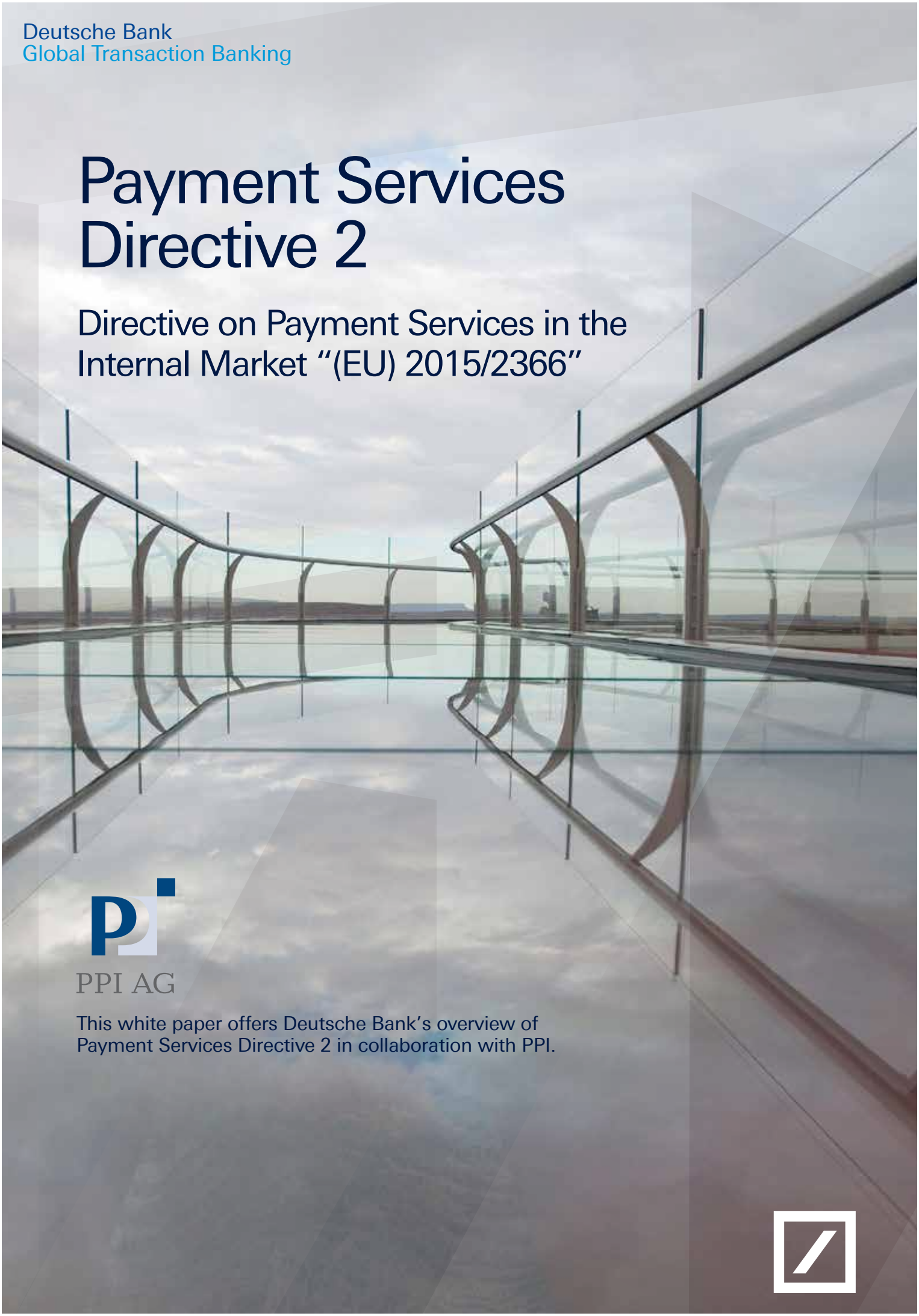
Deutsche Bank
Global Transaction Banking

Payment Services Directive 2

Directive on Payment Services in the Internal Market "(EU) 2015/2366"



PPI AG

This white paper offers Deutsche Bank's overview of Payment Services Directive 2 in collaboration with PPI.

Dear Readers,

Deutsche Bank and PPI have collaborated to give you an overview in this white paper of the key provisions of Payment Services Directive 2 (PSD2)[1]. The paper's primary focus is on changes made by PSD2 to the First Payment Services Directive (PSD1)[2] that directly affect your operations. These include changes affecting the processing of transactions in consequence of PSD2's scope extension, changes to customer authentication requirements, and changes in consequence of third party providers being licensed to offer services in the EU payments market.

We have endeavoured to give you a succinct summary of the most important provisions, together with a clear idea of where, and how, PSD2 will affect your operations. For more detailed information and advice, we refer you to your relationship manager or sales contact at Deutsche Bank, and to the full text of the Directive itself.

Shahrokh Moinian,
Global Head of Cash Management Corporates, Deutsche Bank

Dr. Hubertus von Poser,
Partner, PPI

Shahrokh Moinian

Dr. Hubertus von Poser

[1]Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

[2]Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007.

Table of contents

List of Abbreviations

2FA	Two-factor authentication
AISP	Account Information Service Provider
Art.	Article
ASPSP	Account Servicing Payment Service Provider
CISP	Card-based Payment Instrument Issuer
CVC/CVV	Card Verification Code/Card Verification Value
DP	Discussion Paper
EBA	European Banking Authority
EBF	European Banking Federation
EEA	European Economic Area
ITS	Implementing Technical Standards (to be issued by the EBA)
PISP	Payment Initiation Service Provider
PSC	Personal Security Credentials
PSD1	Payment Services Directive 2007/64/EC
PSD2	Revised Payment Services Directive (EU) 2015/2366
PSU	Payment Service User
PSP	Payment Service Provider
RTS	Regulatory Technical Standards (to be issued by the EBA)
TPP	Third Party Provider

1 Introduction to PSD2

Adopted by the European Parliament on October 8, 2015, and by the European Union (EU) Council of Ministers on November 16, 2015, the "Directive on Payment Services in the Internal Market" (PSD2) updates the first EU Payment Services Directive published in 2007 (PSD1), which laid the legal foundation for the creation of an EU-wide single market for payments. PSD2 came into force on January 13, 2016, and is applicable from January 13, 2018, by which time member states must have adopted and published the measures necessary to implement it into their national laws[3].

Card, internet and mobile payments, were regarded as fragmented along national borders

The clock is therefore ticking on the implementation of an EU Directive of profound importance to Europe's financial institutions, their corporate customers and to consumers. PSD1's aim was to establish a modern and comprehensive set of rules applicable to all payment services in the EU and the wider European Economic Area (EEA). As well as fostering competition by opening up the payment markets to new entrants, its intention was to make cross-border payments as easy, efficient and secure as payments within an EU member state. It also provided the necessary legal platform for the Single Euro Payments Area (SEPA).

PSD2 goes further by:

- extending the scope of its predecessor Directive to payments in all currencies, and to payments where only one provider is located in the EU/European Economic Area (EEA),[4]
- introducing strict security requirements for the initiation and processing of electronic payments, and for the protection of consumers' financial data,
- introducing so-called Third Party Providers (TPPs) that are permitted to provide certain types of services connected to payments.

While the first of these changes will be challenging - global financial institutions (not just those in the EU or EEA) will have to adapt their processes and IT systems for international payments - it is the third change that will have the greatest impact on the payments market. Customers will be allowed to initiate payments at their financial institution via authorised TPPs, to whom financial institutions will be obliged to open their account interfaces. This represents a major change for operators within the payments industry, and one needing to be properly understood.

[3]Payment institutions engaged in activities authorised under national law transposing PSD1 by January 13, 2018 may continue these activities and need not seek authorisation under PSD2 until July 13, 2018 (Title VI - Transitional provisions, transposition etc. (Art. 107-117)).

[4]Certain provisions of PSD2 are excluded from the extension of scope to all currencies and to payments where only one PSP involved in the transaction is located in the EU/EEA, including the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Given this, in the pages ahead Deutsche Bank explains the complexities of the Directive and offers views on its implementation. Our aim is to highlight the main regulatory changes – as well as how they may impact the payments industry. We also provide guidance on smooth and efficient adaptation to PSD2. This paper shall under no circumstances be understood to offer legal advice.

Background to PSD2

In introducing PSD2, the EU institutions expressly recognise that the retail payments market has experienced significant technical innovation since the introduction of PSD1. There has been rapid growth in the number of electronic and mobile payment channels as well as new types of providers and services. As is customary for EU law, PSD1 provided for a future analysis of its own impact, and a review of how well it was working – both with regard to its scope, and how well it was keeping pace with market developments and competition issues, including barriers to entry. Once undertaken, the review revealed there had indeed been significant developments giving rise to regulatory challenges.

On the one hand, since PSD1 many innovative payment products and services had been introduced – in particular in card, internet and mobile payments – many falling entirely or in large part outside the scope of PSD1. In particular, the EU found the elements excluded from PSD1's scope, such as certain payment-related activities, had proved to be too ambiguous or too general given market developments.

On the other hand, the separate development of significant areas of the payments' market within national borders had made it difficult for payment service providers to launch effective, convenient and secure digital payment services for consumers and retailers across the whole of the EU.

The EU considered that all this had led to legal uncertainty, potential security risks in the payment chain, and a lack of consumer protection in certain areas.

PSD2 is therefore focused on remedying these defects, in particular:

– promoting payment innovation and adjusting legal requirements,

– increasing the safety of payment transactions and payment services,

– increasing consumer safety, and

– clarifying the Directive's scope as well as the extent of exemptions from it.

It is therefore important to be aware of the main changes and amendments

PSD2's scope

The text of PSD2 represents a revised and complete version of both existing and new rules. It contains all the unchanged provisions of PSD1, as well as all amended and new provisions. Also, as with PSD1, the main objective of PSD2 is consumer protection. The focus remains on information obligations, transparency regarding contracts and pricing, rights and obligations regarding payment services, as well liability provisions. This means that PSD2 covers the relationship between a Payment Service Provider (PSP) and its corporate and retail customers – and not directly among PSPs on their behalf, as might be the case in correspondent banking.

While the Directive does not generally give member states the option to set standards any more liberally than the minimum, certain provisions do offer some potential for flexibility, and these are listed in Annex 2 to this white paper under "Member State Options".

For corporate customers (i.e. non-consumers), PSPs may decide, by agreement, that some articles need not apply. This includes all of Title III and some provisions of Title IV. That said, providers should check whether their relevant EU member states have opted to treat microenterprises in the same way as consumers.

As for the Directive itself, PSD2 consists of six parts or "Titles". Titles I, III and IV directly impact credit institutions' business:

- Title I is a summary of the Directive's subject matter and scope,
- Title III deals with transparency and information requirements,
- Title IV regulates the authorisation and execution of payment transactions, charges, data protection, operational and security risks and the settlement of disputes.

Titles II, V and VI impact credit institutions only indirectly:

- Title II: licensing requirements and supervisory rules for PSPs,
- Title V: delegated acts and regulatory technical standards,
- Title VI: a review clause, transitional provisions, amendments to other directives, and transposition rules.

Figure 1 below illustrates PSD2's structure and contents.

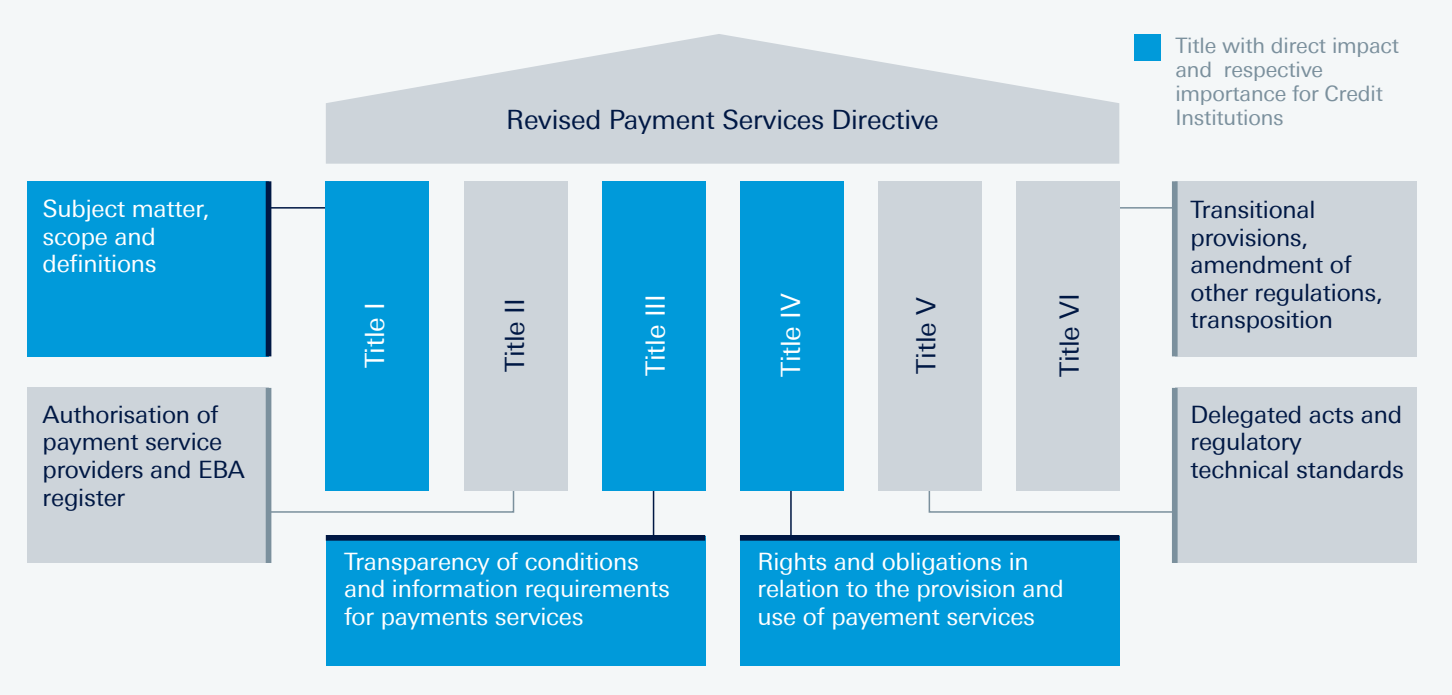


Fig 1: Structure and content of PSD2

Key changes from PSD1

The three key changes PSD2 makes to PSD1 are to extend the Directive's scope, to strengthen security and customer authentication requirements for mobile and internet payments, and to introduce TPPs to the EU payments market – as well as license and supervise them.

Extension of scope

The bulk of the Directive's provisions regarding transparency and information requirements (Title III) and rights and obligations (Title IV) have been extended to apply to:

- transactions where only one of the payment service providers is located inside the EU/EEA, and
- transactions in all official currencies, including non-EU currencies.

However, it is important to note that certain provisions of PSD2 are excluded from the extension of scope to all currencies and to payments where only one PSP involved in the transaction is located in the EU/EEA. These include the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Some payment services exempt from the scope of PSD1 are now included in PSD2 – for example payment activities covered by a limited network (such as shopping cards for a shopping mall). A full list of payment services included in PSD2 previously excluded from PSD1 or of uncertain status is in Annex 1 to this white paper.

Strong customer authentication

The authentication requirements for electronic payments and the protection of PSUs' financial data are strengthened, requiring 2-factor Authentication.

Third Party Providers

The payment services market has been opened up to TPPs.

Other changes

These include higher data protection requirements, a lowering of the maximum liability of consumers for unauthorised payments, and revised rules concerning the imposition of surcharges, or allowing discounts, for using specified payment instruments.

Figure 2 below illustrates the main changes and amendments made by PSD2 to PSD1.

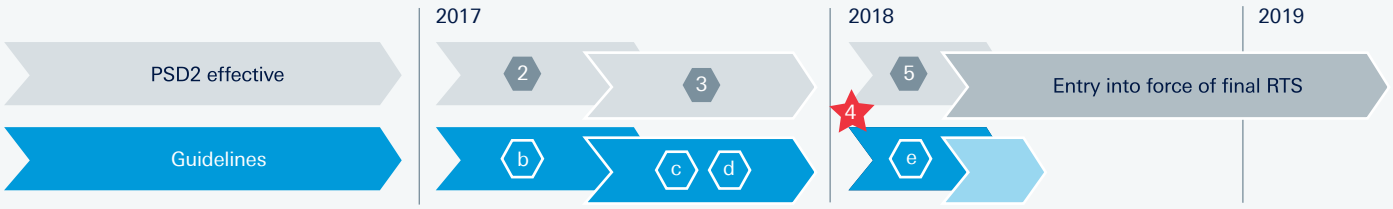
Fig. 2: Overview of changes introduced by PSD2

[5]Certain provisions of PSD2 are excluded from the extension of scope to all currencies and to payments where only one PSP involved in the transaction is located in the EU/EEA, including the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Schedule for implementation

PSD2 must be implemented by member states within two years of its publication, which means that member states have time until January 12, 2018 to transpose it into national law. However, at the same time a number of the basic regulations contained in PSD2 will have to be further clarified by the European Banking Authority (EBA) by means of Implementing Technical Standards (ITS), Regulatory Technical Standards (RTS) and Guidelines.

Figure 3 below provides an overview of the scheduled publication dates for the various Standards and Implementation Guidelines augmenting PSD2 (as announced to date: further changes are likely). References are to article numbers of PSD2. As the publication of its final draft is followed by an implementation period of 18 months, the entry into force of the final RTS could take until September 2019.



Date	Event	Details
12 Jan 2016	see above	PSD2 entered into force
13 Jan 2017	2	Final draft implementing regulatory technical standards: – specifying the criteria to be applied when determining, [...], the circumstances when the appointment of a central contact point is appropriate, and the functions of those(Art. 29.5) – framework for cooperation, and for the exchange of information, between the competent authorities of the home Member State and of the host Member State (Art. 29.6) – strong customer authentication and secure communication (Art.98.2)
13 Jul 2017	3	Final draft implementing technical standards: – details and structure of the information to be notified including the common format and model in which this information is to be provided (Art. 15.5)
12 Jan 2018	4	End of the implementation period for the PSD2 (national law should be in force)
13 Jan 2018	5	Final 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. (Art. 15.4) – specifying the framework for cooperation, and for the exchange of information, between competent authorities of the home and of the host Member State (Art. 28.5)

Date	Event	Details
13 Jan 2016	see above	Guidelines for criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee (Art. 5.4)
13 Jan 2017	b	Guidelines on Management of operational and security risks (Art.95.3)
13 Jan 2017	c	Guidelines specifying the information to be provided to the competent authorities in the application for the authorisation of payment institutions, (Art. 5.5)
13 Jul 2017	d	Guideline with regard to the establishment, implementation and monitoring of the security measures (Art. 95)
12 Jan 2018	4	End of the implementation period for the PSD2 (national law should be in force)
13 Jan 2018	4	Guidelines on incident reporting (Art. 96.3) Guidelines on complaints procedures to be issued, addressed to the competent authorities (Art. 100.6)

Fig. 3: Timetable for PDS2's "Standards" and "Implementation Guidelines"

In total, the EBA is expected to publish six RTSs, one ITS and five Guidelines of which the following four are directly relevant to financial institutions (as highlighted in Figure 3):

- Guideline on the establishment, implementation and monitoring of security measures (deadline: July 13, 2017),
- Guideline on incident reporting (deadline: January 13, 2018),
- RTS on strong customer authentication and secure communication (deadline: January 13, 2017)[6], and
- RTS on development, operation and maintenance of an electronic central register and on access to the information contained therein (deadline: January 13, 2018).

[6]The EBA has published a consultation paper on draft technical standards on strong customer authentication and common and secure communication under PSD2, inviting comments. A public hearing on this topic will take place at the EBA's premises on Friday 23 September 2016, and the final deadline for submission of comments is 12 October 2016. Details may be found on the EBA's website.

2 PSD2's provisions in detail

Title I - Subject Matter and Scope (Art. 1-4)

The subject matter of PSD2 is the same as that of PSD1 – to provide the legal foundation for the creation of an EU/EEA-wide single market for payments. Given this, the Directive distinguishes the following categories of Payment Service Provider (PSP):

- Credit Institutions,
- E-Money and Payment Institutions,
- Post Office Giro Institutions,
- The European Central Bank (ECB) and national central banks.[7]

Title I of PSD2 extends the Directive's scope to non-EU/EEA payment transactions (currencies), and to where only one payment service provider is located in the EU/EEA.[8] The Directive distinguishes between the following three scenarios illustrated in Figure 4 (and again in Figure 14) below:

1. The "Two-Leg-Principle" (reflecting the scope of PSD1): The Directive applies to all payment transactions in all EU/EEA-currencies carried out in the EU/EEA.
2. Foreign currency transactions (new). This extends the "Two-Leg-Principle": payment transactions in every currency, where all participant PSPs are located within the EU/EEA.
3. The "One-Leg-Principle" (new): payment transactions in every currency, where only one of the PSPs is located within the EU/EEA, in respect of those parts of the payment transaction that are carried out in the EU/EEA.

[7]When not acting in their capacity as monetary authorities or other public authorities.

[8]Certain provisions of PSD2 are excluded from the extended scope to all currencies and to where only one PSP involved in the transaction is located in the EU/EEA, such as the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Figure 4 below illustrates the three scenarios 1) to 3) described above.

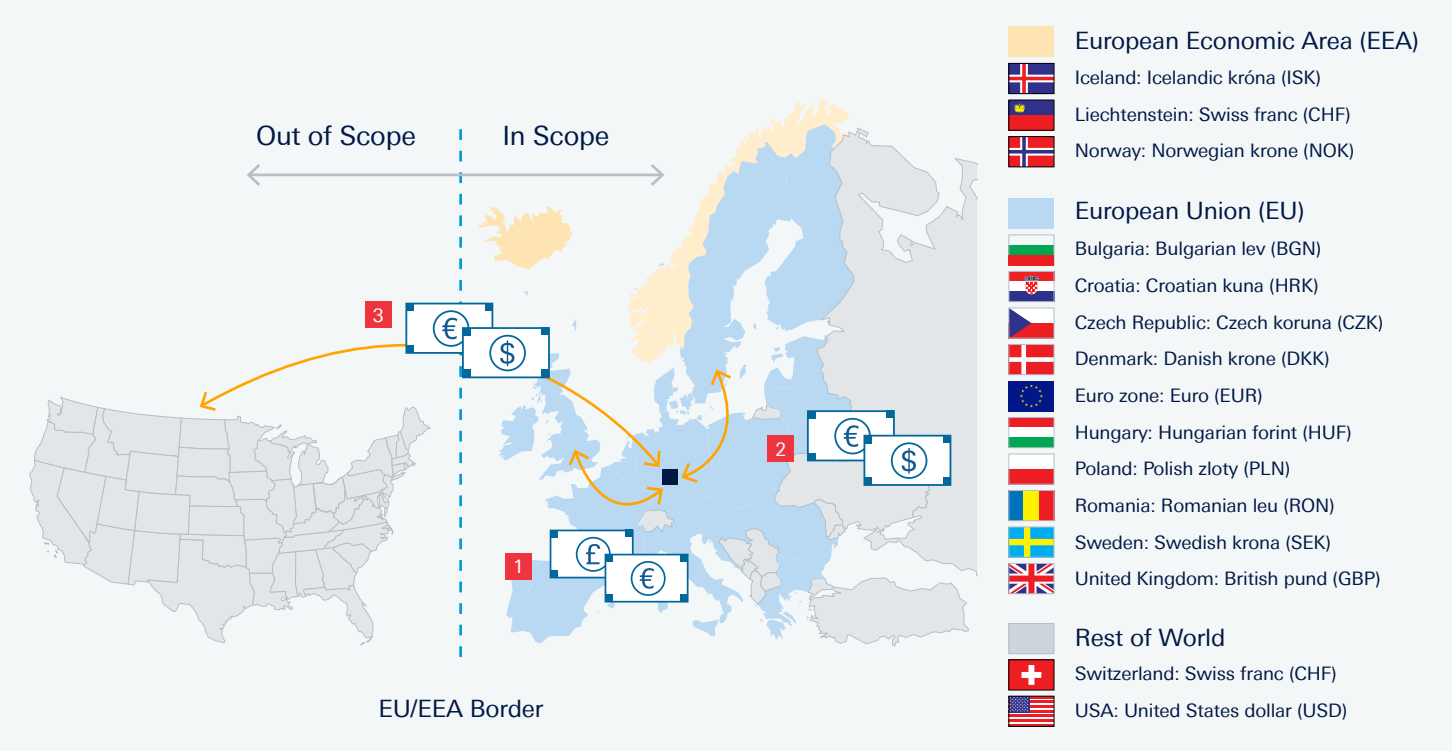


Fig. 4: Regional and Currency Scope of PSD2. For illustration purposes only.

The Swiss Franc occupies a special place. Liechtenstein is an EEA country with the Swiss Franc (CHF) as its official currency – meaning that the CHF counts as an EEA currency despite Switzerland not being in the EEA.

Impact of PSD2's scope extension on PSPs' business

In considering where "One-Leg" starts and ends the following assumptions seem reasonable:

1. Scope definition for "One-Leg in/out": PSD2 starts impacting a PSP as soon as funds are credited to a clearing account of one of its entities domiciled in the EU, and the required information becomes available to this entity.

   Regarding outgoing payments, the PSP is obliged to adhere to PSD2 until the afore-mentioned clearing account is debited.

2. Cut-off time: The relevant cut-off time is always defined by the cut-off time of the PSU's payment service account.

3. Value dating: The relevant clearing system holiday is always the clearing system holiday (e.g. TARGET2 holidays) where the PSU's payment account is held (i.e. the booking location).

Exclusions (Art. 3)

While PSD2 does not add any exclusions regarding payment instruments to those made by PSD1, it defines them more closely. These include, for example:

- Cash payments,
- Cheques,
- Payments between PSPs for their own account,
- Payments between parent companies and subsidiaries, or between subsidiaries of the same parent (no PSP involved),
- Payments within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and others, and PSPs,
- Payments relating to securities asset servicing, including dividends, income or other distributions, or to redemption or sale, or by investment firms, credit institutions, collective investment undertakings or asset management companies and other entities having custody of financial instruments.

Title II - Authorisation of payment service providers and establishment of an EBA-Register (Art. 5-37)

Title II sets out the authorisation requirements and procedures for Payment Institutions (PIs), Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). It also regulates which payment institutions have to be registered, and lays down rules for communication with and between authorities, as well as between member states. Title II also deals with the supervision of these entities, and with the contents and maintenance of both national registers, and a new EBA Register, to record their details. Finally, it formulates the rules governing payment institutions' access to payment systems and to credit institutions' payment accounts services.

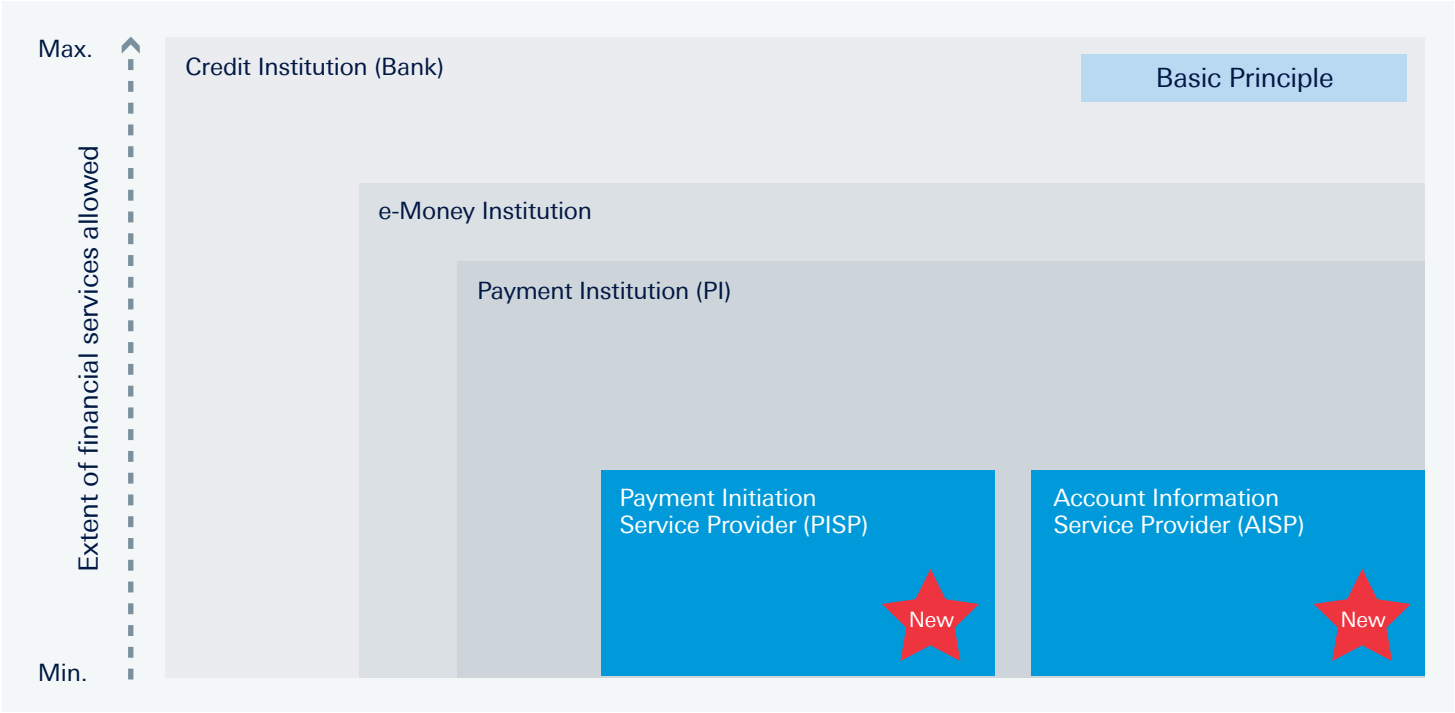


Fig. 5: Types of licences for financial institutions offering payment services. For illustration purposes only.

As can be seen from Figure 5 above, different types of licences are required depending on which types of financial service an organisation wishes to offer. A licence to act as a credit institution includes the permission to provide a wide range of financial services such as granting loans, receiving deposits and – most importantly – offering payment services. Licences for e-money institutions and payment institutions are more limited in scope, only allowing these institutions to provide and carry out specific payment and/or e-money services.

These specific payment services are listed in Annex 1 of PSD2 and include for example:

- executing payment transactions, including transfers of funds from a payment account with the user's PSP or with another PSP,
- executing direct debits, including one-off direct debits,
- executing payment transactions through a payment card or a similar device,
- executing credit transfers, including standing orders,
- issuing payment instruments and/or acquiring payment transactions, and
- money remittances.

Two new types of licence for "Third Party Providers" (TPPs)

PSD2 introduces two new types of licence for TPPs: a licence for Payment Initiation Service Providers (PISPs) and a licence for Account Information Service Providers (AISPs). In terms of the types of services that can be offered, both licences are more restrictive than those held by regular payment institutions. AISP and PISP services are relevant to a PSP and its corporate and retail customers – not to services between PSPs, such as in correspondent banking.

A payment initiation service is defined as a service to initiate a payment order at the request of a PSU with respect to a payment account held at another PSP. Payment initiation services enable the PISP to provide comfort to a payee that the payment has been initiated, as an incentive to the payee to release goods or deliver a service without undue delay.

An account information service is an online service to provide consolidated information on one or more payment accounts held by a PSU with another PSP or multiple PSPs.

Admission requirements for new service providers

In order to be authorised, an AISP is required to hold professional indemnity insurance and be registered by their member state and by the EBA. There is no requirement for any initial capital or own funds. The EBA will publish guidelines on conditions to be included in the indemnity insurance (e.g. the minimum sum to be insured), although it is as yet unknown what further conditions insurers will impose.

The minimum requirements for authorisation as a PISP are significantly higher. In addition to being registered, a PISP must also be licensed by the competent authority, and it must have an initial and on-going minimum capital of EUR 50,000.

The EBA Register

The EBA must operate and maintain a central electronic register of the information notified to it by the national registers and make this publicly available on its website without charge, granting easy access and providing easy research functionalities. Any Account Servicing Payment Service Provider (ASPSP) – the PSP of a PSU – should be able to ascertain electronically, immediately and reliably, whether a service provider is authorised to initiate payments or collect account information (Art. 15).

The EBA Register is not expected to incorporate such data on a real-time basis – meaning that ASPSPs must assess the risk of this register suffering from time gaps, such as:

a) a time gap between a new TPP being listed and its first transaction,

b) a time gap between a national supervisory authority realising that a provider has acted fraudulently and that provider losing its licence.

Payment Institutions' access to payment systems

PSD2 gives authorised and registered payment institutions access to payment systems, and also to credit institutions' payment accounts services (Art. 35, Art. 36). The Directive stipulates that such access shall be extensive enough to allow them to provide payment services in an unhindered and efficient manner. Access must be allowed on an objective, non-discriminatory and proportionate basis. Furthermore, credit institutions shall not inhibit account access unless necessary to safeguard against specific risks. Where a credit institution rejects a request for access, it must provide the competent authority with a detailed statement of its reasons for rejecting the request.

A practical consequence for credit institutions will be that they must carry out risk assessments prior to granting payment institutions access – taking into account settlement risk, operational risk and business risk.

Title III - Transparency of conditions and information requirements for payment services (Art. 38-60)

Title III sets out PSD2's requirements regarding transparency of contractual conditions, and the information to be provided by PSPs to PSUs. It focuses on the key elements of content, conditions, accessibility and charges.

Title III differentiates between single payment transactions (e.g. payment transactions with walk-in clients, where no contractual relationship exists) and transactions under a framework contract.

Content

Specific elements of Title III include:

- Prior general information: regardless of the type of the underlying payment transaction, the relevant information and conditions must be made available to the PSU on a clear and comprehensive basis before actually entering a contractual relationship or initiating a single payment.
- Information relating to the payment order: the key difference between framework contracts and single payment transactions is the actual moment when the information relating to the payment order must be made available to the PSU. In the case of single payment transactions, this is immediately after receipt of the payment order. Under a framework contract, information concerning an individual payment must be given to the PSU either after the amount is debited, or after receipt of the payment order.
- Information provided to the payer: the payer of a single payment transaction will receive the payment data relating to the payment order immediately after they have been received by the ASPSP. Under a framework contract, information regarding individual payment transactions must be provided to the payer either after the amount is debited, or after the receipt of the payment order.

Conditions

The type of a transaction determines what information and conditions must be provided to the PSU, and the level that will have to be specified. The information to be provided must include information on the PSP, the payment service itself, on charges, interest and exchange rates as well as safeguards, corrective measures and changes to and termination of the framework contract (Art. 52).

Accessibility

At any time during the contractual relationship, the PSU has a right to receive, on request, the contractual terms of the framework contract as well as the information and conditions specified in Art. 52. A single payment transaction does not imply any contractual relationship, so no information other than that relevant to the single payment order needs to be given in that case.

Figure 6 below summarises the legal requirements for single payments and for those made under framework contracts.

	Framework Contracts Chapter 3: Art. 50-59	Single payment transactions Chapter 2: Art. 43-49
Prior general information	Providing the informations and conditions, on a clear and comprehensive base, to the PSU before entiring a contractual relationship [Art. 51 (Framework) and Art.44 (Single)]	
Informations & Conditions	Related to the contractual relationship between the counterparties, the overall and the underlying payment processes and contact information [Art. 52 & 54]	Characteristics of the underlying payment procedure and contact information [Art. 45]
Information relative to the payment order	Before the execution of individual payments [Art. 56]	For the payer and payee after the initiation of a payment order [Art. 46]
Information addressed to PISP	Included within the requirements relative to the "informations & conditions"	References of the payment transaction [Art. 47]
Information addressed to Payer	Relative to individual payment transactions including specific payment data:	
	After the amount is debited or after receipt of the payment order [Art. 57]	Immediatly after receipt of the payment order [Art. 48]
Information addressed to Payee	Provision of specific data in regards to the transaction [Art. 58 (Framework) and Art.49 (Single)]	
Accessibility	Anytime: contractual terms of the framework contract as well as the information and conditions [Art. 53]	Not specified
Termination	PSU may terminate at any time. period of notice may not exceeded 1 month. [Art. 55]	Not required

Fig. 6: Requirements concerning transparency and provision of information in framework contracts and in single payment transactions

Charges

No charge shall be made for any mandatory information, such as maximum execution time (Art. 40). Charges may be made for certain other types of information, such as:

- additional information (e.g. graphic analysis),
- more frequent information (e.g. real-time), and
- a different means of communication requested by a PSU (e.g. additional paper-based statements).

The charges applied shall be reasonable and in line with the PSP's actual costs.

Figure 7 below illustrates the principles behind the rules for charges for information.

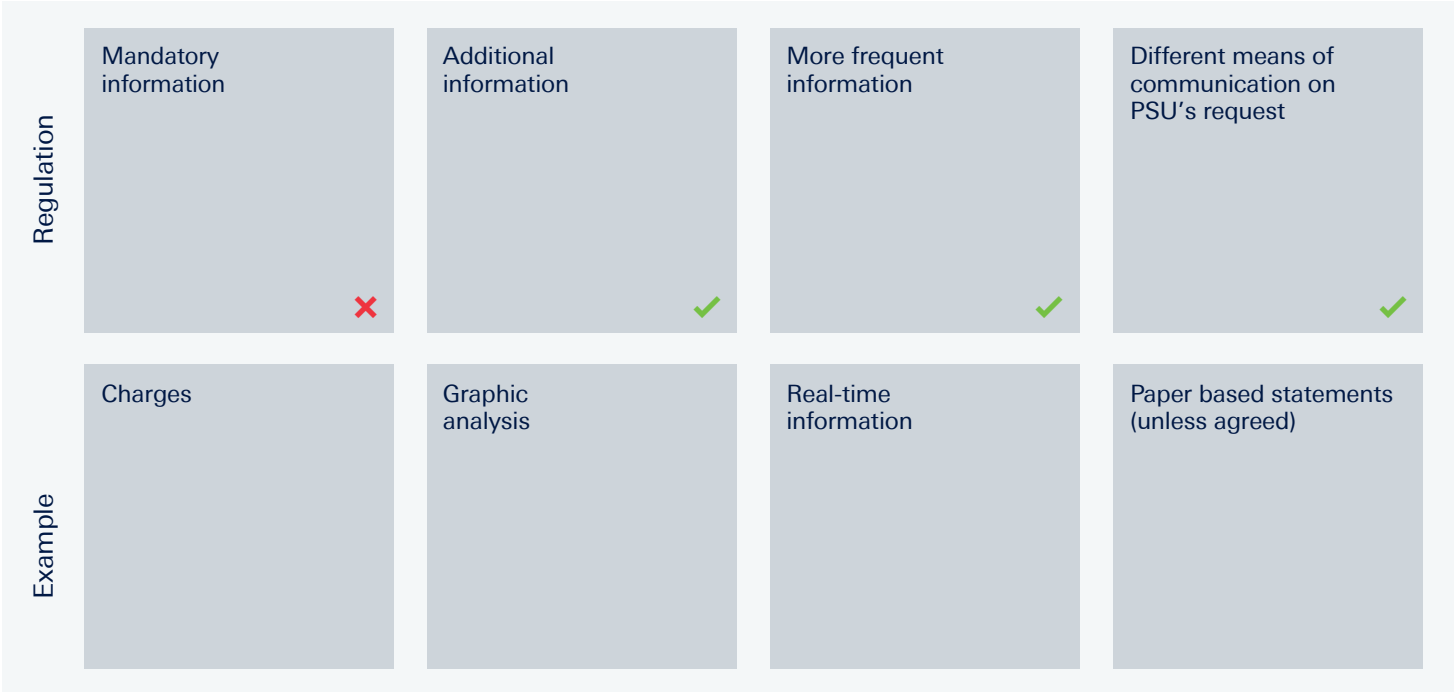


Fig. 7: Charges for providing information to PSUs

Title IV - Rights and obligations in relation to the provision and use of payment services (Art. 61-103)

Charges for international transactions

In PSD2's introduction, it says: "Experience has shown that the sharing of charges between a payer and a payee is the most efficient system since it facilitates the straight-through processing of payments". Despite this clear statement of intent, the legislative text itself is more complex.

Figure 8 below sets out the charges and deductions for different kinds of payments, adopting the SWIFT codes "BEN", "SHA", "OUR" that direct how charges are to be allocated. It also shows that the basic principle for intra-EEA transactions in EEA currencies is to share charges, using the "SHA" code.

The charge code "OUR" is still used by way of existing market practice in light of PSD1. The respective provisions have not fundamentally changed from PSD1 to PSD2. The application of such a charge code – however – requires, at least, a specific request by the payer and that the payer has full transparency on the costs associated with the payment transaction before entering into it.

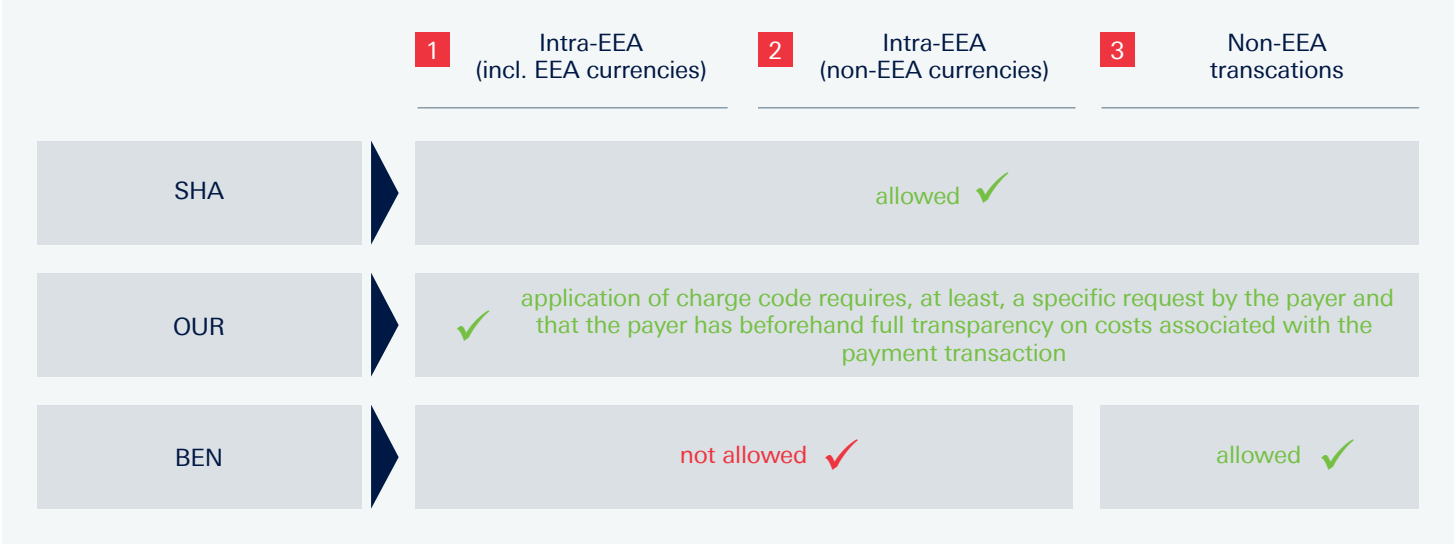


Fig. 8: Charges Codes (Art. 62.2)

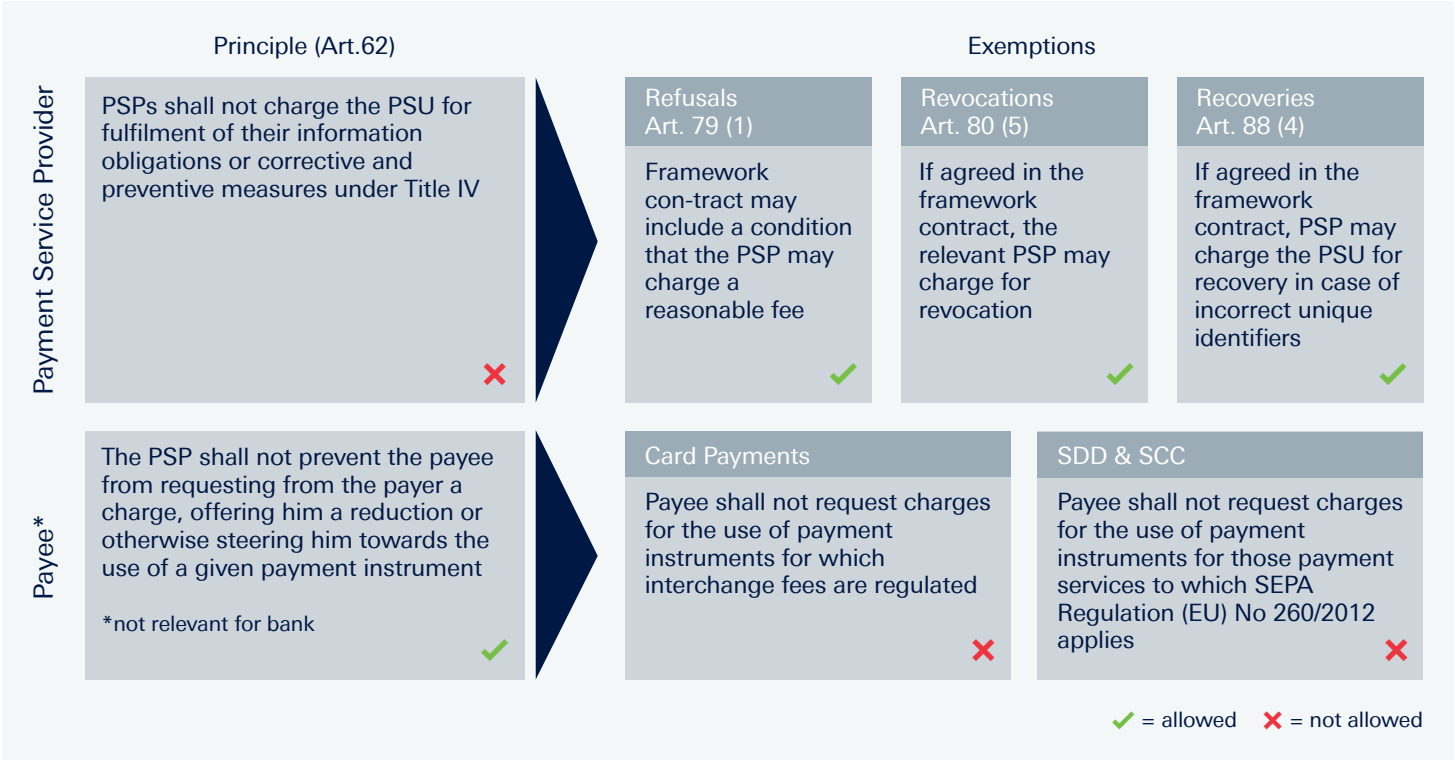
The deduction of fees for transactions where both the payer's and the payee's PSP are located in the EU/EEA and which are carried out in an EU/EEA currency is explicitly not allowed under PSD2 ("full amount principle", Art. 81).

As PSD2 only applies to those parts of the payment transaction that are carried out within the EU, it cannot define rules for charges and deduction of fees outside EU jurisdiction. Therefore, in the case of intra-EEA transactions in non-EEA currencies, and one-leg transactions, it can be concluded that there are no restrictions regarding the deduction of fees.

Other charges

Article 62 of PSD2 provides the legal framework for certain other types of charge. Generally, a PSP must not charge a PSU for fulfilling his information obligations, or for corrective or preventative measures, unless otherwise specified. Title III of the Directive defines the extent of a PSP's information obligations towards PSUs, and Title IV specifies the following exemptions from those rules illustrated in Figure 9 below:

- Refusals: the framework contract may include a condition that the PSP may charge a reasonable fee based on market standards (Art. 79.1 for a payment execution refusal ("if the refusal is objectively justified")),
- Revocations: if agreed in the framework contract, the PSP may charge for revocation (Art. 80.5),
- Recoveries: if agreed in the framework contract, the PSP may charge the PSU for recovery where the PSU gave an incorrect unique identifier (Art. 88.4).



Figs. 9 and 10: Rules for Charges by PSPs

PSD2 also defines rules for charges that payees may request. Under PSD1, agreements between PSUs and payees imposing a surcharge or allowing a discount for using a specified payment instrument were prohibited. Under PSD2, such agreements are allowed, but the payee must inform the payer of this prior to initiation of the payment transaction (Art. 60), and the charges applied must be reasonable, in line with the PSP's actual costs, and must not exceed the payee's direct costs for the use of the specified payment instrument. Also, as is illustrated by Figure 10 above, the payee shall not:

- request charges for the use of payment instruments for which interchange fees are regulated with regard to card payments (Art. 62.4),
- request charges for the use of payment instruments for those payment services to which SEPA-Regulation (EU) No 260/2012 applies – e.g. SEPA Credit Transfers and SEPA Direct Debits.

Security and authentication

In response to the recent rise in volumes of digital payments across the EU/EEA employing a variety of authentication methods, PSD2's second major thrust is strengthening security, as well as trying to introduce a minimum standard for authentication of all electronic payments (though certain categories of payments are exempt). Concomitantly, the Directive aims to ensure that consumers enjoy increased protection of their financial data.

PSD2 introduces a requirement for strong or 2-factor customer authentication (2FA) using two or more elements out of the following three:

- Knowledge: something only the user knows (e.g. a password or PIN),
- Possession: something only the user holds (e.g. a card or a token), and
- Inherence: something only the issuer is (e.g. a finger print or voice).

The elements must be independent of each other, meaning that a breach of one does not compromise the reliability of the others, and they must be designed in a way to protect the confidentiality of the authentication data.

The concept of 2FA was first introduced in the EBA's "Final guidelines of security of internet payments (EBA/GL/2014/12)". Yet PSD2 enjoys a wider scope than the EBA guidelines. While those only apply to browser-based payments, Art. 97 of PSD2 stipulates that a PSP must apply strong customer authentication "where the payer:

a) accesses its payment account online, [or]

b) initiates an electronic payment transaction, [or]

c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."

For electronic remote payment transactions, an additional dynamic element is required, linking the transaction to a specific amount and a specific payee (Art. 97.2). This additional requirement is based on the regulator's view that the solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures.

Payment services offered via the internet or other at-distance channels (where execution is not dependent on the physical location of the device used to initiate the payment transaction or the payment instrument) should therefore include authentication of transactions through dynamic codes. This is in order to make the PSU aware, at all times, of the amount and the payee of the transaction being authorised.

When trying to implement 2FA, one of the first questions to be answered concerns which element of authentication falls under which category. Figure 11 gives some sample applications, although it does not define which combinations of elements are sufficient to achieve 2FA. As the factors have to be independent, a combination of two factors on the same device may not be sufficient.

Element	Knowledge	Possession	Inherence
Combination of access number & PIN	✓	✗	✗
Combination of credit card number & CVC/CVV	✓	✗	✗
Password	✓	✗	✗
M-TAN (Token)	✗	✓	✗
Chip-TAN	✗	✓	✗
Digi Pass	✗	✓	✗
Signature	✗	✗	✓
Fingerprint	✗	✗	✓
smsTAN	ϟ	ϟ	✗
pushTAN	ϟ	ϟ	✗
Crypto-Key (e.g. Corporate Seals, Certificates)	ϟ	ϟ	✗
Electronic signature	✗	ϟ	ϟ
(…)			

✓ = assignment of element clear ✗ = element is not assignable to this category ϟ = assignment of element still in discussion

Fig. 11: Sample applications of strong customer authentication

The implementation period for 2FA is expected to end in October 2018, and the relevant RTS, the first draft of which was recently published, may provide clarification. Figure 12 below provides an overview of the RTS' expected timeline.

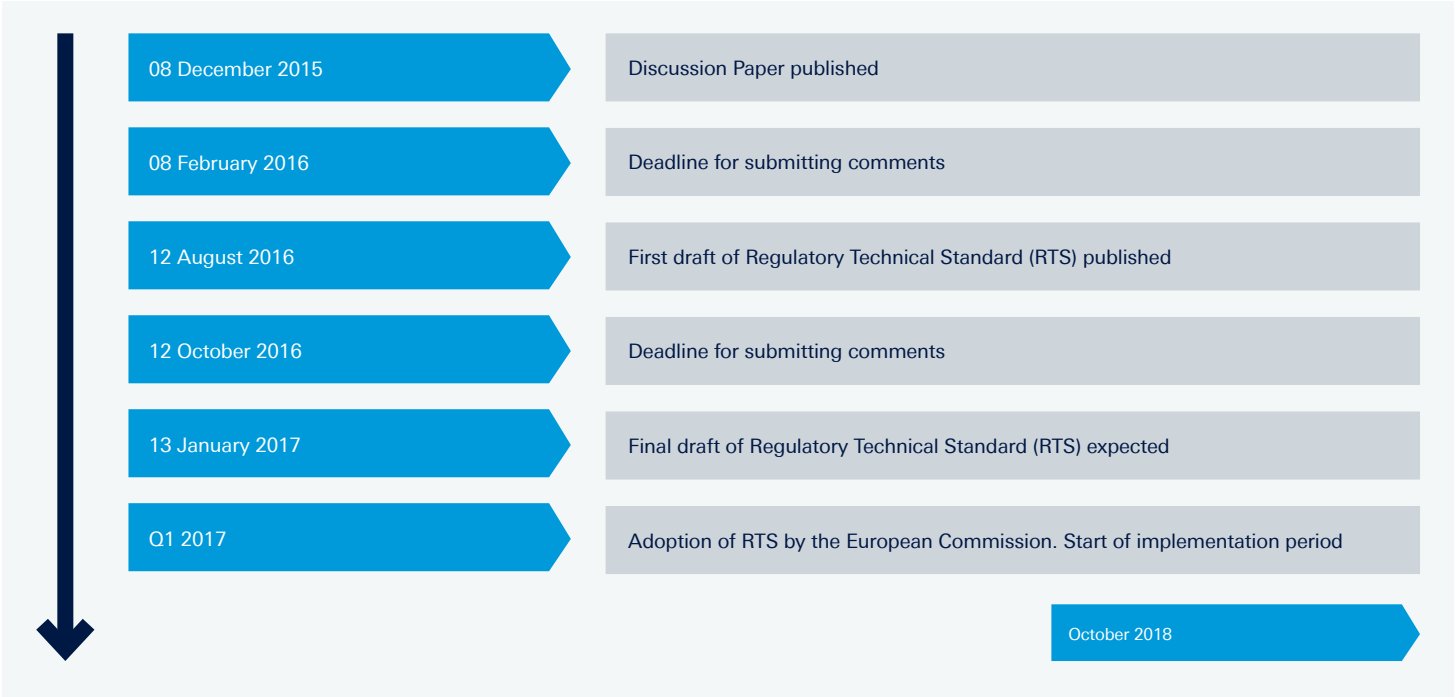


Fig. 12: Timeline for the RTS for 2FA

Exemptions from the requirement for strong customer authentication

As strong customer authentication may not be a necessary requirement for all electronic payment transactions, Art. 98.3 provides for exemptions, based on the following criteria:

a) the level of risk involved in the service provided,

b) the amount, the recurrence of the transaction, or both, or

c) the payment channel used for the execution of the transaction.

In December 2015, the EBA published a discussion paper in which it lists types of payment transactions that might suitably be exempt from strong customer authentication. These are:

a) low-value payments as defined in PSD2, provided the risk of cumulative transactions is monitored,

b) outgoing payments to trusted beneficiaries included in white lists previously established by a PSU,

c) transfers between two accounts of the same PSU held at the same PSP,

d) low-risk transactions based on a transaction risk analysis (taking into account detailed criteria to be defined in the RTS),

e) purely consultative services, with no display of sensitive payment data, taking into account data privacy laws.

The EBA intends to provide further clarification in this area in its forthcoming RTS – particularly with respect to how the risk of a transaction should be evaluated. The following information could provide the basis for a real-time risk analysis:

– an adequate transaction history of the specific customer to evaluate typical spending and behaviour patterns,

– information about the customer device used (e.g. IP address, model, operating system, language preferences), and, where applicable,

– a detailed risk profile of the payee (e.g. types of service provided, transaction history) and the payee's device (where applicable).

Operational and security risks

PSD2 requires every PSP to establish a framework with appropriate mitigation measures and control mechanisms to manage its operational and security risks with regard to payments. It must also establish and maintain effective incident management procedures (including detection and classification of major operational and security incidents). It must submit an annual report containing a comprehensive assessment of its operational and security risks to the competent authority. An additional report to the competent authority, as well as to the customer, is mandatory in case of a major operational or security incident, and this must be written without undue delay.

The Guidelines and RTS to be published by the EBA will contain further requirements:

– Guidelines for the establishment, implementation and monitoring of security measures (expected: July 13, 2017);

– Guidelines for the classification of incidents and competent authorities (expected: January 13, 2018;

– Regulatory technical standards for authentication and secure communication (expected: January 13, 2017).

Procedures for the settlement of disputes

PSPs have to make every possible effort to reply, on paper – or, if agreed between the PSP and the PSU, in another durable medium – to a PSU's complaints. Such a reply must address all points raised within an adequate time frame 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 PSP's control, then it must send a holding reply, clearly indicating the reasons for the delay in answering the complaint and specifying the time by which the PSU will receive a final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days (Art. 101.2).

There are "Member State Options" relating to dispute procedures (see Annex 2 to this white paper).

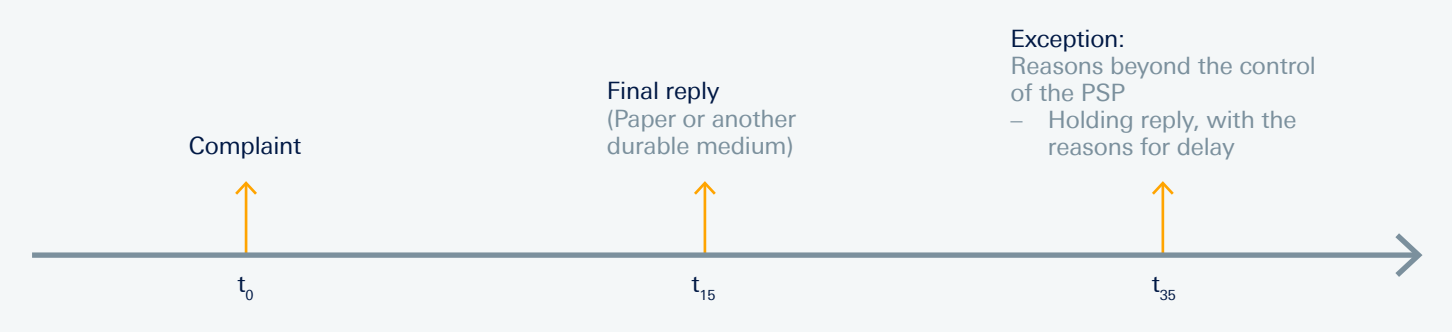


Fig. 13: Timeline for complaints handling

Conditional Payments

Non-payments products, such as documentary credits, are beyond the scope of PSD2. However, given that banks aim for standardised processes and platforms one may consider to process such payments as per PSD2 conditions.

Obligation to inform consumers of their rights

PSD2 imposes an obligation on the European Commission to produce an electronic leaflet listing the rights of consumers under this Directive and related EU law by January 13, 2018. This must be made available in an easily accessible form on the Commission's website and be user-friendly, clear and easily comprehensible. Payment service providers will have to make this information available on their websites, as well as in hard copy at their branches, and may not charge clients for so doing.

3 The impact of PSD2's scope extension on transactions

PSD2's extension of the Directive's scope – both in terms of geography and in terms of currencies covered – is likely to be one of the major concerns for financial institutions when implementing PSD2. The work required should not be underestimated. Below are just some examples of the impact this may have on booking, value date and availability of funds.

PSD1 applied only to payment services provided within the EU/EEA and made in euros or another currency of an EU member state outside the euro area. Additionally both the payer's PSP and the payee's PSP, alternatively the sole PSP in the payment transaction, had to be located in the EU/EEA. PSD2 extends its scope to payment transactions within the EU/EEA carried out in non-EEA currencies, and to payment transactions where only one PSP is located in the EU/EEA.[9]

Figure 14 below shows transactions falling under the provisions of PSD2. It also represents scenarios 1), 2) and 3) introduced in Part Two above illustrated in Figure 4 above.

Impact on credit notes, value date and availability

The extended scope of PSD2 results in a number of process adjustments for financial institutions. Requirements for transactions covered by PSD2 have to be applied to various parts of international transactions. PSD2 defines certain points in time during the execution of payment transactions. To differentiate between these points in time, the terms "crediting/booking", "value date" and "availability" of the money are defined as follows:

Credit note/booking date

Act of documenting receipt of funds - the credit note is an abstracted promise of claim of the PSU against the PSP.

Value date

Value date means a reference time used by a PSP for the calculation of interest on the funds debited from, or credited to, a payment account.

Availability

Once the funds are available, the PSU can dispose of them, for example by credit transfer, direct debit, or by withdrawing them in cash.

In general, the value date for the PSU is based on the same standards as for transactions under PSD1. If funds reach the payment account of the account servicing payment service provider (ASPSP), the value date has to be on the same day. Funds have to be made available to the PSU as soon as possible.

[9]Certain provisions of PSD2 are excluded from the extended scope to all currencies and to where only one PSP involved in the transaction is located in the EU/EEA, such as the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Outgoing transactions

Figures 15 and 16 below describe the handling of outgoing transactions. The PSU's value date and booking date are the same date as the date of payment initiation. PSD2 does not specify any time-frame for currency conversion in case of outgoing payments.

Incoming transactions

In case of an incoming transaction in euros (and in case of a preliminary currency conversion, when the currency conversion into euros is performed outside the EEA), on reaching the EEA the transaction would be deemed to be a euro transaction (see Figure 17 below). The credit note on the ASPSP's payment account corresponds with the booking date and value date on the PSU's account. The funds must be immediately available to the PSU. In general, availability is assured through the credit note on the PSU's account.

In case of an incoming transaction in any other currency (e.g. USD) and where the receiving customer's account (e.g. USD) is kept in the same currency, the funds shall also be booked and made available immediately. Therefore the same rule applies for incoming transactions without currency conversion. If the amount reaches the ASPSP's payment account, the credit note, value date and availability will be on the PSU's account on the same day.

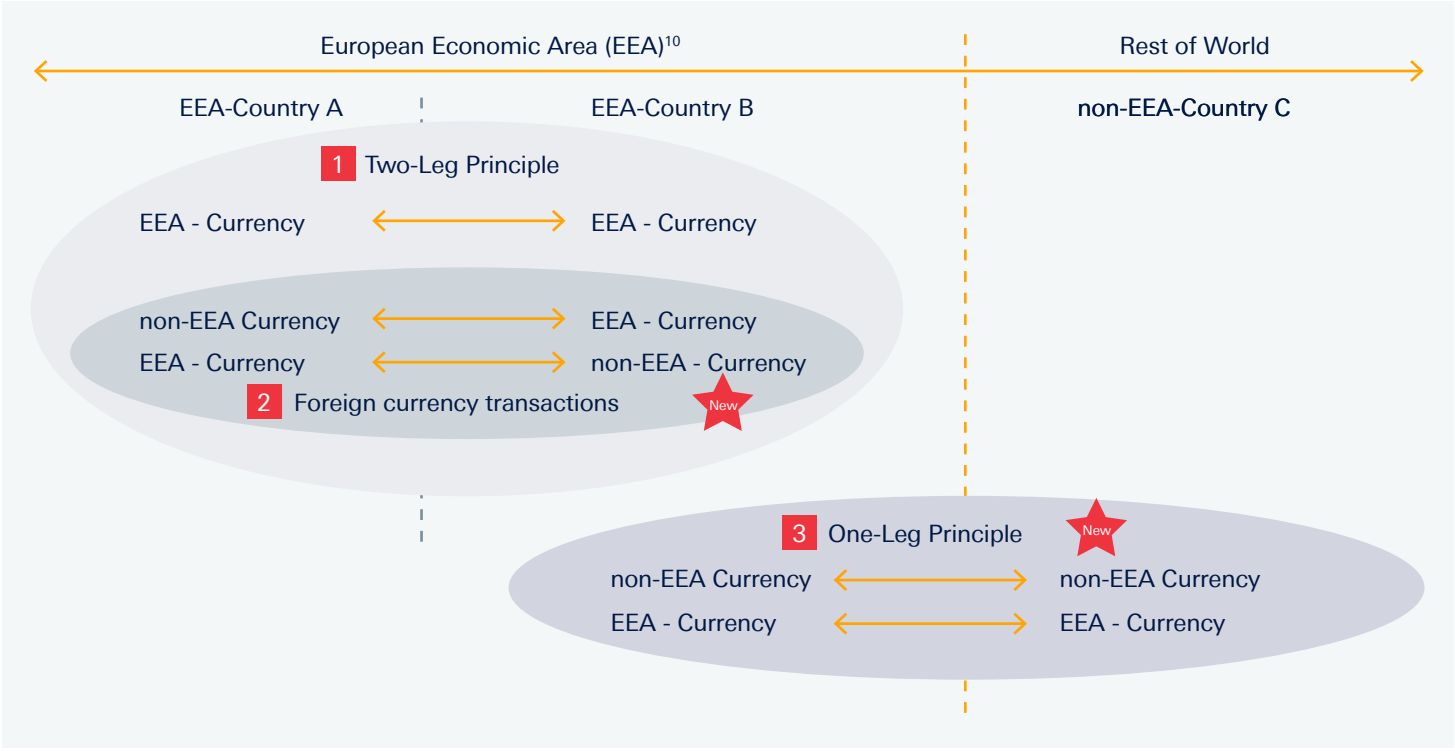


Fig. 14: Overview of transactions covered by PSD2. For illustration purposes only.

[10]The term EEA is used as synonym for EEA & EU

In case of an incoming transaction in a non-euro EEA currency with subsequent currency conversion in the EEA into euro (see Figure 18 below) (or vice versa) the amount has to be credited to the payee's payment service provider's account at the latest on the next business day. There is an ongoing discussion among market participants regarding the value date: does it have to be the same date as the credit note, or is it the date when the conversion of the currency into euros is finalised? If the former, it would lead to increased interest rate risk.

In the case of an incoming transaction in a non-EEA currency with subsequent currency conversion into euros (see Figure 19 below) the same discussion concerning the value date is ongoing. However, there is no requirement for the availability of funds under PSD2.

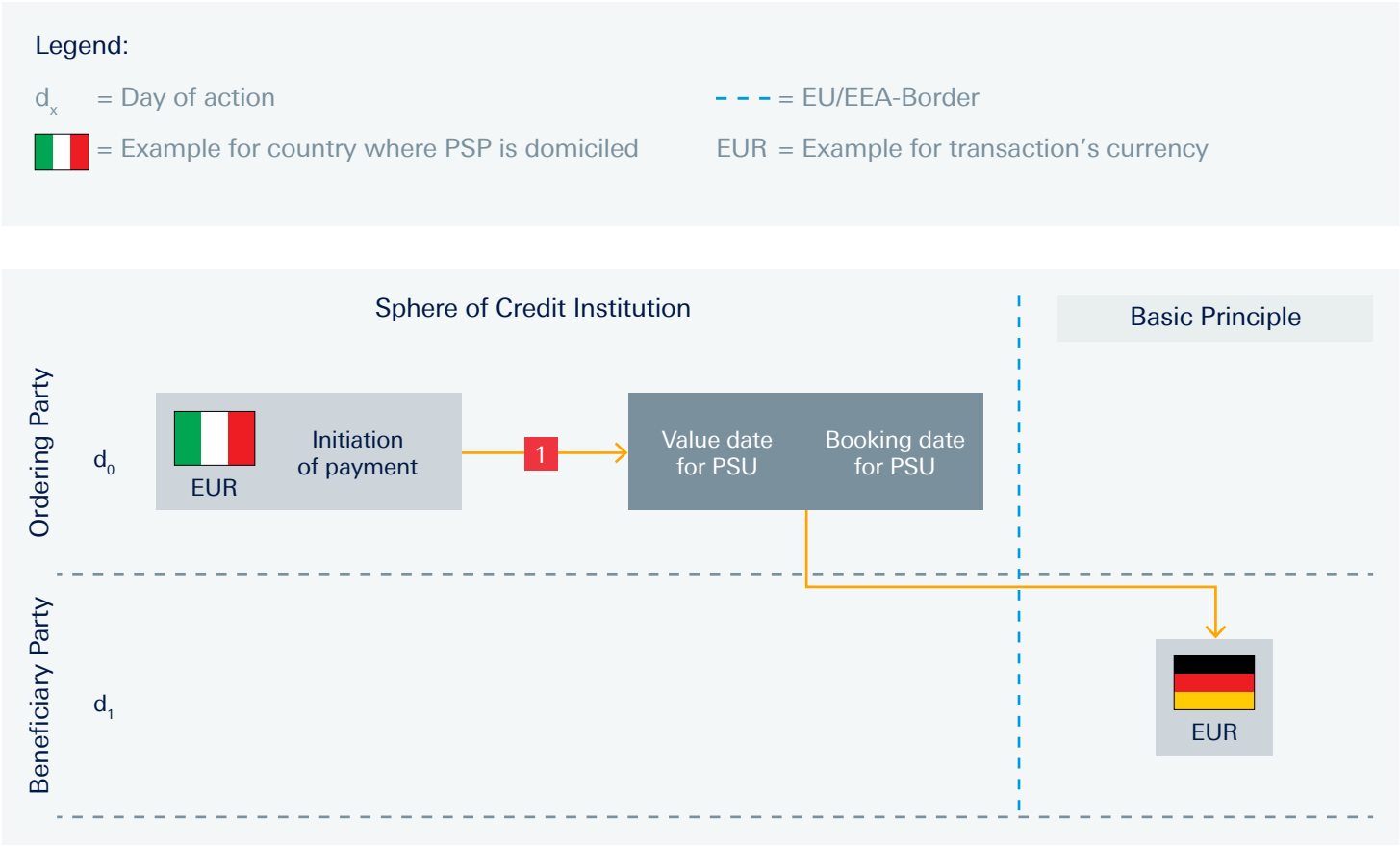


Fig. 15: Outgoing transactions without currency conversion

There are Member State Options relating to transaction processing (Arts 76.4 and 86 – see Annex 2).

Cash placement on payment accounts

PSD2 states that where a consumer places cash on a payment account 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. Unlike previously under PSD1, PSD2 now requires that, for both consumers and corporates, the amount shall be made available and value-dated at the latest on the following business day after receipt of the funds.

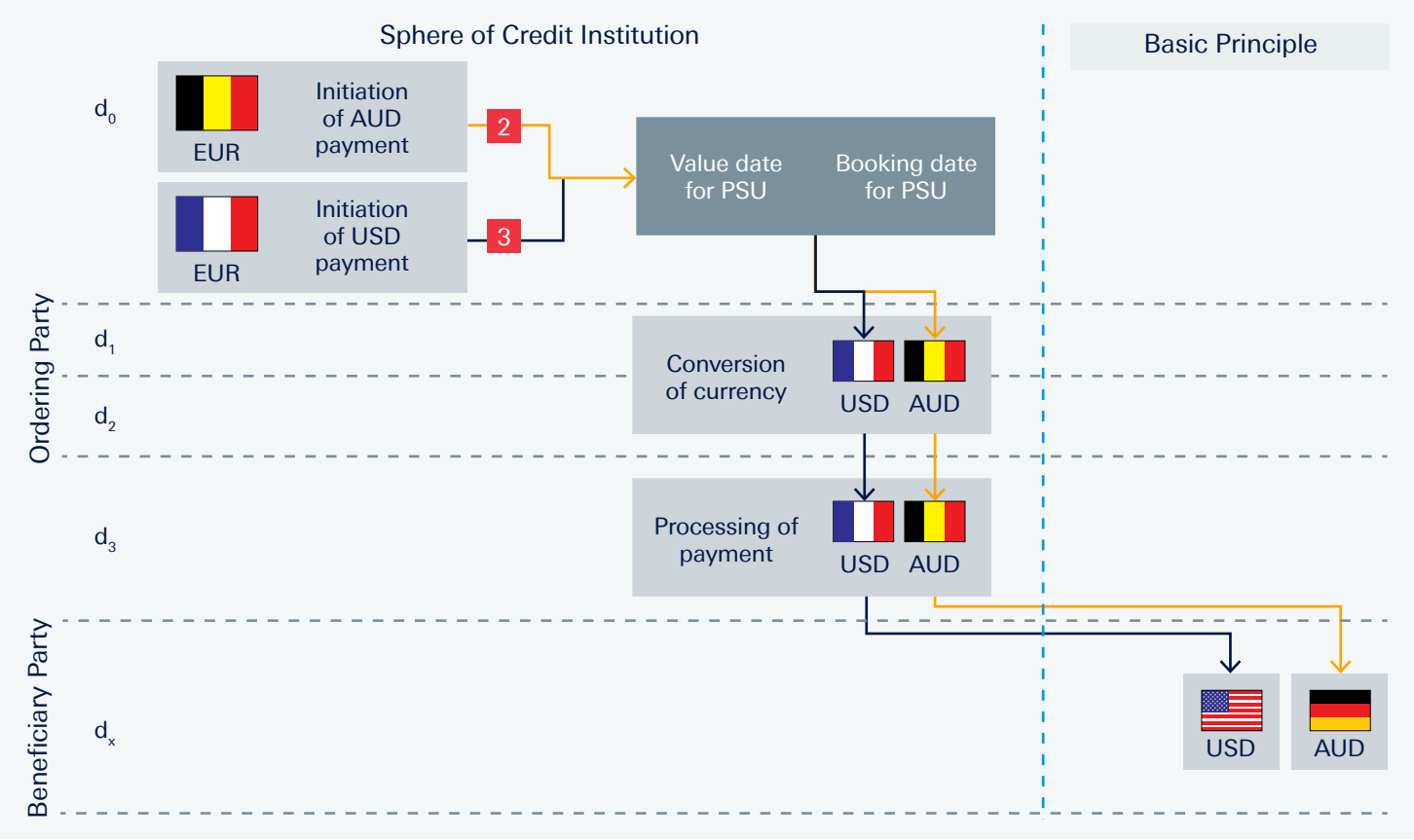


Fig. 16: Outgoing transactions with currency conversion. For illustration purposes only.

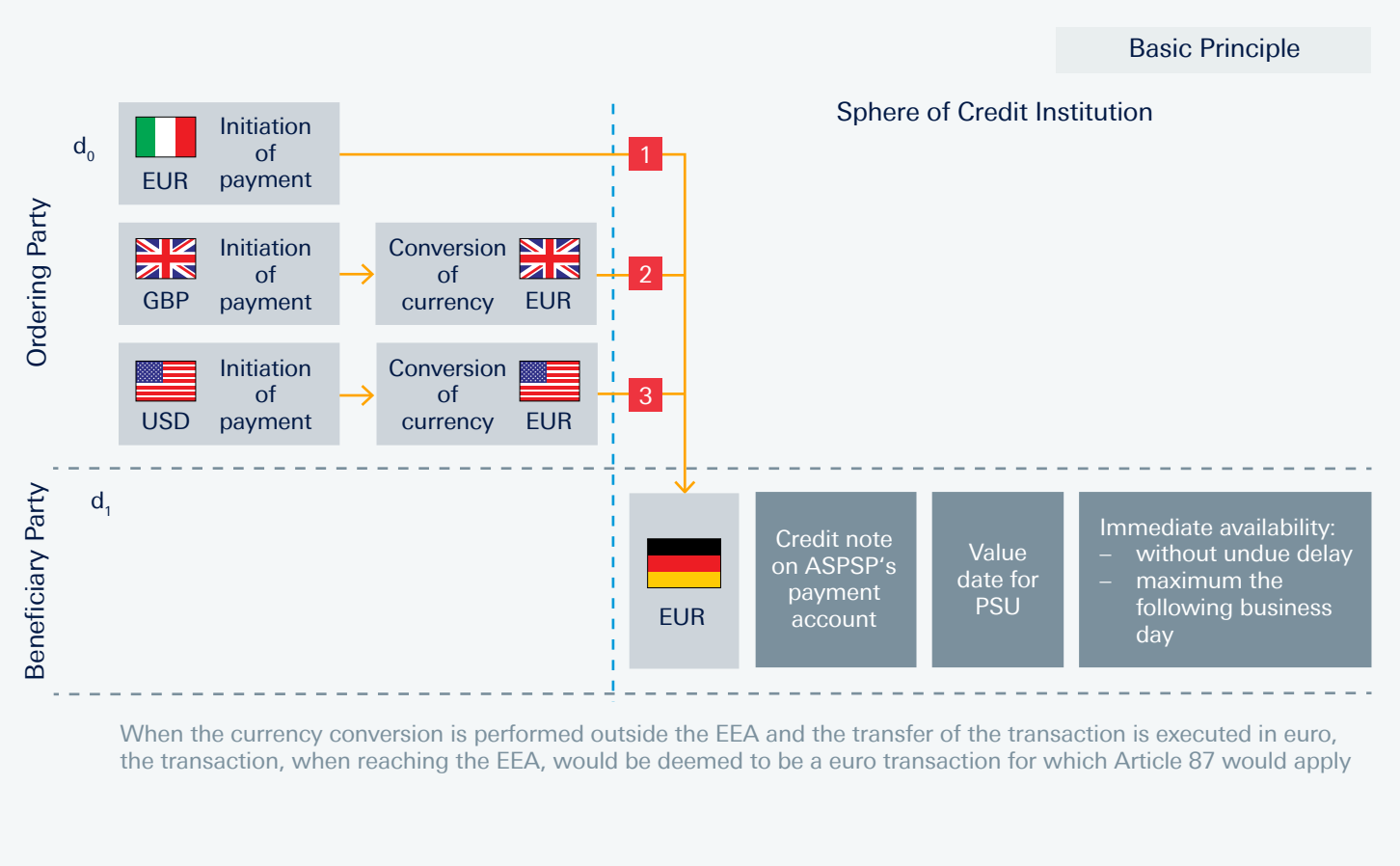


Fig. 17 Incoming transactions without currency conversion on the beneficiary side. For illustration purposes only.

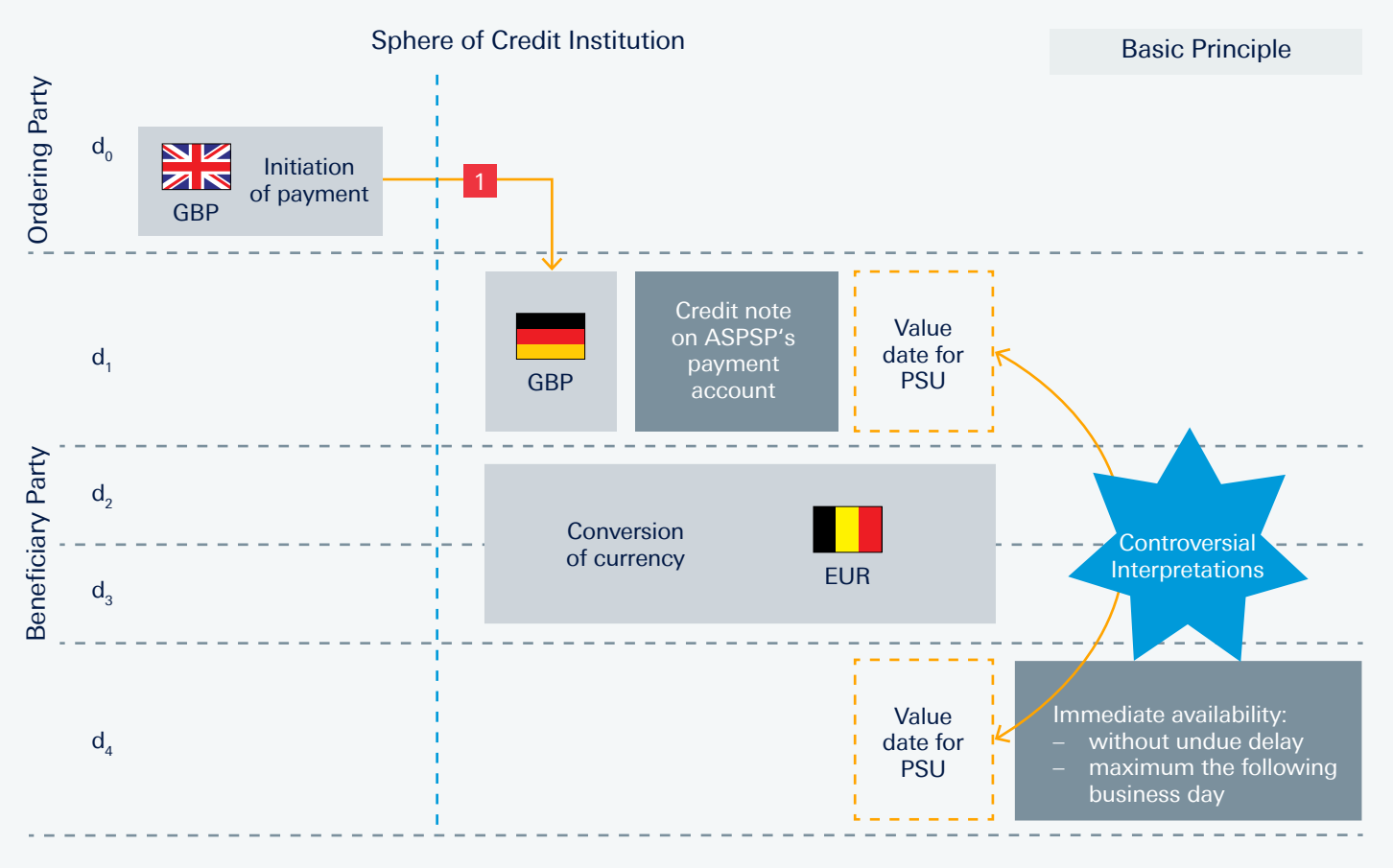


Fig. 18: Incoming transactions with currency conversion from EEA-Currency. For illustration purposes only.

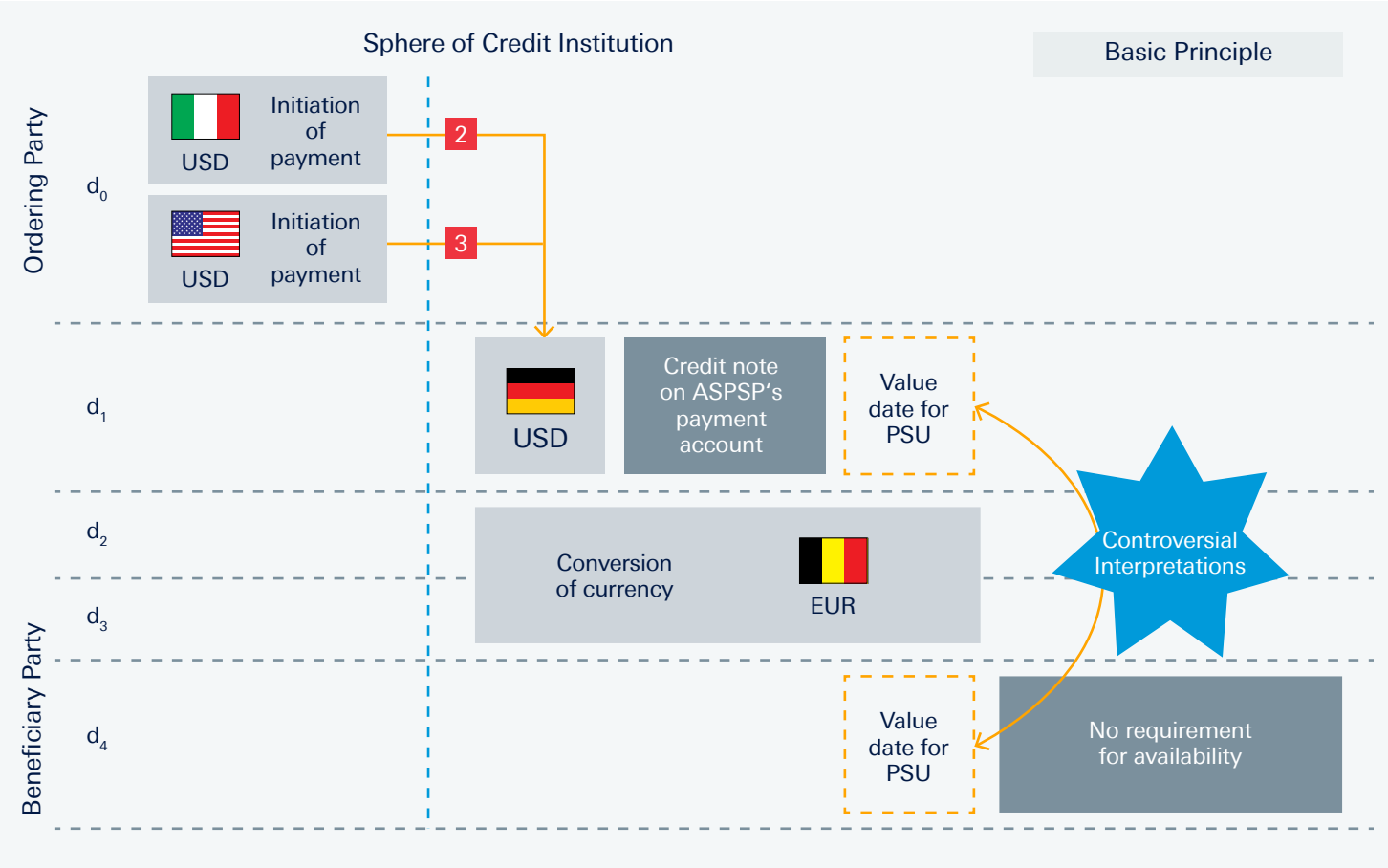


Fig. 19: Incoming transactions with currency conversion from non-EEA currency. For illustration purposes only.

4 The impact of introducing Third Party Providers (TPPs)

The third major change made by PSD2 is to license and regulate the new market entrants or Third Party Providers (TPPs) – capturing the new payment channels and services that have emerged since PSD1 was adopted, especially in the areas of internet payments and online account services. Payment initiation services have evolved in e-commerce, while at the same time technology has enabled a range of complementary services such as account information services. As neither of these new types of provider were subject to PSD1, they have so far not been subject to supervision.

PSD2 closes this gap by introducing two categories of TPPs: payment initiation service providers (PISPs) and account information service providers (AISPs). Each has its own type of business model, with Figure 20 showing how a PISP operates, and Figure 21 how an AISP operates – Illustrating the key differences between the two.

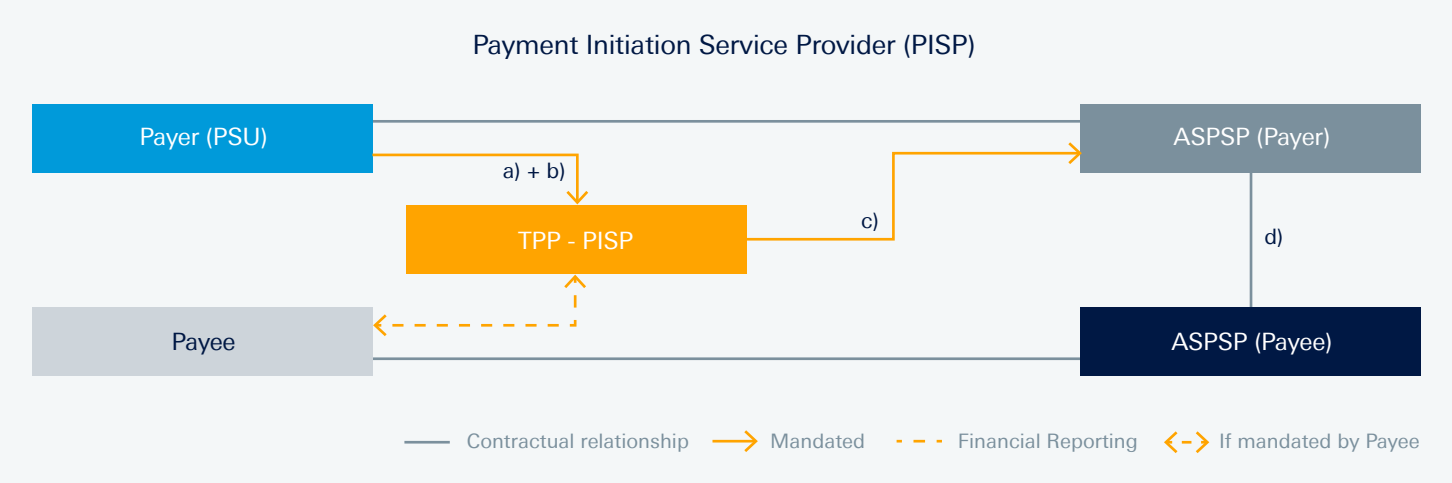


Fig. 20: Process overview PISP. For illustration purposes only.

The PISP process involves the following steps:

a) A PSU agrees the terms and conditions of a PISP,

b) The PSU mandates the PISP to initialise a payment,

c) The PISP communicates the payment order to the PSU's ASPSP,

d) The ASPSP executes the payment transaction initiated by the PISP on behalf of the PSU.

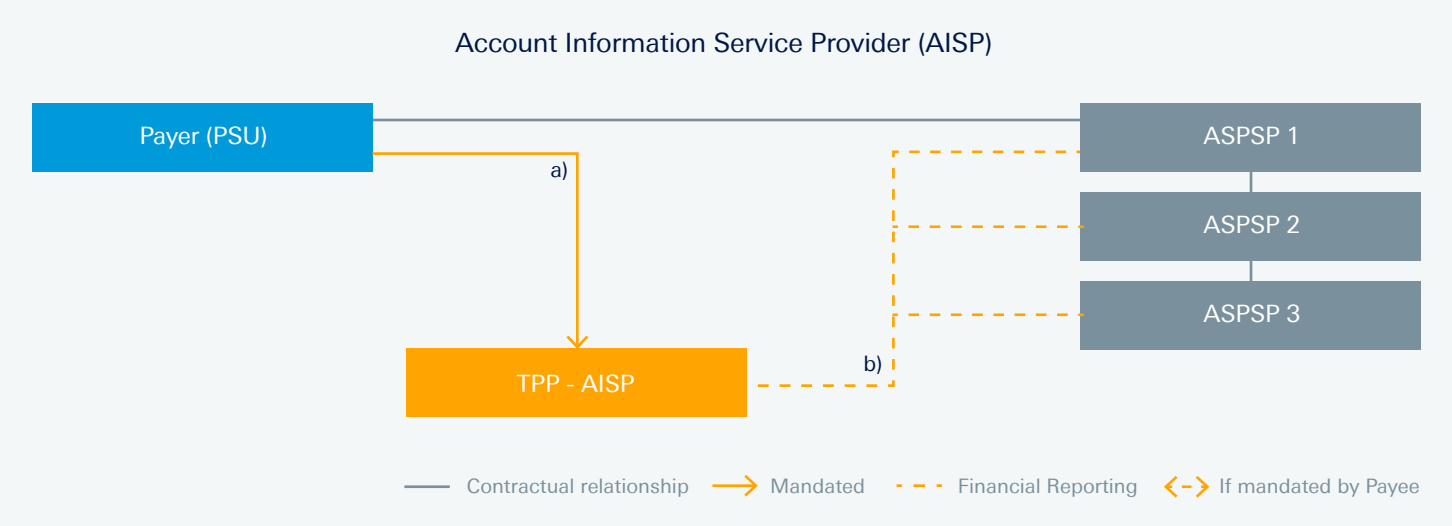


Fig. 21: Process overview AISP

The AISP process involves the following steps:

a) A PSU grants an AISP access to the information on his accounts held by one or several ASPSPs,

b) Acting on behalf of the PSU, the AISP reports the financial situation.

Rules for the execution of transactions with PISPs and AISPs

Scope of the definition of a TPP

The scope of the provisions governing TPPs is for online and mobile services. Machine-to-machine payments are regarded as not being within scope of the Directive although corporate clients using machine-to-machine payments may opt in to use TPP services.

Overlay banking services

It is not clear whether overlay banking services fall under PSD2's provisions governing TPPs. Overlay banking comprises multibank compatible services or software for example initiating payments on external accounts via MT101, or collecting account statements via MT940, and is a popular solution for corporate customers. If it is captured by PSD2's new provisions, one question would be whether it would have to use the new common interface, or would remain free to use existing channels including the SWIFT network. TPPs are obliged to provide authentication and communicate in a secure way, so were the SWIFT network to be officially recognised as a secure way of communicating, that would provide a satisfactory answer to the question.

Third party access

Access

Every ASPSP offering access to online payment accounts – having an online agreement with a customer, and having provided the customer with tools for online authentication – will have to be accessible to TPPs and to provide them with an online interface. There need not be any contractual relationship between a TPP and an ASPSP.

Communication, authentication and authorisation

In general, a TPP will have to identify itself to an ASPSP every time a payment is initiated, or for each communication session. The TPP will have to use the authentication method (credentials) agreed by the PSU and ASPSP for accessing a PSU's account. While the content of the ASPSP's response message has not yet been defined, the assumption is that this response will have to include the same information as the response in online banking (payment initiated, no payment executed).

The latest draft of the RTS suggests that the data formats used to exchange data should be based on ISO 20022, and that standard communication methods should be used.

Use of credentials by TPPs

Since TPPs are not allowed to view, store or save PSUs' credentials, ways must be devised to allow them to initiate payments without doing so. Two options are currently under discussion. The first sees a PSU entering the requested credentials (which could include a dynamic element) and the TPP receiving them and routing them straight on to the ASPSP. In the second, the TPP merely initiates the payment and is not involved in any way in the exchange of credentials. Authentication occurs exclusively between PSU and ASPSP, with the PSU entering the required credentials in the normal way, using the ASPSP's usual and trusted channel of communication.

Interface between ASPSPs and TPPs

With respect to the interface between ASPSPs and TPPs, the EBA will develop RTSs with more detailed requirements. While these are expected to be published in January 2017, based on the EBA's recent draft RTS, they are unlikely to define the interface's technical specifications. Discussions on these are ongoing among market participants.

Market participants currently emphasise the need for a single, common, non-ambiguous, European interface – ensuring that ASPSPs are able to communicate securely with TPPs and thus able to fulfil their regulatory obligations by TPPs access. At present, it is unclear whether there will be a single European interface, a number of national interfaces and an interface for each institution, or some kind of aggregation at different levels. Additionally, a standard communication protocol – common to all – needs to be defined and agreed in order to ensure interoperability among providers. While ASPSPs could in principle meet their legal obligations under the Directive by each building their own interface for TPPs, market participants do not consider this the best solution.

Non-discrimination

ASPSPs are prohibited from discriminating against AISPs or PISPSs in any way, for example by imposing additional costs on them or by delaying payment execution.

Information and transparency requirements and data protection

As both PISPs and AISPs access sensitive data they have to comply with strict information and transparency requirements. PSPs may only access, process and retain the personal data necessary to provide their payment services, and with the explicit consent of the PSU.

Furthermore, PISPs/AISPs are restricted from:

- storing PSUs' sensitive payment data, or
- requesting any data from a PSU other than those necessary to provide the payment initiation service, or
- using, accessing or storing any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer.

The EU General Data Protection Regulation (GDPR (EU) 2016/679), which will apply from May 25, 2018, will also have an impact on payment services.

Interface for confirming availability of funds to issuers of card-based payment instruments

While credit institutions remain the principal gateway for consumers to obtain payment instruments, the EU recognises the benefits – in terms of competition and increased consumer choice – of PSPs (whether credit or payment institutions) being allowed to issue card-based payment instruments, particularly debit cards. PSD2 therefore requires ASPSPs to provide a new interface through which they can confirm the availability of funds on their customers' accounts in response to requests made by PSPs who have issued card-based payment instruments, to aid issuers to better manage and reduce their credit risk. At the same time, that confirmation must not allow the ASPSP to block funds on the payer's payment account. PSD2 gives the following guidance on this new interface (Art. 65):

- The PSU's (payer's) underlying account has to be accessible online at the time of the request,
- The PSU (payer) must give explicit consent to his ASPSP to allow it to respond to a specific request from a PSP/CISP confirming that the specified amount (corresponding to a proposed card-based payment transaction) is available on the payer's payment account,
- The PSU (payer) initiates the card-based transaction triggering the underlying process (for a detailed process overview, please see Figure 22 below),

– The PSP/CISP must comply with secure communication standards. Authentication via a secure communication channel is required prior to each confirmation request.

The following summarises the operating business model of this new interface, as defined so far:

1. a) The payer signs an agreement with a PSP/CISP that offers an alternative debit card and the PSP/CISP issues the payer a new debit card with the necessary credentials (PIN code = strong authentication),

   b) The payer gives consent to his ASPSP, identifying the PSP/Card-based Payment Instrument Issuer (CISP) to whom his ASPSP is to give an answer on availability of funds when requested.

2. At the merchant's point of sale (POS), the payer initiates the card payment by entering his PIN code (strong authentication).

3. The merchant's PSP requests confirmation of the availability of funds by the PSP/CISP issuing the payment card.

4. The PSP/CISP requests confirmation of availability of funds from the payer's ASPSP holding the payer's account.

5. The payer's ASPSP gives a simple yes/no answer concerning the sum specified to the PSP/CISP.

6. The PSP/CISP sends the answer to the merchant via the merchant's PSP, and the card transaction at the POS can either be concluded, or - in the case of insufficient funds - denied.

Meanwhile, if agreed with the payer, his/her ASPSP sends the information that there has been a request of confirmation of availability of funds from a specific PSP/CISP, and what answer was given.

There is, as yet, no process for blocking such a card, and it is unclear whether a PSU is able to block a card by alerting either the ASPSP or the PSP/CISP.

Figure 22 below provides an overview of the operating business model as defined so far.

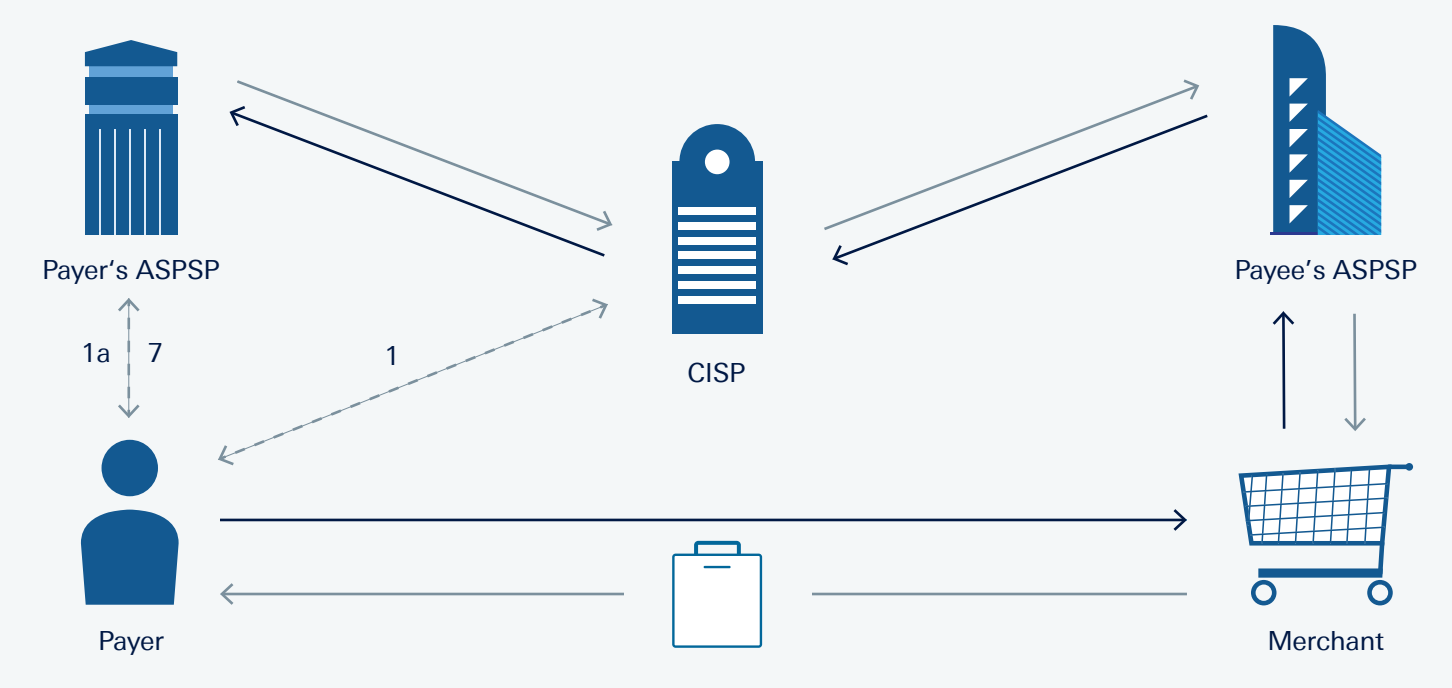


Fig. 22: Process overview PSP/CISP. For illustration purposes only.

Liability of Third Party Providers for processing errors

Where a payment order has not been executed properly, the ASPSP is initially deemed responsible for any processing error, and the ASPSP holding the client´s account must immediately refund the transaction amount to the payer's account, regardless of who is ultimately found liable: the TPP or the ASPSP. Yet the burden of proof subsequently falls on the TPP to show the payment process was valid.

Having to refund any sums paid in error upfront means ASPSPs conducting business with TPPs must carry out continuous risk assessments and manage risks such as interest rate and liquidity risk in case a TPP found liable for an error is unable to pay.

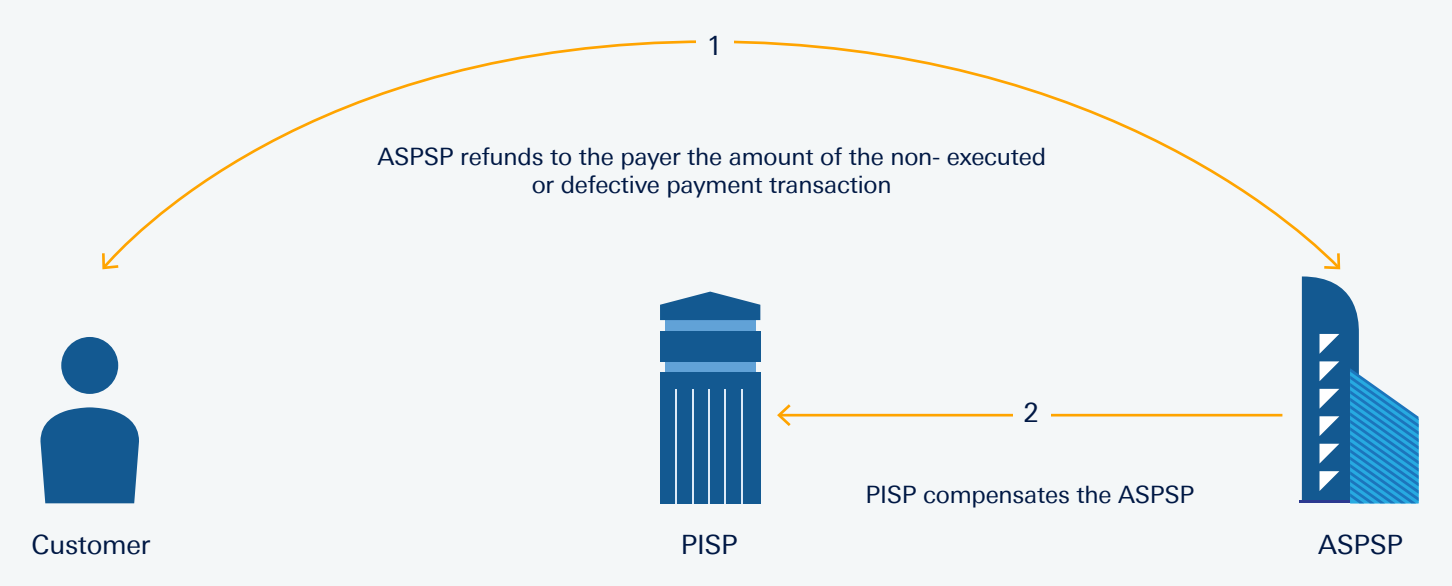


Fig. 23: Dispute procedure in case of non-executed or defective payment transactions through a PISP

Incorrect payment execution due to an incorrect Unique Identifier

In case of incorrect payment execution due to an incorrect unique identifier (e.g. a PSU uses the wrong IBAN) the PSP shall support the PSU in initiating a refund. Refusing to give information on grounds of data protection is not permitted.

The payer's PSP shall make reasonable efforts to recover the funds involved in the payment transaction. The payee's PSP shall cooperate in those efforts, including by giving the payer's PSP all the information required to collect the funds.

If collection of the funds is not possible, the payer's PSP shall provide the payer upon written request all available information relevant for the payer to file a legal claim for recovery of the funds.

Liability for unauthorised payments

PSD2 sets out the following rules concerning liability for unauthorised payments.

The payer may be obliged to bear the loss 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. But if the payer was acting fraudulently or failed to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence, the maximum shall not apply and the payer shall bear all losses.

If a customer disputes a payment despite the credentials being correctly entered and a secure method of authentication being used, the ASPSP will consider this a case of fraud. The customer's request for a refund can be blocked and the standard fraud investigation procedures initiated including a report to the relevant national authority.

Where the payer's PSP does not require strong customer authentication, the payer shall not bear any financial loss unless he/she has acted fraudulently. Where the payee – or the payee's PSP – fails to accept strong customer authentication, it shall refund any financial damage caused to the payer's PSP.

Also, where there is an unauthorised payment transaction, the payer's PSP must refund the amount of the unauthorised payment transaction to the payer immediately, and in any event no later than by the end of the business day following the PSP noting or being notified of the transaction. An exception is where the payer's PSP has reasonable grounds to suspect fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer's PSP 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.

A PSP may agree to vary the provisions concerning liability with corporate clients, although that liability may also be reduced by the exercise of a Member State Option (see Annex 2).

Conclusion

PSD2 provides a major update of payment market regulation in the EU/EEA. It extends the Directive's application both geographically – to payments where only one PSP is located in the EU/EEA area – and to payments in all official currencies, not just those of EU member states[11].

It initiates "strong" – 2-factor – customer authentication and increases other security and data protection measures for electronic payments. Finally, it ushers in licensed third party providers to the EU/EEA payments market, albeit with closely defined remits to offer specific payment–related services.

The changes brought about by PSD2 will impact financial institutions' operations and value chains in many ways. For example, when processing outgoing transactions, multiple adaptations may be required to meet each of the following requirements:

- allowing PISPs access to customer accounts,
- in international transactions, following the new rules for currency conversion, value dating and making funds available to PSUs,
- where appropriate applying the one-leg principle,
- allowing AISPs access to customer account information,
- adapting charges and fees,
- following the new rules regarding information giving and transparency, refunds, consumer liability and dispute settlement.

While none of this fundamentally alters the activities of financial institutions offering payments and servicing customer accounts, its impact – and the work that will be required to implement PSD2 – will be considerable. Processes and systems will have to be adapted to take into account all the new rules, for example regarding currency conversion, value dating and availability of funds in international payments. 2-factor authentication will have to be introduced in any electronic payment systems where it is not yet in use, and customer accounts will have to be made accessible to TTPs via a new third party interface, the details of which are yet to be finalised.

Some areas of PSD2 will receive clarification by the issuance of ITS, RTS and Guidelines, and there are provisions whose final form may be influenced by market advocacy. That said, much of the technical specification – for example for the new third party interface, and of standard communication protocols to ensure interoperability – is likely to be agreed among market participants.

PSD2 should be welcomed as a clear indication that the EU wishes to be at the heart of a digital payments era already well underway across the globe. Its implementation should eventually help level the playing field across the EU payments market, while at the same time encouraging competition and increasing consumer protection. We therefore approve of both its objectives and thrust and aim to play a positive role in its implementation.

[11]Certain provisions of PSD2 are excluded from the extension of scope to all currencies and to payments where only one PSP involved in the transaction is located in the EU/EEA, including the provision on amounts transferred and amounts received ("full amount principle", Art. 81), and the provision on payment transactions to a payment account ("maximum execution time", Art. 83.1).

Annex

1 Payment Services

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account. The following is a list of payment services (as referred to in point (3) of Article 4) now included in PSD2 previously excluded from PSD1 or of uncertain status.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's PSP or with another PSP:
   a) execution of direct debits, including one-off direct debits
   b) execution of payment transactions through a payment card or a similar device;
   c) execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a PSU:
   a) execution of direct debits, including one-off direct debits;
   b) execution of payment transactions through a payment card or a similar device;
   c) execution of credit transfers, including standing orders.

5. Issuing of payment instruments and/or acquiring of payment transactions.

6. Money remittances.

7. Payment initiation services.

8. Account information services.

2 Member State Options

This section sets out the options granted to Member States when transposing PSD2 into national law. Decided at local level, the following table lists all Member State Options, citing the relevant articles (of both PSD1 and PSD2) and summarising their content.

1 Title I – Member State Options

PSD1	PSD2	
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 => a special purpose institutions Extract of DIRECTIVE 2013/36/EU Art. 2.5 No. 2-23: (4) in Belgium, the Institut de Réescompte et de Garantie/ Herdiscontering-en Waarborginstituut; (6) in Germany, the Kreditanstalt für Wiederaufbau, undertakings which are recognised under the Wohnungsgemeinnützigkeitsgesetz as bodies of State housing policy and are not mainly engaged in banking transactions, and undertakings recognised under that law as non-profit housing undertakings; (10) in Spain, the Instituto de Crédito Oficial; (11) in France, the Caisse des dépôts et consignations ; (12) in Italy, the Cassa depositi e prestiti; (16) in the Netherlands, the Nederlandse Investeringsbank voor Ontwikkelingslanden NV, the NV Noordelijke Ontwikkelingsmaatschappij, the NV Industriebank Limburgs Instituut voor Ontwikkeling en Financiering and the Overijsselse Ontwikkelingsmaatschappij NV; (17) in Austria, undertakings recognised as housing associations in the public interest and the Österreichische Kontrollbank AG;

2 Title II – Member State Options

PSD1	PSD2	
Article reference		Description
7 (3)	8 (3)	Derogation for MS not to apply the calculation of own funds (Art. 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 § 1.
22 (3)	24 (3)	MS may apply this Article taking into account, mutatis mutandis, Article 53 to 61 of Directive 2013/36/EU. à Professional secrecy.
	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.

3 Title III – Member State Options

PSD1	PSD2	
Article reference		Description
30 (2)	2 (5)	Extension of the scope, as microenterprises should be considered equally to consumers
33 (optional)	Manda-tory	PSP has to prove that its compiling with the defined information requirement
34 (1) & (2)	42 (2)	Frame for derogation from information requirements: – Reduction or increase of transaction amount or spending limits – Increase to EUR 500 specifically for prepaid payments
45 (6)	55 (6)	Opportunity to provide more favourable conditions (charges & duration) for PSUs, in regard to the termination of framework contracts
47 (3) 48 (3)	57 (3) 58 (3)	Information on individual payment transactions should be provided to payers and payees, free of charge, on paper or on another durable medium at least ones a months

4 Title IV – Member State Options

PSD1	PSD2	
Article reference		Description
51 (2) and (3)	Article 61 (2) and (3)	MS may provide that Article 102 [ADR procedures] 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 may provide for shorter maximum execution times than those provided for in this section.
	Article 101 (2) 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.

5 Title V – Member State Options

No Member State Options have been introduced within Title V.

6 Title VI – Member State Options

PSD1	PSD2	
Article reference		Description
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.