exact amount and immediately after receipt of the payment order. As mentioned, it should be noted that the issuer is dependent on the merchant to advise the exact amount. The issuer cannot act without merchant co-operation. However, the latest the block will be released is when the issuer receives the payment order.

IX. STRONG CUSTOMER AUTHENTICATION

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;*"

Guidance

The EBA has given non-exhaustive lists of compliant SCA factors in its Opinion on the elements of strong customer authentication under PSD2, dated 21 June 2019.

- Possible inherence elements include fingerprint scanning, voice recognition, vein recognition, hand and face geometry, retina and iris scanning, keystroke dynamics, heart rate or other body movement pattern identifying that the PSU is the PSU, and the angle at which the device is held. Importantly, the information transmitted using the 3DS communication protocol is not accepted as inherence factor.
- Possible possession elements include possession of a device evidenced by a One Time Password (OTP) or a signature generated by the device, card reader, etc. Card details printed on the card do not constitute a valid possession element.
- Possible knowledge elements include a password, PIN, knowledge-based challenge questions, passphrase and memorised swiping path. Card details printed on the card do not constitute a valid knowledge element.

Article Reference

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 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

It results from the above that SCA is required in these three scenarios:

1. **The payer accesses his/her payment account online**, e.g. the payer accesses his/her accounts via his/her e-banking platform either from a computer/browser or via a banking app on his /her mobile (smartphone, tablet or others).

2. **The payer initiates an electronic payment**, whether in a brick-and-mortar shop or makes an ATM withdrawal, or "*remote*", e.g. online from his/her browser on his/her computer or his/her mobile phone, or in an app on his/her mobile phone. When the payer is initiating a "*remote*" transaction, the SCA needs to include "*elements which dynamically link the transaction to a specific amount and a specific payee*" – for example a One Time Password (OTP) sent via SMS (Short Messaging System) (if that is the SCA method applied by the payer's PSP) stating that the payer is trying to buy from merchant XYZ for an amount of e.g. 100 EUR. In a cards context, the authentication code can include cryptograms which represent the digital signature of the transaction. Further requirements about this "dynamic link" are specified in Article 5 of the RTS on SCA and CSC.

A remote payment is made when the PSU is not physically present at the point of sale or when, at the point of sale, the PSU does not use the POS but a remote payment solution: 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 NFC payments use the POS terminal when initiating a payment. This was confirmed by the EBA in the feedback table included in the final draft RTS (dated 23 February 2017). In this feedback table, the EBA responded to a comment (question 76) in relation to contactless payments with mobile devices and confirmed that contactless payments executed through mobile devices are to be treated as other contactless payments.

MOTO transactions (Mail Order/ telephone Order) are not considered as electronic payment transactions and therefore not subject to SCA requirements – see recital 95 of PSD2: "*There does **not seem to be a need to guarantee the same level of protection** to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders*

or telephone orders". In addition, EBA confirmed this view in the Final draft of the RTS (dated 23 February 2017), in comment 46 on page 73 by stating that "*mail and telephone orders are out of the scope of the principle of SCA under PSD2 and therefore not subject to the RTS requirements*". The EBA further confirmed this view in the final Guidelines on fraud reporting under PSD2 (dated 18 July 2018), stating in the feedback table that MOTO transactions were equivalent to "Paper-based transactions" and thus not to be considered electronic payment transactions (see responses to questions 58 and 202 and 4058). PSD2 nor the RTS define mail order or telephone orders. Traditionally, MOTO transactions are defined as those were a cardholder shares his/her card details with a merchant, so a card transaction can be initiated manually. However, there are also situations in which payers interact with their PSP through paper-based, mail or telephone orders. Accordingly, the clarification in relation to paper-based, mail and telephone orders should also apply to situations in which the payer is interacting directly with his/her PSP (e.g. phone banking) which should not be considered subject to SCA mandate since they are not initiated electronically. That said, considering that the "*security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce*", these transactions, even if not falling under the RTS on SCA & CSC, should be anyway performed ensuring that general PSP's security requirements, other than SCA rules, are applied in order to guarantee the customer protection.

3. **The payer "*carries out any action through a remote channel which may imply a risk of payment fraud or other abuses*"** (Article 97(1)(c)). In rationale 13 of the final report of the RTS on SCA &CSC (dated 23 February 2017), the EBA clarified that "*In relation to payment instruments, and as stated in the CP, the EBA understands that Article 97(1)(b) applies to electronic payments initiated by the payer, or by the payer through the payee such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only*". Payments initiated by the payee include direct debits, which are therefore not subject to the SCA requirements. However, in case the payer "*carries out any action through a remote channel which may imply a risk of payment fraud or other abuses*" (Article 97(1)(c)), an SCA is required. The EBA stated in the above mentioned recital 13 that "*an exception is a transaction where the payer's consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP*". In this case, the electronic direct debit mandates will be subject to the provisions of the SCA as they fall within the scope of Article 97(1)(c).
   The EBA endorsed this view in the Final draft of the RTS (dated 23 February 2017), in comment 272 on page 144 by stating that "*creating an e-mandate falls under SCA, according to Article 97(1)(c) PSD2, and the exemption under Article 13 RTS requires SCA when creating or amending a series of payments*". Same position is also stated in comment 278.
   It should be noted that payees can collect directly electronic mandates for direct debits, without the involvement of a PSP. The SCA requirement does not apply to a mandate collected directly by the payee, as PSD2 only applies to PSPs and not to payees.

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 […]
Pursuant to Article 98 PSD2, the EBA had to develop draft RTS, to be ultimately adopted by the EC. The full text of Article 98 is not replicated here.

Guidance

The final RTS were adopted by the EC on 27 November 2017 and published in the OJ on 13 March 2018[23]. They become applicable starting from 14 September 2019; this means that the SCA requirements of PSD2 will also become applicable on that date. However, in order to be able to benefit from the exemption from a fallback ASPSP that intend to provide a dedicated interface need to make the documentation on that interface (Article 31(3) third subparagraph of the RTS), as well as the testing facility (Article 31(5) of the RTS), available no less than 6 months before that, i.e. by 14 March 2019 at the latest. The Guidelines on the conditions to be met to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) published by the EBA provide further detail on the conditions to be met by ASPSPs wishing to benefit from an exemption. The Guidelines are covered in Chapter X.

In addition to the RTS, the EBA published on 13 June 2018 an Opinion to seek further clarity in a number of areas in the context of the implementation of the RTS on SCA and CSC (EBA-Op-2018-04[24]).

In particular, the RTS contain rules on SCA and CSC as well as a series of exemptions/exceptions that PSPs (i.e. the payer's PSP and the payee's PSP) may invoke in order not to perform SCA on a given action. According to the scenarios mentioned under article 97, main rules are as follows:

1. **Category: user accessing his/her payment account online**

As regards the first category of actions that require SCA (i.e. the user accessing his/her payment account online), in principle SCA is required pursuant to Article 97(1)(a), except if the user is merely accessing the balance of the account and/or the transation history for the last 90 days (Article 10 of the RTS). However, as an exception to the exception, SCA is required if (1) the user is accessing the above information for the first time or (2) the user did not access with SCA that above information for more than 90 days.

2. **Category: Payer initiating an electronic payment**

As regards the second category of actions that require SCA (i.e. the payer initiating an electronic payment transaction), the application of SCA to different types of payments is defined as follows:

[23] COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ 13 March 2018, L 69/23.
[24] https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

- Direct debits are generally considered to be initiated by the payee (as opposed to the payer), and therefore not subject to the SCA requirements (and there is therefore no requirement to try and find an exemption in the RTS).

- Credit transfers are generally considered to be initiated by the payer, and therefore subject to the principle of SCA. Credit transfers include e-money transfers.

- Card payments are generally considered as being "*initiated by the payer through the payee*" and therefore in principle subject to the SCA requirements (ie PSPs may look for an exemption in the RTS where appropriate). However, so-called Merchant Initiated Transactions (MIT) have been confirmed by the EBA to be out of scope of SCA requirements. Response to Question 4031 in the EBA Q&A tool provides that *"where the payer has given a mandate authorising the payee to initiate a transaction or a series of transactions through a particular payment instrument that is issued to be used by the payer to initiate the transactions, and where the mandate is based on an agreement between the payer and that payee for the provision of products or services, the transactions initiated thereafter by the payee on the basis of such a mandate can be qualified as payee initiated transactions, provided that those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee".*

In relation to payments initiated by the payer (i.e. SCTs and at least some types of card payments), the RTS provides for exemptions that PSPs (i.e. in relation to cards, acquirers and/or issuers) can invoke in order to avoid the need for an SCA on a given transactions. In a nutshell, those exemptions are the following:

- Transport fares and parking fees paid at unattended terminals (i.e. non-remote, including in a face-to-face context) may be exempted from SCA (article 12 RTS).

- Trusted beneficiaires or "*white-listing*" (Article 13 RTS). Payments to white-listed beneficiaries do not require SCA (only the creation and the changes to the list of trusted beneficiaries by the payer require SCA). The white-listing exemption is available for card-based payments as well as for credit transfers[25], in relation to remote and non-remote transactions. This has been confirmed by the EBA in the Single Rulebook Q&A tool, that this exemption is applicable to both, face to face and remote payments[26].

- Recurring payments (article 14 RTS): when a payment is initiated by the payer (1) to the same payee and (2) of the same amount, SCA is only required when a payer creates, amends, or initiates the first payment. SCA would be required again if the conditions of the recurring transactions are modified (e.g. change in the amount or change in the beneficiary).

[25] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, 13 June 2018 (EBA-Op-2018-04), paragraph 45.
[26] Q&A available here: https://www.eba.europa.eu/single-rule-book-qa?p_p_id=questions_and_answers_WAR_questions_and_answersportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_questions_and_answers_WAR_questions_and_answersportlet_jspPage=%2Fhtml%2Fquestions%2Fviewquestion.jsp&_questions_and_answers_WAR_questions_and_answersportlet_viewTab=1&_questions_and_answers_WAR_questions_and_answersportlet_questionId=2265817&_questions_and_answers_WAR_questions_and_answersportlet_statusSearch=1

- Contactless and Low-value payments (articles 11 and 16 RTS). Face-to-face contactless payments below a certain transaction amount (i.e. 50 EUR) and below a cumulative number of consecutive transactions (taps) **or** EUR value (i.e. not more than 5 taps or 150 EUR without SCA) do not require SCA (i.e. no requirement for the payer to enter a PIN). The same principle applies for remote (e.g. online payments) but with different values (i.e. less than 10 EUR for the individual transaction, and not more than 5 transactions or 100 EUR cumulative without SCA). In addition, the EBA Opinion on 13 June 2018 clarified that:

    - "*the exemptions in relation to payment transactions are separate and independent from one another, and only one exemption needs to be applied for any given transaction, even if the given transaction could qualify for more than one exemption",* meaning that, for example, "*the limit of five transactions needs to be calculated not on the basis of all transactions where the exemption could have been applied but on the basis of transactions where the particular exemption was applied*". (point 41 and 42)
    - "*the cumulative limit is either the limit based on the number of transactions or the monetary amount (but not both). This means that it may be preferable for PSPs to decide at the outset which cumulative limit they use (rather than on a transaction-by-transaction basis), as it may otherwise be confusing for consumers. They should also ensure that their systems and other technical solutions used to provide a particular service cater for this possibility*" (point 43).

  Moreover, over time EBA published numerous answers in its Q&As tool in relation to those type of transactions clarifying various aspects such as the criteria for application of the limit for SCA exemption under Article 11 and 16 RTS[27] from both the issuers' and acquirers' perspectives[28].

- Secure Corporate Payment processes and protocols (article 17 RTS): this exemption allow PSP not to apply SCA when the payment is executed through a dedicated process or protocol. It requires that the payment process or protocol is only made available to payers who are not consumers and that the level of security is comparable to the standards set in PSD2 (i.e. similar to SCA). Competent Authorities in EU Member States may grant the exemption for these solutions *where the competent authorities are satisfied that those*

[27] In particular it is to be noted that EBA clarified (Q&A 2018_4036) that the calculation of the limits under Article 11 will apply separately for contactless payment transactions initiated with a physical payment card and for contactless payment transactions initiated with a digitised version of the payment card based on a payment token, even if both are linked to the same underlying payment account and (Q&A 2018_4182) that in the event that PSPs decide to apply the exemptions on a transaction-per-transaction basis, they would need to simultaneously check whether either of the limits under Article 11(b) and Article 11(c) - or Article 16(b) and Article 16(c) respectively - has been reached and apply SCA as soon as either or both limits are reached. Conversely (Q&A 2018_4225), the PSP may decide at the outset whether it will apply the cumulative monetary limit of €150 under Article 11 (€100 under Article 16), in which case the number of transactions could exceed 5, and apply it consistently for all transactions, or the limit based on the number of transactions, in which case the amount of the transactions could exceed €150 (€100 under Article 16), and apply it consistently for all transactions.

28 For instance, EBA clarified (Q&A 2018_4227) that it is not mandatory for the PSP to include in the calculation of the limits, the cross-border transactions where the payer's PSP (the issuer) is located in the EEA and the payee's PSP (the acquirer) is located outside the EEA.

processes or protocols guarantee at least equivalent levels of security" than those set in PSD2.

Transaction Risk Analysis (TRA– articles 18,19 and 20 RTS): the TRA exemption allows PSPs (of the payer or the payee), subject to various elements being tracked, not to apply SCA when they conclude that a remote transaction is low-risk. This exemption is subject to the PSP having basis points of fraud below certain levels and having implemented TRA as a real time monitoring mechanism[29]

3. **Category: PSU carring out any action through a remote channel which may imply a risk of fraud**

E-mandates (even if considered to be initiated by the payee) fall under SCA requirements as they represent actions through a remote channel which may imply a risk of payment fraud or other abuses.

Further details will be published once the EBA will have provided answers to some of the questions raised via the EBA Single Rulebook Q&A portal.

The RTS (article 2) require PSPs to have transaction monitoring mechanisms in place in order to detect unauthorised or fraudulent payment transactions for the purpose of applying and exempting the procedure of SCA in accordance with article 97 of PSD2.

Concerning the application of SCA to online card transactions, in its Opinion on elements of SCA under PSD2 (dated 21 June 2019), the EBA granted on an exceptional basis and in order to avoid unintended negative consequences for some PSUs that NCAs may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time for the enforcement of SCA. In its Opinion on the deadline and process for completing the migration to SCA for e-commerce card-based payment transactions (dated 16 October 2019), the EBA clarified that the deadline to migrate to SCA is 31 December 2020. The Opinion also prescribed the expected actions to be taken during the migration period.

X. EBA GUIDELINES ON THE EXEMPTION FROM THE FALL BACK MECHANISM UNDER THE RTS ON SCA & CSC

On 4 December 2018 the EBA published the final Guidelines on the conditions to be met to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) that detail the conditions to be fulfilled by ASPSPs in order to benefit from an exemption from the fall back mechanism for those ASPSPs that opt to provide access to PISPs, AISPs and CBPIIs via a dedicated interface.

[29] Single Rulebook Q&A EBA: http://www.eba.europa.eu/single-rule-book-qa?p_p_id=questions_and_answers_WAR_questions_and_answersportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_questions_and_answers_WAR_questions_and_answersportlet_jspPage=%2Fhtml%2Fquestions%2Fviewquestion.jsp&_questions_and_answers_WAR_questions_and_answersportlet_viewTab=1&_questions_and_answers_WAR_questions_and_answersportlet_questionId=2276716&_questions_and_answers_WAR_questions_and_answersportlet_statusSearch=1

Given that Guidelines are subject to NCA's adoption and may present some differences among countries , in this section we highlight the main features of these guidelines by assuming they will be entirely applied in a homogeneous way across PSPs and hence leaving each PSP to precisely check and implement the requirements according to specific local instructions.

See the table below for further details.

GL reference	GL Description	Reporting to NCA	Notes from rationales (R#)/table comments (TC#)
Article 33.6.a - complies with all the obligations for dedicated interfaces as set out in Art. 32			
GL1 ***Fulfilment of the conditions set out in Article 33(6) of Delegated Regulation (EU) 2018/389***	ASPSPs should provide their NCA with such information as is necessary to satisfy that the requirements in GLs 2 to 8 are met.	ASPSP to apply for exemption with regard to dedicated interfaces only	***(TC160)*** Any ASPSP that has not obtained an exemption is required to build the fall back mechanism by 14 September 2019
GL2 ***Service level, availability and performance***	ASPSPs should define key performance indicators (KPIs) and service level targets, including for problem resolution, out of hours support, monitoring, contingency plans and maintenance for the dedicated interface that are as stringent as the KPIs used for the interface(s) made available to its own payment service users (PSUs). Details of service level, availability and performance are described in GL 2 to 4.		***(R10)*** if the ASPSP offers more than one customer channel (e.g. online banking and mobile banking interfaces), the dedicated interface should match the best of the KPIs and service level targets across all offered ASPSP's customer-facing interfaces. ***(R12)*** The GLs only define a minimum set of KPIs for both availability and performance.
GL3.1 ***Publication of statistics***	ASPSPs should provide their NCA with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in Guidelines 2.2 and 2.3, and of each of the interfaces made available to its own PSUs for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication.	ASPSP to provide plan for publication	***(TC42)*** where an ASPSP applies for an exemption ahead of the date of application of the RTS, it should submit a plan for the publication of data to its NCA starting with the date of application of the RTS, i.e. from 14 September 2019, given that the obligation to publish data starts only when the RTS apply, namely on 14 September 2019. The EBA agrees that it may be more meaningful to define the first quarter from 14 September 2019 until the end of the year (rather than until 14 December 2019).
GL3.2 ***Publication of statistics***	The publication referred to in GL 3.1 should enable PISPs, AISPs, CBPIIs and PSUs to compare the availability and performance of the dedicated interface with the availability and performance of each of the interfaces made available by the ASPSP to its PSUs for directly accessing their payment accounts online on a daily basis.		

GL reference	GL Description	Reporting to NCA	Notes from rationales (R#)/table comments (TC#)
GL4 ***Stress testing***	ASPSPs should have in place processes for stress testing of the dedicated interface. (GL4.1) ASPSPs should provide their NCA with a summary of the results of the stress tests, including the assumptions used as a basis for stress testing each of the elements in GL 4.2 and how any issues identified have been addressed. (GL4.3)	ASPSP to provide stress tests results	***(TC65)*** ASPSP should demonstrate that it has conducted the stress testing at least once before applying for the exemption. However, the obligations applicable to dedicated interfaces under the RTS will have to be complied with at all times, which means that stress testing is an ongoing obligation, although it is not within the scope of these GL. For the purpose of the application for an exemption ahead of the 14 September 2019 deadline, ASPSPs should conduct the stress testing in the context of their production environment (i.e. simulating settlement of payments).
GL5 ***Obstacles***	ASPSPs should provide their NCA with: a) a summary of method(s) of carrying out the authentication procedure(s) of the PSUs that are supported by the dedicated interface (i.e. redirection, decoupled, embedded or a combination thereof), and b) an explanation and evidence of why these methods do not constitute an obstacle for the provision of payment initiation or account information services	ASPSP to provide summary of method(s) and explanation/ evidence it(they) is(are) not an obstacle	***(R25)*** The EBA reiterates the view expressed in the EBA Opinion from June 2018 that redirection is not, in itself, an obstacle to AIS or PIS, but that it 'may' be so, if the ASPSP implements it in a manner that creates delay or friction in the customer experience that would dissuade PSUs from using the services of AISPs or PISPs. ***(R26)*** Evidence requested in point b) may include the results of customer testing, examples of customer experience journeys when using an AISP or PISP (for instance using screenshots).
Article 33.6.b - Designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein			
GL6 (1 to 6) ***Design and testing to the satisfaction of PSPs***	ASPSPs should, amongst others, demonstrate TPPs involvement in the design and testing of the dedicated interface (GL6.1) by submitting the feedback received from TPPs, the issues identified and a description of how these issues have been addressed as part of the testing activities (GL6.6). ASPSPs shall inform their NCA on which market initiative standard the ASPSP is implementing, including results of the conformance testing developed by the market initiative as well as any possible deviations from such standard, and if so, how they have deviated and how they meet the legal requirements (GL6.3) ASPSPs should make the technical specifications of the dedicated interface available and, at a minimum, publish a summary of the specification of the dedicated interface on their website. (GL6.4)	ASPSP to provide evidence that the dedicated interface meets the legal requirements, information on standards adherence, if any, the engagement with TPPs and a summary of testing results	***(R35)*** Non-real PSU data should be used during the testing referred to in Article 30(5) of the RTS. ***(TC108)*** For the purpose of TPPs identification during testing, ASPSP may rely on: - e-IDAS certificates - national public registers for credit institutions - national public registers of TPPs (art. 14 of PSD2) - EBA Credit Institutions Register (art. 15 of PSD2) - EBA Register of TPPs (art. 15 of PSD2) ***(TC107)*** From 14 September 2019, ASPSPs should rely on e-IDAS certificates, to identify PISPs, AISPs, CBPIIs, and credit institutions (CI) acting as TPPs. Before 14 September 2019, ASPSPs can verify the authorisation status of CI using the national public registers for CI and the EBA CI Register, accessible at:

GL reference	GL Description	Reporting to NCA	Notes from rationales (R#)/table comments (TC#)
			https://www.eba.europa.eu/risk-analysis-and-data/credit-institutions-register.
GL6.7 ***Design and testing to the satisfaction of PSPs***	NCAs may also take into account any problems reported to them by PISPs, AISPs and CBPIIs in relation to testing activities as per GL 6.5.	TPPs may provide feedback directly to NCA	
Article 33.6.c - widely used for at least 3 months by PSPs to offer AIS, PIS and CoAF			
GL7 ***Wide usage of the interface***	In order to evidence wide usage of the interface, ASPSP should provide their NCA with a description of the usage and should demonstrate that it has made all reasonable efforts to ensure wide usage. (GL7.1) The three-month period of wide usage can run concurrently with the testing phase. (GL7.3)	ASPSP to provide wide usage	***(R35)*** The condition in Article 33(6) of the RTS should be assessed in relation to the production interface, i.e. where real PSU data are used for TPPs to provide services to their customers. ***(R38)*** The RTS do not require ASPSPs to wait a certain period before launching their production interface. This means that an ASPSP does not need to wait a period of 6 months before launching the production interface. The ASPSP may choose to launch it at any time it deems appropriate after having considered the feedback from TPPs and made any relevant changes. ***(R39)*** Testing period may be longer or shorter than 6 months.
Article 33.6.d – any problem related to the dedicated interface has been resolved without undue delay			
GL8 ***Resolution of problems***	ASPSPs should provide their NCA with information on the systems or procedures in place for tracking, resolving and closing problems as well as an explanation of the problems, particularly those reported by PISPs, AISPs and CBPIIs, that have not been resolved in accordance with the service level targets set out in GL2.1.	ASPSP to provide resolution of problems	***(R17)*** ASPSPs should provide the NCA with an explanation of the problems reported by TPPs regarding the ASPSP's production interface that have not been resolved by the ASPSP
Article 33.6 – NCA shall grant the exemption after consulting EBA to ensure a consistent application of the conditions set out in the article 33.6			
GL9 ***Consultation with the EBA***	For each planned exemption, NCAs should submit an assessment form for the EBA to comment upon. (GL9.1) The Form has to be submitted both in case of positive and negative assessment by the NCA. (GL9.3) Where an ASPSP is part of a group with subsidiaries in different Member States that will use the same dedicated interface, each of the NCAs of those Member States should inform the other relevant NCAs on their assessment and of their reasoning behind it including, where relevant, the issues reported by PISPs, AISPs and CBPIIs to the NCA. (GL9.4)	Subject to NCA's instructions, amongst others (process, timing, documents, etc.), ASPSP may be asked to provide indication on the usage of the same dedicated interface by other Group entities in other Member States	***(TC154)*** As a branch does not have legal personality, an ASPSP will always have to apply for an exemption from the fall back mechanism with the NCA in the Member State where its head office is located, irrespective of whether or not the ASPSP has branches in other Member States that will use the same dedicated interface as that used by the head office. In this case, the exemption granted by the NCA of the Member State where the ASPSP's head-office is situated will also be valid in the other Member States where the ASPSP is providing payment services via branches using the same dedicated interface. By contrast, subsidiaries are separate legal entities from the ASPSP and, therefore, each subsidiary would

GL reference	GL Description	Reporting to NCA	Notes from rationales (R#)/table comments (TC#)
			need to apply for a separate exemption with its NCA in the Member State where the head-office of the subsidiary is located. In order to limit the risk of inconsistent assessments of the same dedicated interface by different NCAs, the EBA encourages NCAs to request information from ASPSPs, when applying for an exemption, on whether or not the same dedicated interface will be used by other Group entities in other Member States, and, where necessary, to consult with the other NCAs before granting, or refusing to grant, an exemption for the same dedicated interface.

XI. TRANSITIONAL PROVISION, TRANSPOSITION AND EBA/EC MANDATES

Article references

Article 106 – Obligation to inform consumers of their rights

1. By 13 January 2018, the Commission shall produce a user-friendly electronic leaflet, listing in a clear and easily comprehensible manner, the rights of consumers under this Directive and related Union law.
2. The Commission shall inform Member States, European associations of payment service providers and European consumer associations of the publication of the leaflet referred to in paragraph 1.
The Commission, EBA and the competent authorities shall each ensure that the leaflet is made available in an easily accessible manner on their respective websites.
3. Payment service providers shall ensure that the leaflet is made available in an easily accessible manner on their websites, if existing, and on paper at their branches, their agents and the entities to which their activities are outsourced.
4. Payment service providers shall not charge their clients for making available information under this Article.
5. In respect of persons with disabilities, the provisions of this Article shall be applied using appropriate alternative means, allowing the information to be made available in an accessible format.

Guidance

The Commission has made available the leaflet *"Your rights when making payments in Europe"*, together with translations into official EU languages, on its website[30]. As per paragraph 3, PSPs must make the leaflet available both on their websites and in branches.

Article 109 – Transitional provision

"1. Member States shall allow payment institutions that have taken up activities in accordance with the national law transposing Directive 2007/64/EC by 13 January 2018, to continue those activities in accordance with the requirements provided for in Directive 2007/64/EC without being required to seek authorisation in accordance with Article 5 of this Directive or to comply with the other provisions laid down or referred to in Title II of this Directive until 13 July 2018.

Member States shall require such payment institutions to submit all relevant information to the competent authorities in order to allow the latter to assess, by 13 July 2018, whether those payment institutions comply with the requirements laid down in Title II and, if not, which measures need to be taken in order to ensure compliance or whether a withdrawal of authorisation is appropriate.

Payment institutions which upon verification by the competent authorities comply with the requirements laid down in Title II shall be granted authorisation and shall be entered in the registers referred to in Articles 14 and 15. Where those payment institutions do not comply with the requirements laid down in Title II by 13 July 2018, they shall be prohibited from providing payment services in accordance with Article 37.

2. Member States may provide for payment institutions referred to in paragraph 1 of this Article to be automatically granted authorisation and entered in the 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 payment institutions concerned before the authorisation is granted.

3. This paragraph applies to natural or legal persons who benefited under Article 26 of Directive 2007/64/EC before 13 January 2018, and pursued payment services activities within the meaning of Directive 2007/64/EC.

Member States shall allow those persons to continue those activities within the Member State concerned in accordance with Directive 2007/64/EC, until 13 January 2019 without being required to seek authorisation under Article 5 of this Directive or, to obtain an exemption pursuant to Article 32 of this Directive, or to comply with the other provisions laid down or referred to in Title II of this Directive.

Any person referred to in the first subparagraph who has not, by 13 January 2019, been authorised or exempted under this Directive shall be prohibited from providing payment services in accordance with Article 37 of this Directive.

4. Member States may allow natural and legal persons benefiting from an exemption as referred to in paragraph 3 of this Article to be deemed to benefit from an exemption and automatically

[30] https://ec.europa.eu/info/files/leaflet-your-rights-payments-eu_en

entered in the registers referred to in Articles 14 and 15 where the competent authorities have evidence that the requirements laid down in Article 32 are complied with. The competent authorities shall inform the payment institutions concerned.

5. Notwithstanding paragraph 1 of this Article, payment institutions that have been granted authorisation to provide payment services as referred to in point (7) of the Annex to Directive 2007/64/EC shall retain that authorisation for the provision of those payment services which are considered to be payment services as referred to in point (3) of the Annex I to this Directive where, by 13 January 2020, the competent authorities have the evidence that the requirements laid down in point (c) of Article 7 and in Article 9 of this Directive are complied with."

Guidance

PSD2 foresees transitional provisions for PIs that are already authorised to provide services under PSD1. These PIs are allowed to continue providing payment services until- 13 July 2018 - (authorised institutions) or until 13 Jan. 2019 ("*small*" institutions that benefited from the waiver under art. 26 of PSD1). The relevant PSD2 wording reads as follows:

- "*Member States shall allow payment institutions that have taken up activities in accordance with the national law transposing [PSD1] by 13 January 2018, to continue those activities in accordance with the requirements provided for in [PSD1] without being required to seek authorisation in accordance with Article 5 of this Directive or to comply with the other provisions laid down or referred to in Title II of this Directive until 13 July 2018.*" (Article 109(1) first subparagraph)
- "*This paragraph applies to natural or legal persons who benefited under Article 26 of [PSD1] before 13 January 2018, and pursued payment services activities within the meaning of [PSD1]. Member States shall allow those persons to continue those activities within the Member State concerned in accordance with [PSD1], until 13 January 2019 without being required to seek authorisation under Article 5 of this Directive or, to obtain an exemption pursuant to Article 32 of this Directive, or to comply with the other provisions laid down or referred to in Title II of this Directive.*" (Article 109(3), first and second subparagraph).

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.
Failure to satisfy the regulator of the conditions for authorisation or a waiver would mean the firm is no longer authorised to offer payment services under PSD2, or the waiver is lost, as the case may be.

All authorised credit institutions are entitled to provide the whole range of payment services, including AIS and PIS, and to do so without any need for additional authorisation, pursuant to Articles 33 and 34 of Directive (EU) 2013/36 on capital requirements, known as "CRD IV" setting forth that financial institutions and credit institutions can provide all payment services(see Guidance on Article 15 PSD2, above).

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

As explained by the EBA in its Opinion recalled above on the transition period from PSD1 to PSD2, the full application of the PSD2 depends on the application of RTS and Guidelines across a number of provisions. During the period in which a particular EBA level 2 document is not yet legally applicable but the underlying national transpositions of PSD2 provisions are, the EBA "*advises CAs to take into account the most recent available version of the final draft requirements as an indication of what is required to comply with PSD2, and of what will be required to comply with the EBA instrument once it becomes applicable*"

The EBA has finalised all of its mandates under PSD2 and all but two RTS (RTS on Home-Host cooperation and RTS on central contact points) have been formally adopted by the European Commission.

The following table summarises and lists all the EBA mandates with the current status update. It has to be noted that while RTS will become applicable according to European regulatory deadlines which are directly mentioned in the Delegated Regulation as published in the OJEU,

Guidelines will be subject to decision by National Competent Authorities that have to declare their intention to comply whitin 2 months after the publication date of the guidelines translated into all official languages. Publication of EBA Compliance Tables for each Guideline is ongoing and progressively updated according to the information received from NCAs about their intentions to comply.

Type of document	Document Description	PSD2 article	Code	Publication date in the OJEU	Compliance Table GL (Y/N)	Note
RTS	Pass-porting notification and supervision	28	UE - 2017/2055	11 November 2017 - (L294)	-	
GL	Authorisation and registration	5 and 15.4	EBA-GL-2017-09		Y	
GL	Minimum amount of professional indemnity insurance for PSPs	5	EBA-GL-2017-08		Y	
GL	Incident reporting	96.3	EBA-GL-2017-10		Y	
GL	Fraud reporting	96.6	EBA/GL/2018/05			
GL	Procedures set up by CAs for complaints of alleged infringements	100	EBA-GL-2017-13		Y	
GL	Security measures for operational and security risks	95	EBA-GL-2017-17			
RTS	Strong customer authentication and common and secure communication	98	UE – 2018/389	13 March 2018 – (L69)	-	
RTS	ITS and RTS on the EBA register	15	EBA-RTS-2017-10 and EBA-ITS-2017-07	29 November 2018	-	
RTS	Central contact points	29	EBA-RTS-2017-09		-	
RTS	Home-host cooperation	29.6	EBA-RTS-2018-03		-	
GL	Conditions to be met for exemption from contingency measures under Article 33(6) SCA and CSC	98	EBA/GL/2018/07			

XII. INTERACTION BETWEEN PSD2 AND GDPR

On 25 May 2018, the General Data Protection Regulation (GDPR) became effective.

One of the key motives of both GDPR and PSD2 is to give data subjects (in the context of PSD2: payment service users – PSUs) increased control over their data, particularly their personal data[31]. Also, both bodies of law set standards with respect to the safe-keeping of personal data and information provision to customers; GDPR applies broad rules across all industries, while PSD2's standards are specific to payment services.

PSD2 is not a lex-specialis of GDPR but provides a specific framework limited to payments data concerning how these can be accessed. Payments data is not generally excluded from the scope of the GDPR but, where PSD2 requires that access is given to previously carefully shielded (payment account-related data), GDPR reaffirms the obligation to protect these data[32].

As a general rule, Payment Service Providers (PSPs), including ASPSPs, PISPs and AISPs, providing payment services under PSD2 need to comply with both PSD2 and GDPR[33]. A limited number of questions and issues persist however, notably where the applicable PSD2 provisions could be interpreted as regulating in a different way the same matters regulated by the GDPR (e.g. where a data subject withdraws consent under GDPR, but wants to use a Third Party Provide - TPP service regulated under PSD2).

The control mechanism of PSD2 is that the TPP is a licensed (or registered in the case of PSPs that provide AIS only) entity, and its activities are supervised by the national supervisory authority. This means that, even though ASPSPs have some responsibilities in ensuring their offered interfaces work, they do not have a duty to ascertain a TPP's compliance with GDPR, as per PSD2.

This chapter intends to provide a better understanding on some of the more pressing issues that the banking sector has identified in reconciling PSD2 and GDPR. This chapter may need to be amended as further clarity and guidance is provided from supervisory authorities.

It is also important to keep in mind, throughout this chapter, that banks are subject to multiple legal and regulatory obligations (including additional national legislation) to protect consumers and their data.

1. Each PSP is considered as a separate controller and is responsible for its own processing

Article Reference:

[31] GDPR applies only to personal data, while PSD2 applies to payment account-related data of payment service users.
[32] Please note that the duty to keep personal data safe is not a new obligation introduced under GDPR, GDPR merely unifies the EU national laws in this respect.
[33] See PSD2 consideration 89 of the explanatory notes and article 94.1.

As controllers, and in accordance with GDPR (articles 4.7, 5 and 32), ASPSPs have the responsibility to protect personal data and keep them safe. In that capacity, they have to ensure that the processing of these data by them, or on their behalf, complies with the law & regulation, including in case of data sharing with third parties.

Guidance and interpretation:

Once a TPP gains access to personal data of a PSU, the TPP assumes its own responsibilities with respect to the processing of these data as a controller. At that point, it must be assumed that subject to PSD2 both the ASPSP and the TPP are separately considered controllers in their own right, and each is responsible for its own processing (and not for the processing of the other party).

In addition, the TPP is a licensed (or registered in the case of AISP) entity, its activities are supervised by the national supervisory authority, is not selected by the ASPSPs and is a forced interlocutor for the ASPSP. As a result, even though ASPSPs have responsibilities in ensuring their offered interfaces work, they do not, as per PSD2, have a duty to ascertain a TPP's compliance with GDPR.

- Responsibility for security of data transfers to TPPs

Under GDPR, ASPSPs have obligations to ensure data transfers are secure. PSD2 and the RTS for strong customer authentication and common and secure open standards of communication set specific requirements to ensure the security of the transfer of data from ASPSP to TPP (PISPs and AISPs also have obligations to ensure secure data transfers). As such, complying with the RTS requirements in respect in particular of the 'common and secure open standards of communication' must be taken as sufficient for the ASPSP to meet GDPR requirements relating to the security of the transfer, especially as the ASPSP has a legal obligation to allow access to the data according to PSD2.

However, the RTS refer to both TPPs and ASPSPs as payment entities and thus both institutions are obliged to comply with the set-out requirements.

Complying with PSD2 and the RTS (which must be implemented as of 14 September 2019) does constitute a legal basis for the data transfer from ASPSP to PISP or AIS. Compliance with PSD2, and in particular the RTS, therefore constitutes the appropriate technical measure to secure the transfer and shall be sufficient for GDPR compliance purposes in this context.

2. Data Minimization

Article reference:

Article 5 (1)(c) of the GDPR makes it clear that the processing of personal data shall respect the principle of data minimisation: "*Personal data shall be (...) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

A similar provision is contained in Article 66 (3)(f) and (g) of the PSD2 which states that a PISP may:

- (f) "*not request from the payment service user any data other than those necessary to provide the payment initiation service*;" and
- (g) "*not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer*".

Other restrictions are included in Article 65(3) of the PSD2 which makes it clear that the information transmitted to the third party should consist in a simple 'yes' or 'no' answer to the question if there are sufficient funds available — not in for example a statement of the account balance and in Article 67(2)(f) which requires that an AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. Furthermore, Article 67(2)(d) mentions that AISP shall "*access only the information from designated payment accounts and associated payment transactions*".

Guidance and interpretation:

Both PSD2 and GDPR require the minimization of processing of personal data. PSD2 not only incorporates data minimization requirements, but also explicitly refers to this requirement under EU privacy law in the explanatory notes (*e.g.* Recital 29), and in article 94(2). GDPR prescribes that only those personal data that are necessary for the defined purpose of a processing operation may be processed. Any personal data that are no longer required for this purpose or any legitimate secondary purpose must be deleted.

For payment initiation services, the data minimization requirements in the GDPR align with those set out in PSD2: **only those data that are necessary for the initiation of a payment transaction may be requested and accessed**. This rule must be observed, especially when requesting access as described in the RTS on strong customer authentication (article 33(4) and 33(5)) and the European Banking Authority's Opinion of 13 June 2018 (paragraph 26).

For account information services, PSD2 provides that an AISP shall *"not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules".* **Dedicated interfaces designed to allow TPPs to request specific data sets according to PSD2 provisions will endorse data minimization requirements.**

Furthermore, it should be noted that other legal obligations than the one prescribed by the PSD2 might apply. This is for instance the example of obligations with regard to data content in payment orders[34].

[34] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

3. Information rights

Article reference:

Articles 13 and 14 of the GDPR provide that data subjects have the right to receive certain information from controllers. Under Article 13, data subjects have the right to be provided with certain information describing their relationship with a controller. Additionally, Article 14 provides that the controller must identify the source of the data if it was obtained or collected from a third-party.

PSD2 establishes harmonized rules to ensure that TPPs provide necessary, adequate and comprehensible information to PSUs. Article 44 and 45 provide that, in the interest of efficiency, the required information should be reasonably proportionate to the needs of the user and should be provided in a standard format.

Guidance and interpretation:

The primary responsibility for information provision to a user in the context of AIS and PIS rests on the TPP providing these services. **It lies on the TPP to inform the customer about its products, services, and data processing** as required by the GDPR (articles 13 and 14).

From an ASPSP point of view, the *transfer* of data from the ASPSP to the TPP could *arguably* be considered 'further processing' by the ASPSP[35]. However, the PSU should already have received information about the data transfer when granting its consent to the TPP. It thus follows that, under GDPR Article 13(4)[36], the ASPSP would be exempted from explaining this a second time. ASPSPs could however specify in their privacy notices that a possible transfer to an AIS or PISP (due to a legal obligation) may occur.

4. Legitimate ground

Article Reference:

Article 94(2) PSD2 requires that PSPs obtain the "explicit consent" of a PSU before accessing, processing and retaining personal data necessary for the provision of their payment services.

Article 5(1)(b) of the GDPR requires that for all processing of personal data, which includes the sharing of data, a specific purpose should be determined, and the processing must be based on one of the legitimate grounds listed in Article 6 of the GDPR (consent, necessary for the performance of a contract, necessary for compliance with a legal obligation, necessary in order to protect the vital interests of the data subjects, public interest or necessary for the purposes of the legitimate interests pursued by the controller).

[35] Under GDPR, 'processing' is defined as "*any operation or set of operations which is performed on personal data*". The transfer of the data from the ASPSP to the TPP could thus fall under this definition.
[36] Article 13(4) of the GDPR exempts the ASPSP to provide this information to the data subjects "*where and insofar as the data subject already has the information*".

As the European Data Protection Board (EDPB)[37] specified in its Guidelines on Consent (revised and adopted on 10 April 2018): "*Consent remains one of the six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing*" (page 3, second paragraph).

Guidance and interpretation:

Consent under PSD2 and consent under GDPR are two different types of consent, with different objects and with different validity requirements. The GDPR consent refers to the processing of personal data in general and is only one of the ground available. The consent referred to in PSD2 is related to payment services.

The specific reference to consent in relation to payment services should not be interpreted to imply that PSD2 prescribes "consent of the data subject" as the legitimate ground for this type of processing, with the exclusion of the other legitimate grounds. For example, an institution may then still be allowed to process personal data, based on other grounds provided by the GDPR, *e.g.* the necessity of data access for the fulfillment of a contract or legal obligations.

This is confirmed by the EDPB in a letter it sent to MEP Sophie in't Veld (dated 5 July 2018)[38] in which it says the following:

> The EDPB is of the view that the "explicit consent" referred to in Article 94 (2) of PSD2 is a contractual consent. Payment services are always provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of PSD2, "*This*
>
> (...)
>
> subject. The concept of explicit consent under Article 94(2) of PSD2 is therefore an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR.

Fairly, from the ASPSPs point of view, arises a legal obligation to share the data with the TPP according to the terms of PSD2. This provides a legitimate basis for the processing, other than consent.

Indeed, it stems from PSD2 (Article 66(1) and (4) and Article 67(1)) that ASPSPs have a legal obligation to provide all relevant data to the AISP or PISP.

[37] The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. It is composed of representatives of the national data protection authorities and the European Data Protection Supervisor (EDPS). The EDPB is established by the GDPR.
[38] EDPB, *Letter regarding the PSD2 Directive EDPB* (**EDPB-84-2018**), dated July 5th, 2018.

The legal obligation to grant access to the payment data and to transfer to TPP payment data also provides a legitimate basis for processing personal data under GDPR (under GDPR Article 6(1)(c) and 6(3)(a)).

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)	**CANCELLED**	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)	**Mandatory**	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. I. 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)	**CANCELLED**	Transitional provision for natural or legal persons eligible for the waiver under article 26.

Figure 9 – Member States exemptions and derogations

This guidance was drafted by the PSD2 Expert Group:

Ruth Wandhöfer	Chair
Wulf Hartmann	Bundesverband deutscher Banken - Germany
Gijs Boudewijn	Dutch Payments Association and Chair of the EBF Payment Systems Committee
Marc van de Maarel	Dutch Payments Association – The Netherlands
Rita Camporeale	Associazione Bancaria Italiana (ABI) - Italy
Pilar Clavería	Spanish Banking Association (AEB) - Spain
Cicely Dudley	UK Finance
David Song	UK Finance
Anne Ballerini	Fédération Bancaire Française (FBF) - France
Inkeri Tolvanen	Finance Finland
Teija Kaarlela	Finance Finland
Lars Rutberg	Svenska Bankföreningen - Sweden
Saar Carré	Febelfin– Belgium
Loiuse Laidi	BPCE
Jean-Yves Jacquelin	Erste Bank
Thea Melsbø Aarseth	Bits
Xavier Albalate Aceña	Caixa Bank
Diederik Bruggink	ESBG
Marieke Van Berkel	EACB
Pablo Lahoz Marco	EACB

With special expert contribution by:

Bird & Bird

Scott McInnes	Bird&Bird
Adrian Calvo	Bird&Bird