The revised Payment Services Directive (PSD2)

Information meeting for banks
The revised Payment Services Directive (PSD2)

Information meeting for banks

Introduction

Anne Demelenne
Febelfin
Introduction


- **13 January 2018**: official deadline for transposition into national law.

- **Lack of certainty** however, about the **exact timing** for the approval and coming into effect of the PSD2 and EBA Regulatory Technical Standards (RTS) and guidelines.
Overview of progress of EBA mandates under PSD2
Introduction

- The various **texts are not clear. Interpretation is difficult** and can differ from one bank to another.

- Taking the **commercial space of each individual bank** into account.
Goldplating: “Member States may …”

- The PSD2 contains 21 goldplating options for its transposition by the Member States.
- A cornerstone for equal terms of competition in all of the Member States (Level Playing Field) and for all stakeholders.
Time to analyse and prepare …
Programme

9:15 – 10:00  Scope and Objectives
Ingrid Vanweddingen, KBC Bank

10:00 – 10:45  Third Party Providers: Who, what, how and the potential impact on banks
Begoña Blanco Sanchez, ING Belgium

10:45 – 11:00  Coffee break

11:00 – 11:30  Rights, obligations and liabilities of the parties
Christine Defechereux, BNP Paribas Fortis

11:30 – 12:00  Security and Regulatory Technical Standards
Pascale Brien, EBF

12:00 – 12:15  Other provisions
Camille Carlier, Febelfin

12:15 – 12:30  Q&A
The revised Payment Services Directive (EU) 2015/2366

Objectives and Scope

Ingrid Vanweddingen
KBC Group NV, Group Legal
Senior Legal Adviser, Company lawyer
PSD2 – Key changes
1. Key changes

### PSD1 - Focus

- the establishment of a single EU market in payment services - consistency between national rules
- applies to all types of payment services carried out in EU currencies within the EU
- transparency of conditions and information requirements for payment services
- a clear description of the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services
- focus on consumer protection

### PSD2 - Focus

- extension of the scope to “one-leg transactions” and “two-legs transactions” in non-EEA currencies
- focus on electronic payments: cards, online and mobile payments
- strengthen the security of electronic payments – introduce and define the concept of strong customer authentication
- inclusion of new players on the market: TPP’s (PISPs and AISPs). Non-discriminatory access. **The most controversial aspect of the Directive!**
- strong emphasis on transparency and consumer protection
Timeline for implementation
2. **Timeline**

- **25/11/2015**: Approval of PSD2
- **23/12/2015**: PSD2 published in the Official Journal
- **12/01/2016**: Entry into force of PSD2
- **13/01/2017**: Deadline for EBA to submit draft RTS to the Commission (delegated act)
- **2017**: Adoption by the Commission of the RTS → Regulation entry into force 20d of its publication
- **13/01/2018**: Deadline for transposition of PSD2 into national law
- **2018**: Entry into force of the security measures referred to in the Articles 65, 66, 67 and 97 of PSD2

Entry into force of the security measures referred to in the Articles 65, 66, 67 and 97 of PSD2 18 months after entry into force of the RTS – October 2018?
3 mandates to EBA
3. Mandates EBA

- PSD2 confers 11 mandates to EBA.
- 3 of which relate to draft Regulatory Standards and Guidelines to ensure the establishment of adequate security measures for electronic payments.
- EBA shall develop in close cooperation with ECB draft RTS addressed to PSP specifying:
  - Strong customer authentication + exemptions
  - Requirements for common and secure open standards for the purpose of identification, authentication, notification, implementation security measures (…)

PSD2 - 15/11/2016
3. Mandates EBA

- European passport payment institutions
- RTS on authentication and communication
- Guidelines on security measures + certification processes
- Operate a central register list of the names of the entities providing payment services
- Guidelines on the complaints procedures
- Guidelines on classification major incidents + Notification templates and procedures
Subject matter and scope
4. Categories of payment service providers

The categories under PSD I remain.

Extension:

- payment initiation service providers;
- account information service providers;
- payment service provider issuing card-based payment instruments.

→ New payment institutions
4. Payment services

Payment services are defined in the Annex 1 to the Directive, and cover activities that most banks operating in the market are involved in.

The key activities listed are as follows:

- Cash placed and withdrawn on/from a payment account
- Execution of payment transactions
  - Credit transfers, including standing orders
  - Direct debits, including one-off direct debits
  - Payment card transactions
4. Payment services

- issuing and / or acquiring of payment instruments
- money remittance

Extension:

- payment initiation services;
- account information services;
Extension of the territorial scope and currencies
5. Territorial scope

© EBF

[Image of a map showing the territorial scope of the EU and non-EU member states, including Iceland, Norway, and Liechtenstein.]
5. Territorial scope and currencies

PSD II shall apply to intra-EEA payments and payments in EEA-currencies (euro and currency of a member state) = PSD1.

But the scope of PSD II is extended to:

1. Two legs intra-EEA non-EEA currency transactions;

   Example: a USD payment within the EU from the UK to FR

2. One-leg in and out payments to non-EEA countries regardless of currency used, in respect to those parts of the payments transaction which are carried out in the Union;

   Examples: One-leg out transaction in an EU-currency:
   - a EUR payment transaction from France to Japan
   - a CHF payment transaction from Liechtenstein to Switzerland.
5. Territorial scope and currencies
5. Territorial scope and currencies

Extension of the scope of PSD2

Article 2: Scope

GEOGRAPHICAL SCOPE

Two Legs EEA

EEA (European Union, Iceland, Lichtenstein, Norway)

Full application of Title III and IV

One Leg EEA

PSD1

Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 4

Non EEA

Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 3

Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 4

Bron: © EBF - PSD2 GUIDANCE FOR THE IMPLEMENTATION OF THE PAYMENT SERVICES DIRECTIVE 2 Final 7th June 2016
5. Territorial scope and currencies

- Art 45 (1)(b) single payment transactions - info on the maximum execution time for the payment service to be provided
- Art 52 (2)(e) framework contract – info on the maximum execution time for the payment service to be provided
- Art 56 (a) framework contract - the maximum execution time;
- Art 81-86 amounts transferred and amounts received + execution times
- Remark: No exception for the value date!
5. Territorial scope and currencies

Titel III and IV apply to one-leg payment transactions regardless of the currency used except for:

- Art 45 (1)(b) single payment transactions - info on the maximum execution time for the payment service to be provided
- Art 52 (2)(e) and (f) framework contract - information on the maximum execution time + information with regard to the refund right (Art 67-68)
- Art 56 (a) framework contract - information on the maximum execution time
- Art 62 (2) and (4) on the interchange fees
- Art 76 and 77 refunds for payment transactions initiated by or through a payee (refund) + request for a refund
- Art 81 amounts transferred and amounts received
- Art 83(1) execution times – amount of the payment transaction to be credited to the payee’s PSPs account by the end of the following business day (D+1)
- Art 89 payment service providers’ liability for non-execution, defective or late execution of payment transactions
- Art 92 right of recourse
5. Impact of the extension of the scope of PSD2

Impact on

- Information requirements

Consequences

- Shall apply to two legs intra-EEA non-EEA currency transactions and the one-leg in and out payments to non-EEA countries regardless of currency used. There are some exceptions cf. supra.

- The information requirements under PSD I are mainly unchanged.
5. Impact of the extension of the scope

Impact on

• Charges

Consequences

• PSD I: for payment transactions within the Union (two legs) in euro or a EU-currency without any currency conversion SHA shall apply.

• PSD II: for all payment transactions provided within the Union (two legs) SHA shall apply regardless of the currency used and regardless of any currency conversion. For one-leg in/out transactions BEN and OUR remain possible.
5. Impact of the extension of the scope

<table>
<thead>
<tr>
<th>Impact on</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surcharging</td>
<td>• Different national practices → extreme heterogeneity market → confusion for consumers in particular in the e-commerce and cross-border context.</td>
</tr>
<tr>
<td></td>
<td>• PSD II: no surcharging for the use of payment instruments for which interchange fees are regulated under the IF Regulation (EU) 2015/751 and for payment services to which the End dates Regulation (EU) No 260/2012 applies</td>
</tr>
<tr>
<td></td>
<td>⇒ prohibition for more than 95% of the card market.</td>
</tr>
</tbody>
</table>
5. Impact of the extension of the scope

Impact on

• Execution times

Consequences

• Not applicable on two-legs payment transactions in a non-EEA currency;

• Apply to one-leg in/out transactions regardless of the currency used in respect to those parts of the payments transaction which are carried out in the Union.

Example: a payment transaction
- in EUR from France to Japan;
- in USD from the UK to USA;
- in EUR from Japan to Belgium.
5. Impact of the extension of the scope

<table>
<thead>
<tr>
<th>Impact on</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value date</td>
<td>• Shall apply to all payment transactions two legs and one leg in/out regardless of the currency used.</td>
</tr>
</tbody>
</table>

→ 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 in for example $ is credited to the payee’s payment service provider’s account.

• 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 on its account where, on the part of the payee’s payment service provider, there is:

(a) no currency conversion
Example: a proper payment transaction in euro
(b) a currency conversion between the euro and a Member State currency or between two Member State currencies
Example: there is a currency conversion between the £ and the Danish crown.
Payment initiation in GBP by PSU → Debit account PSU → Incoming payment in GBP on account ASPSP → Currency conversion EUR → Immediate availability of funds on account PSU
Payment initiation in $ by PSU

Incoming payment in $ on account ASPSP

Currency conversion EUR

No availability requirement

• credit value date for the PSU account
Negative scope
6. Main exemptions and changes

Scale back of the existing exemptions. Changes to:

- **Commercial agents exemption:** requirement for commercial agent to put in place a formal agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee.

- **Limited network exemption:** restriction to instruments that meet one of the following conditions:
  
  • 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 → no intermediaries;
  
  • used only to acquire a very limited range of goods or services → “very limited” remains unclear;
  
  • valid in a single Member State to acquire specific goods or services regulated by a public for specific social or tax purposes

Examples: client cards, mobility cards, fuel cards, luncheon vouchers
6. Main exemptions and changes

- Telecommunication exemption:
  payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services:

  (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 is limited to EUR 50 and cumulatively to not more than 300 EUR/month.

Example: purchase of a transport ticket or a ticket for a cultural event.

- Automated teller machines:
  Exemption maintained. But ATM operators will have to give information on withdrawal charges.
Time to get ready for PSD2
PSD2 & the Third Party Providers (TPP’s)

15/11/2016

Begoña Blanco Sanchez
Expert Payments/Product management
ING Belgium
Agenda

- What’s a TPP?
- How a TPP will be able to perform its activity?
- Obligations and responsibilities of a TPP
- Specific obligations for PISP
- Specific obligations for AISP
- EBA authorisation & registration
- Transitional period for existing entities
Players on the market: who is who?

- PISP: Payment initiation Service Provider
- AISP: Account Information Service Provider
- CISP: Card based payment Instrument Issuer Service Provider
- TPP: Third Party Provider
- PSP: Payment Service Provider
- PSU: Payment Service User
- Payer: natural or legal person who holds a payment account & allows a payment order from that payment account or, where there is no payment account, a natural or legal person who gives a payment order
- Payee: natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction.
- ASPSP: Account servicing Payment Service Provider
- PI: Payment Institution
What's a TPP?

TPP is a Legal entity performing activities of:

- Payment Initiation Services
- Account Information Services

✓ A 3rd party payment transaction is a transaction involving a payer, a payee and a 3rd party player who will initiate a payment for a purchase in the name of the customer (the payer)

✓ Payer: natural or legal person who holds a payment account & allows a payment order from that payment account or, where there is no payment account, a natural or legal person who gives a payment order

✓ Payee: natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction.
Types of TPPs

- **PISP** “Payment Initiation Service Provider”
  Legal entity offering initiation of payment on behalf of the PSU

- **AISP** “Account Information Service Provider”
  Legal entity offering account information services to a customer (Account aggregation)
  They can typically provide services offering cross banks account information

- **How?**
  Making use of the online banking infrastructures
  (ASPSP’s will provide same service level as the service they offer today through their channels)

- The account owner has to be informed & give explicit consent.

NB: no obligation to enter in a framework contract with the ASPSPs.

-> impacts on existing contracts?
Obligations & responsibilities of a TPP

- Have to register its business with the competent authority (in Belgium, the National Bank)
- License to operate
- Authorisation for the PISP & Registration for the AISP in the home member state and EBA
- Meet same security requirements as Payment/Credit Institutions
- Make available & comprehensive information in easily accessible manner
  - Service offered, name, geographical address
  - Electronic mail address for the communication with the customer

- Have to hold a profesional indemnity insurance or comparable guarantee against their liability towards the bank and the user of their services
Obligations & responsibilities of a TPP

- Personalized credentials not accessible to other parties & that when transmitted, in safe and efficient channels
- Explicit consent from the client
- Communication in a secured way between payer & payee with the standards of EBA
  - Sensitive data
- not store sensitive payment of the PSU or account data of the Payment account

✓ Payment account: account held in the name of one or more payments service users which is used for the execution of payment transaction
Specific obligations for PISP

Explicit consent of the PSU.

- not hold the PSU’s funds at any time
- ensure that the credentials of the PSU are not accessible to other parties and that they are transmitted through safe and efficient channels
- ensure that any other information about the PSU is only provided to the payee and only with explicit consent of the PSU
- identify itself towards the ASPSP and communicate with the ASPSP, the payer and the payee in a secure way every time a payment is initiated (RTS)
- not request from the PSU any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer (only request pertinent data)
- (not store sensitive data)
- not modify any feature of the transaction (amount, payee...)
Specific obligations for PISP

Immediately after payment initiation, the PISP should:

- Confirm the successful initiation of the payment order
- Specify the amount of the purchase & when applicable charges linked to the payment
- The PSU has to receive this confirmation
- TPP will have to prove that the transaction was authorised by the PSU
- If TPP is liable for the unauthorised transaction, shall immediately compensate the bank any losses incurred or sums paid as a result of the refund to the payer (including the amount of the unauthorised transaction)
Specific obligations for AISP

Explicit consent of the PSU.

- ensure that the credentials of the PSU are not accessible to other parties and that they are transmitted through safe and efficient channels.
- identify itself towards the ASPSP and communicate with the ASPSP (RTS)
- access only the information from designated accounts and associated transactions.
- Not request data other than for performing the account information service explicitly requested by the PSU in accordance with data protection rules (not store sensitive data, only request pertinent data, use data according to purpose).
EBA registration

- Guidelines on authorisation & registration of Payment institutions
- Consultation running until 3/2/2017
- “information & documentation to be provided to the national authorities by applicants to obtain authorisation as payment & electronic money institutions & Registration as AISP “
  - One of the objectives is to promote equal conditions for competition

- **3 separate sections**
  - Payment institutions
  - AISP
  - Electronic money institutions

- Examples: business plan, evidence of initial capital, internal control mechanisms, procedures in place to monitor, handle & follow up for security incidents, customer’s complaints ...
Transitional period for existing entities

- Legal persons having performed in their territories before 16/1/2016 activities of PISP or AISP to continue to perform the same activities in their territories during the transitional period.
- Transitional period = 13/01/2018 + 18 months of entry into force of the RTS.
Payment Services Directive 2

RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES

Christine Defechereux
BNP Paribas Fortis
The parties

1. Payment Service User: PSU

2. Account Servicing Payment Service Provider: AS PSP

3. TPP:
   a) Payment Initiation Service Provider (PISP)
   b) Account Information Service Provider (AISP)

4. Card Based Payment Instruments Issuers (CISP)
Obligations of the payment service user in relation to payment instruments and personalised security credentials (art 69)

Rem: Extension to “Personalised security credentials”

- 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;

- notification to the PSP (or the entity specified by the latter) the loss, theft, misappropriation or unauthorised use of the payment instrument.
Obligations of the payment service user in relation to payment instruments and personalised security credentials (art 69)

Take all reasonable steps to keep its personalised security credentials safe

- Extension to "Personalised security credentials"
- Personalized security features => Personalised security credentials
- Challenge to conciliate this obligation with use of the TPP’s service
Obligations of the payment service provider in relation to payment instruments (art 70)

- No access to the personalised security credential to parties other than the PSU entitled to use the payment instrument: what about the TPP’s?

- Refrain from sending an unsolicited payment instrument (except replacement)

- Ensure that appropriate means are available at all times to block/unblock the payment instrument (means to prove the notification)

- Provide an option to make the notification free of charge and to charge, if at all, only replacement cost directly attributed to the payment instrument.

- Prevent the use of the instrument after notification.

Bearing the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.
Notification and rectification of unauthorised or incorrectly executed payment transactions (art 71)

Cumulative conditions

- Without undue delay
- No later than 13 months after the debit date
Notification and rectification of unauthorised or incorrectly executed payment transactions (art 71)

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).

LIABILITY OF THE ASPSP.
Payment service provider’s liability for unauthorised payment transactions (art 73)

PSU can obtain rectification from the AS PSP in the event of unauthorized (or incorrectly executed) payment transactions

REFUND IMMEDIATELY

“and no later than by the end of the following business day”, after noting or being notified of the transaction,

except suspicion of fraud communicated the relevant national authority.

same rule apply when the transactions is initiated through a PISP

The PISP will have to prove that the transaction was authenticated, accurately recorded, and not affected by a technical breakdown.

Recourse available if the PISP denies any wrong doing ?
Payer’s liability for unauthorised payment transactions (art 74)

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.

Lost/Stolen/Misappropriation of a payment instrument

Liability limited to EUR 50 => currently EUR 150.

Member state can lower this amount ( ... the payer may be obliged... OR MAY NOT !)
Payer’s liability for unauthorised payment transactions (art 74)

2 exceptions

Loss, theft or misappropriation (...) not detectable to the payer prior to a payment

Acts of lacks of action of an employee, agent or branch of a PSP

Third exception: the payer is not liable (and the amount of EUR 50 does not apply) if the PSP does not require a STRONG CUSTOMER AUTHENTICATION
Obligation towards CISP: confirmation on the availability of funds (art 65)

CISPs: Card Based Payment Instruments Issuers:

For the CIPS, obtaining confirmation of availability of funds from the ASPSP reduces its credit risk.

The ASPSP is only obliged to provide the confirmation IF
• the accounts are electronically accessible.
• the payer has given explicit consent to its ASPSP to respond
• the consent must be given before the 1st request for confirmation.

The confirmation is YES or NO answer.

The confirmation shall not allow the ASPSP to block the funds on the payer’s account.

Not Applicable for card-based payment transactions initiated through electronic money.
Rules on access to payment account in the case of payment initiation services (art 66)

The PSU have the right to use PISP in relation to payment account accessible online.

Condition: Explicit consent of the PSU.

The PISP has the following obligations:

- not hold the PSU’s funds at any time
- ensure that the credentials of the PSU are not accessible to other parties and that they are transmitted through safe and efficient channels
- ensure that any other information about the PSU is only provided to the payee and only with explicit consent of the PSU
- identify itself towards the AS PSP and communicate with the AS PSP, the payer and the payee in a secure way every time a payment is initiated => RTS
- obligations related to data (not store sensitive date, only request pertinent data, use data according to purpose
- not modify any feature of the transaction (amount, payee...)
Rules on access to payment account in the case of payment initiation services (art 66)

The AS PSP has the following obligations:

- Securely communicate with PISP => RTS.
- Immediately provide to the PISP all information on the initiation of the payment transaction and on the execution of the transaction.
- Treat payment order without discrimination.

Contractual relationship? nor mandatory nor prohibited.
Rules on access to payment account in the case of account information services (art 67)

The PSU have the right to use AISP in relation to payment account accessible online.

Condition: Explicit consent of the PSU.

The AISP has the following obligations:

- ensure that the credentials of the PSU are not accessible to other parties and that they are transmitted through safe and efficient channels.
- identify itself towards the AS PSP and communicate with the AS PSP => RTS
- access only the information from designated accounts and associated transactions.
- obligations related to data (not store sensitive data, only request pertinent data, use data according to purpose).
Rules on access to payment account in the case of account information services (art 67)

The AS PSP has the following obligations:

- Securely communicate with PISP => RTS.
- Treat payment order without discrimination.

Contractual relationship ? nor mandatory nor prohibited.
Limitation to the access to account (art 68)

The AS PSP can deny access to a payment account for an PISP or an AISP for objectively justified and duly evidenced reasons relating to unauthorised access to payment account.
To be continued …
Security – PSD2 level 2 measures

Pascale-Marie BRIEN
European Banking Federation
Senior Policy Adviser Payment
Coordinator Digital Agenda

15/11/2016
Security challenges for the banking industry

MILESTONES

PSD2 was adopted on 8th October 2015, it updates PSD1 and must be implemented in National laws by January 2018

Draft RTS published on 12th August was open for consultation until 12th October – will not be implemented before October 2018
Security challenges for the banking industry

Strong Customer Authentication but

TPPs have access to security credentials

Whereas the customer must keep his/her credentials safe and not transmit them to third parties...

How can a customer distinguish a “good” TPP from a fraudster on the internet?
Security challenges for the banking industry

Banks must reimburse in all circumstances “first port of call”

Even if the unauthorised transaction was initiated by a third party

No contract between banks and TPPs
PSD2 level 2 measures – EBA RTS

- **Strong customer authentication and exemptions**
  - Exemptions limited to contactless 50€ (max) and remote 10€ (max)
  - Quid parkings, tollways? Quid customer experience?
  - Liability shift ends in October 2018
  - Segregation of channels within mobile

**EBF proposals**

- Include contact payments in exemptions
- Revert to a risk based approach to give agility to react to fraud trends
- Maintain liability shift as stated in PSD2 (article 74.2)
PSD2 level 2 measures – EBA RTS

- Secure communications between banks and TPPs
  - Development of common solutions to allow all players to communicate in a secure manner
  - The EBA and the ECB are working on building the appropriate framework

EBF proposals

- Legally binding and pan-European register 24/7/365 (real-time check of status)
- Mutual authentication through electronic seals based on certificates
- May be based on the provisions of the eIDAS Regulation
PSD2 level 2 measures – EBA RTS

Secure identification of TPPs by the public

- Trust marks issued by a certification body (LEI foundation?)
- Trust marks withdrawn if certification is withdrawn

Governance structure to ensure all participants receive the level of service they expect

- Develop and maintain standards
- Define and monitor the rights and responsibilities of all stakeholders
- Manage TPPs certification and trust marks
- Offer dispute resolution mechanisms
What’s next?

- Hearing at EBA on 23rd September 2016
- Meeting at ECB on APIs for Payment Initiation Services 6th October 2016 (what about an umbrella agreement to secure the entire process?)
- Response on EBA draft RTS on 12th October
- Publication final RTS: Spring 2017 for implementation October 2018 at the earliest.
- Probable creation of a working group at the ECB
Any Question?

Pascale-Marie BRIEN, PhD
Senior Adviser, payments and digital
@PascaleBrien
Payment Services Directive 2

Other provisions of the PSD2

Camille Carlier
Febelfin
Other provisions of the PSD2

- Payment transactions where the transaction amount is not known in advance (Article 75 – new)
- Data protection (Chapter 4)
- ADR procedures for the settlement of disputes (Chapter 6)
Other provisions of the PSD2

- Payment transactions where the transaction amount is not known in advance (Article 75 – new)

- Data protection (Chapter 4)

- ADR procedures for the settlement of disputes (Chapter 6 – Article 99 to 103)
Payment transactions where the transaction amount is not known in advance

Article 75 (new)

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 PSP 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 PSP 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.
Payment transactions where the transaction amount is not known in advance

Preliminary comment

« Card-based payment transaction » is not defined into PSD2, but there is a definition into Regulation IFR 2015/751:
« a service based on a payment card scheme’s infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this result in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services » (art. 2 (7) Règlement IFR).
Payment transactions where the transaction amount is not known in advance

- Linked to the issue of reserved amount (gas stations, hotels, etc.).

The new disposition is actually based on a few problematics cases (on million cases) where funds were not directly released.

The implementation of this disposition will be difficult, mainly for the gas stations where the exact amount of the reservation is not known in advance and may vary based on the acquirer, the merchant, the card scheme, etc.

Solution? Indicate a maximum amount in the terms and conditions on accounts / cards / securities settlements?

Who bears the risk? The merchant or the bank?

- To be compliant, two options (under investigation):
  1) Adapt the mechanism of reserved amount.
  2) The merchant accepts the risk / liability (from a civil law perspective)
Other provisions of the PSD2

Payment transactions where the transaction amount is not known in advance (Article 75 – new)

Data protection (Chapter 4)

ADR procedures for the settlement of disputes (Chapter 6 – Article 99 to 103)
Data protection

• National law must permit processing of personal data by payment systems and PSP’s when necessary to safeguard the prevention, investigation and detection of payment fraud.

• The provision of information to individuals about the processing of personal data and the processing of such personal data shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.

• PSP’s shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the PSU (art. 94, §2) → important impact on the way the banks work.
Other provisions of the PSD2

- Payment transactions where the transaction amount is not known in advance
  (Article 75 – new)

- Data protection (Chapter 4)

- ADR procedures for the settlement of disputes (Chapter 6 – Article 99 to 103)
ADR procedures for the settlement of disputes

1) Complaint procedures

2) ADR procedures and penalties
ADR procedures for the settlement of disputes

1) Complaint procedures

2) ADR procedures and penalties
Complaint procedures

Complaints (art. 99)

- Member states must foresee procedures by the competent authority.
- Complaints are introduced by the consumers (including consumer organisations).
- The competent authorities must inform the complainant of the existence of the ADR procedures.
Complaint procedures

Competent authorities (art. 100)

• A competent authority must be designated to ensure the respect of the rules of the PSD2. The PSD2 gives more conditions than the PSD1.

Possible competent authorities?

1) Following the definition of Article 4 Regulation 1093/2010 establishing a European Supervisory Authority (European Banking Authority).

→ In BE: BNB, Federal Public Service Economy

2) Bodies recognised by national law or by public authorities expressly empowered for the exercise of control. They shall not be payment service providers (except for national central banks).
Complaint procedures

• The authorities shall possess all powers and adequate resources necessary for the performance of their duties.

• The competent authorities shall exercise their powers in accordance with national law either:
  (a) directly under their own authority or under the supervision of the judicial authorities; or
  (b) by application to courts which are competent to grant the necessary decision, including, where appropriate, by appeal, if the application to grant the necessary decision is not successful.

• In the event of infringement or suspected infringement of the provisions of national law transposing Titles III and IV, the competent authorities shall be those of the home Member State of the payment service provider.
  → Exception: for agents and branches conducted under the right of establishment where the competent authorities shall be those of the host Member State.
Complaint procedures

• Member States shall notify the Commission of the designated competent authorities. They shall immediately notify the Commission of any subsequent change concerning the designation and respective competences of those authorities.

• EBA Guidelines will follow. The aim is to achieve a common, uniform and consistent application of EU law.

Article 16 Regulation 1093/2010: public consultations - financial institutions and competent authorities must do every efforts to comply with the guidelines. They have the obligation to give notice to the EBA if the Guidelines will be followed or not (the EBA has the possibility to disclose publicly the authorities that comply with the Guidelines).
ADR procedures for the settlement of disputes

1) Complaint procedures

2) ADR procedures and penalties
ADR procedures and penalties

Dispute resolution (art. 101 - NEW)

• Member States shall ensure that PSP’s put in place and **apply adequate and effective complaint resolution procedures** for the settlement of complaints of PSU’s 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 PSP 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 PSP and the PSU.
ADR procedures and penalties

• Deadline for answering:

PSP’s make every possible effort to reply, on paper (on another durable medium if agreed between PSP and PSU), to the PSU’ 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 PSP, 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 PSU will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.
ADR procedures and penalties

- The PSP inform the PSU about at least one ADR he can address. This information must be mentioned in a clear, comprehensive and easily accessible way on the website of the PSP (where one exists) and in the general terms and conditions of the contract between the PSP and the PSU. It must be specified how further information on the ADR entity concerned and on the conditions for using it can be accessed.

- Concretely: clause in the General terms and conditions of the Bank regarding Ombudsfin, as well as a reference on the website of the Bank.

- Overlap with Regulation n° 524/2013 on online dispute resolution for consumer disputes.
ADR procedures and penalties

ADR Procedures (art. 102)

- Adequate, independent, impartial, transparent and effective (new criteria’s) alternative procedure for the settlement of disputes between PSU’s and PSP’s must be foreseen. The competence of this authority is limited to discussions regarding Titles III and IV.

- Concretely, Belgium can use the existing Ombudsfin.

- If the dispute has a cross-border nature, the authorities on alternative dispute resolution should cooperate.

- Platform FIN-NET (network of ADR entities within the European Economic Area with the objective of, in the event of an international dispute, help consumers get into contact with the foreign body on alternative dispute resolution).
ADR procedures and penalties

Penalties (art. 103)

- “Member States shall lay down rules on penalties applicable to infringements of the national law transposing this Directive and shall take all necessary measures to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.”

  - De facto: possibility to impose criminal penalties and to determine an administrative fine.

- “Member States shall allow their competent authorities to disclose to the public any administrative penalty that is imposed for infringement of the measures adopted in the transposition of this Directive”

  - New: the authorities may disclose information about sanctions.
Thank you for your attention