Ref.:EBF_004743
Brussels, 08.11.2013

European Banking Federation (EBF) Position Paper on the European Commission Proposal for a Revised Payment Services Directive (PSD2)

Launched in 1960, the European Banking Federation (EBF) is the voice of the European banking sector from the European Union and European Free Trade Association countries. The EBF represents the interests of some 4,000 banks, large and small, wholesale and retail, local and cross-border financial institutions. Together, these banks account for over 80% of the total assets and deposits and some 80% of all bank loans in the EU alone.

Executive Summary

On 24th July 2013, the European Commission adopted a proposal for a revised Directive 2007/64/EC on Payment Services ("the PSD2"). The main high-level objectives of the revision are to promote better integration, more innovation and more competition in the market for payment services within the EU. **These are goals that the EBF welcomes and supports, just as the EBF encourages innovation and welcomes the entry of new players in the payments sphere**. Furthermore, **the EBF welcomes the increased degree of harmonization and the reduction of the options allowed to Member States that is inherent in the proposal**. One of the problems of the current PSD is the quite heterogeneous implementation across the EU.

The EBF has also, however, identified a number of areas of concern and need for further clarification in relation to, *inter alia:*

- Third party payment service providers ("TPPs"),
- Liability rules,
- Treatment of "one-leg transactions" and
- Surcharging rules.

These are described in detail in the present document, and the key issues are highlighted below.

A key, overarching consideration must surely be **the need to safeguard the integrity of the payment systems and, in the final instance, trust in these systems. The EBF does not feel that this consideration is reflected adequately in the proposal as it stands. This is most pertinent in relation to TPPs**.

I. Treatment of TPPs

TPPs are service providers that offer so-called Payment Initiation Services (PIS) or Account Information Services – and that make use of the online banking infrastructure provided by banks to their customers to deliver their services.

Access to consumers' personal and financial data – and not the least to dispose of their funds – requires a high level of security to protect against the risk of fraud, theft and misappropriation of data. Hence, **the EBF very much welcomes the inclusion of TPP's within the scope of the PSD, making them subject to a proper supervisory and licensing regime**. However, the EBF notes several areas in the proposed Directive, where the treatment of TPPs is not sufficiently clear and leaves important questions unresolved:

Obligations of TPPs: Although TPPs are brought into scope of the PSD, the extent of this coverage is not clear. Some articles refer specifically to TPPs, while others refer to the broader term payment

EBF a.i.s.b.l
ETI Registration number: 4722660838-23
Avenue des Arts 56, B-1000 Brussels
+32 (0)2 508 37 11 Phone
+32 (0)2 511 23 28 Fax
www.ebf-fbe.eu

service providers – which supposedly also includes TPPs. **It should be made entirely clear that TPPs must also comply with the PSDs general requirements on security, business conditions etc**.

Handing over of personal log-in details: The proposed Directive allows consumers to hand over their personal log-in details to third parties. In a time where identity theft and digital fraud is an increasing problem, **the EBF strongly believes that this should not be allowed**.

Roles and responsibilities between AS PSPs and TPPs: While the proposed Directive gives TPPs a right to access to the account, the Directive is less explicit in how this affects the roles and responsibilities of TPPs and AS PSPs, e.g. in relation to security issues, the requirement for TPPs to authenticate themselves towards AS PSPs, the coverage of increased costs for AS PSPs as a result of the introduction of TPPs etc. **The EBF requests further clarity on these issues**.

Need for clearer liability rules for TPPs: Preamble 52 rightly states that liability rules should ensure that each party takes responsibility for their part of the transaction. The EBF, however, does not feel that this principle is reflected adequately in the Directive itself, which leaves the AS PSP as the sole point of contact for the customer in case of disputes. **The EBF believes that the Directive should make more explicit the fact that TPPs are liable for any errors or fraud assignable to them.**

Need for a contractual basis: The above clearly demonstrates that the introduction of TPPs in the payment chain creates complicated legal and operational interactions between the TPP, the AS PSP and the customer. **The EBF thus firmly believes that these relationships should be governed by clear and transparent agreements between the three parties involved**.

II. Selected other issues

"One-leg" transactions: The inclusion of transactions, where only one leg is carried out within the EU, introduces a number of challenges in relation to e.g. providing information on execution times and costs, as the PSP located in the EU will not be in control of what happens outside the EU. **The EBF believes the Directive should acknowledge this challenge more clearly.**

Surcharging: While the EBF welcomes efforts to harmonise surcharging rules across the EU, the wording of the Directive, which bans surcharging on payment cards subject to the IF regulation but not on other payment instruments, is not helpful as it discriminates against credit transfers and direct debits. **The EBF strongly believes that legislation should support electronic payment means, to the detriment of cash payments, the most expensive payment form in the EU**.

Liability rules and refunds: Liability rules should give all actors incentives to minimise the risk of theft, fraud etc. **While provisions in the Directive concerning liability are, in general, quite complicated, the EBF sees in particular a need for further clarification relating to**:

- *The treatment of TPPs,* c.f. above
- *The lowering of the maximum loss to be borne by the payer to €50*, which the EBF does not feel is high enough to encourage diligent and cautious behaviour;
- *The long period (8 weeks) allowed for a request for unconditional refund for direct debits;*
- *The lack of recognition of the time it takes to treat complaints and requests for refund,* e.g. in relation to the requirement to refund an unauthorized transaction "immediately", and to respond to complaints within 15 days;
- *The proposed reduction in the right to refund in cases where "the payee has already fulfilled its obligations… services have already been received… or goods… already consumed"*, which leaves the PSP with an unfortunate role pertaining to the underlying commercial contract between the payer and the payee.

Specific Remarks

TITLE I - SUBJECT MATTER, SCOPE AND DEFINITIONS

Art.2 - *Scope*

Some of the requirements set by Title III (for example articles 38(b), 41(c), 45(2)(e), 49, 51) are practically impossible to fulfill, such as providing information from countries outside the EU on the exact execution time, applicable fees and exchange rates. The routing and processing end-to-end of the transaction is not fully in the control of the PSP located in the EEA. The EU has no jurisdiction on these countries.

Art. 3 – *Negative scope*

The redrafting of the exclusion for limited network (k) is appreciated as it provides clarity on a debated interpretation issue.

Also exclusion (l) for transactions carried out by a provider of electronic communication networks benefited from redrafting. However, it should be further clarified what "ancillary service to electronic communication services" means as well as provide a reference in the definitions to the definition in the Consumer Rights Directive for the term "digital content", and what the rationale is for setting the exempted values at €50 and €200. We consider these limits as much higher than needed or indeed even prudent given the difference in economic realities of the Member States. There is a risk opening a hole in legislation of which "over the top" companies and telecom operators would benefit in a totally unleveled playing field.

Art. 4 - *Definitions*

4-32 - Payment Initiation Service

It is unclear what is meant by the text: "...where the payer can be actively involved in the payment initiation or the third party payment service provider's software...."

Does it mean that the third party payment service provider's software can initiate a payment without the consent of the payer or that a software can replace a human being?
The sudden reference to a software is odd, to say the least.

This definition could be understood as restricting the concept of payment initiation services ("PIS") only to cases involving the use of the payer's personal security credentials by the TPP. It could appear as if the concept of impersonation (use of the payer's personal security credentials by the TPP) is encouraged with this definition.

Furthermore the question remains if this concept violates the principle that legislation should remain technologically neutral as to the solutions that would be used to achieve the results foreseen, i.e. the innovation of payment initiation services to be addressed within the scope of PSD2. It could be argued that one particular (technical) concept of providing 'payment initiation services' would be promoted via PSD2 at the expense of other technical concepts.

The following new wording is suggested:

"A payment initiation service means a payment service enabling a third party payment service provider to access a payment account and initiate a payment upon request by the payer and in full agreement with the payer's account-servicing PSP."

4-33 - Account information service

The qualification *"user-friendly"* is a subjective judgement and should not be part of a legal text - to be deleted.
The definition is lacking any suitable limitation of the scope of such 'account information services". Given that account information is of an extremely delicate nature in the context of data protection and banking secrecy rules it would appear essential that a suitable definition for such services be found.

TITLE II – PAYMENT SERVICE PROVIDERS

Art. 10 - *Granting of Authorisation* and Art. 27 - *Waivers-Conditions*

All PSPs - including TPPs - should require prior authorisation before being able to provide their services. However, in those cases of undertakings where the average total amount of payment transactions executed is less than EUR 1 million/month no prior authorisation will be required. This could effectively lead to many TPPs remaining unauthorised. We believe that it is not the size of a TPP alone that demands a regulatory oversight but the simple fact that a third party is able to intervene in the chain of a payment transaction which is triggered by a bank customer who has to rely on the proper conduct of the TPP, the security of the payment, the protection of its data, the speed of the execution and last but not least that in case of any mishandling of a payment order the responsible party is able to pay for any loss incurred.

Art. 29 - *Access to payment systems*

We appreciate the maintenance of firm soundness principles in relation to access. However, the last part of paragraph 2 is unclear: it may be interpreted as an obligation for the PSP to take on board any indirect participant irrespective of its own assessment, market, risk considerations and choice. This obviously would be against the principle of contractual freedom in a market economy.

TITLE III – TRANSPARENCY OF CONDITIONS AND INFORMATION – REQUIREMENTS FOR PAYMENT SERVICES

As mentioned in our introduction, the treatment of TPPs in respect of transparency obligations is unclear and needs to be reconsidered.

More specifically, we would like to point out that the following articles are not clear and need to be redrafted:

- Article 34, which puts the burden of proof on compliance with respect to the information requirements on the PSP (understood as the account-holding PSP);

- Article 39, which assumes the account-holding PSP knows there is a TTP offering a payment initiation service, but this cannot be guaranteed as the proposed PSD2 does not impose a mandatory contractual relation between these two parties.

It is also unclear whether TPPs are equaled to account-holding PSPs with reference to the framework contracts. We believe they should in order to ensure high consumer protection.

In terms of consumer awareness and protection, the requirements stated on articles 38 and 39 should also be reviewed with the purpose of illustrating clearly to the user the characteristics and consequences of TPP intervening in a transaction.

It should also be specified that the information and data detailed in art. 38.2 and art. 39 should be rendered before initiation of a payment order and not after.

Art.40: the proposal provides that where a payment order is initiated by the third party payment service provider's own system, it shall in case of fraud or dispute make available to the payer and the account servicing payment service provider the reference of the transactions and the authorisation information. This concept would suggest that the AS PSP will only learn about the transactions where a payment order is initiated by the third party payment service provider's own system in an *ex post* manner.

The Article should be rephrased to extend the obligation of the TPP in all cases – not only in the case of fraud or dispute. How would the TPP know about and be certain about cases of fraud? In other words: how would the TPP know when and within which limitations its obligation would apply? Who would decide if there is a case of fraud or dispute? What exactly constitutes a case of dispute?

Art. 44 – *Prior general information*

As to pre-contractual information it would be important to indicate in paragraph 1 that such information could be also made available in the premises of the PSP, in order to allow potential users to become aware of the information and conditions as per Article 45.

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

CHAPTER 1 - Common provision

Anti-Money Laundering and Counter-Terrorism Requirements

The EBF believes that reference should be made in this Chapter to existing Customer Due Diligence obligations (Know You Customers (KYC) requirements) as defined in the third EU AML Directive[1].In order to ensure a level playing field and ensure the full integrity of payment system against money laundering and terrorist financing, these KYC requirements should indeed apply to TPPs.

Art. 55 - *Charges applicable*

This article introduces the general possibility for payees to surcharge the payer for the use of a payment instrument. In this respect the following is noted:

[1] DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Currently under review)

- considering that paragraph 4 excludes from the scope of paragraph 3 card payment transactions (because they are regulated under the Interchange Fees Regulation), this article will apply only to credit transfers and direct debit penalizing those instruments vis-à-vis other payment instruments not covered by the PSD2, which appears in contradiction with the stated objective of promoting electronic payment means, as well as with the completion of SEPA. Discounts and not surcharges should be allowed on those instruments; rather surcharges should be allowed on cash;

CHAPTER 2 – Authorisation of payment transactions (Articles. 57-68)

Art. 57 – *Consent*

We strongly object to the last sentence of par. 2, as consent can never be considered given if such consent is not known to all parties involved in a payment transaction and namely in case of TPPs offering payment initiation services to **both the user and the account-holding PSP.** In order to address the security requirements and the need for identification of parties, to clarify the allocation of liabilities between parties and to comply with banking secrecy, data protection and other legislative requirements which aim to protect the consumer, an explicit consent from both the payer and from the account-servicing PSP is required before the services can be implemented and used.

Articles 58-59

These articles are specific for TPPs and provide for a non-discrimination principle against the payment orders initiated by TPPs. Rather, we would say that there is a discrimination principle *against the account-holding PSP*, because the latter appears to be deprived of the freedom to allow or not access to the accounts that it has opened and managed with the related costs and responsibilities.

Art.58.1 seems to impose the provision of PIS by all Account-servicing PSPs, which would of course be against the principle of freedom of enterprise.

Unless the PSD2 would clearly impose a transparent contractual relationship between TPPs and account-holding PSPs, this provision would result in an extremely unbalanced treatment of market players.

As stated in our introduction, **any business model based on the consumer handing over their personal log-in credentials should not be allowed**.

If a consumer opts to hand-over his/her credentials to a TPP and if something goes wrong with the transaction, it will be under the consumer's full responsibility.

Indeed in the absence of an agreement between the AS PSP, the account holder and the TPP on the consumer's use of the TPP for the provision of payment initiation services, the account holder shall not have a claim for compensation against the PSP relating to any failures or unauthorised payment transactions resulting from his / her use of a TPP.

Furthermore, it should be clarified that this article does not apply to Account-servicing PSPs that do not offer on-line banking. If a PSP offers only "conventional" banking, it should not be forced to offer online banking services just to enable its PSUs to use TPPs.

Article 58.1 should be modified as follows:

“1. Member States shall ensure that the account servicing payment service provider shall agree with the payment users the terms and conditions under which the later may use a third party payment service provider to obtain payment initiation services as defined in article 4. (32).”

Article 58.2 wrongly presupposes that a TPP is able to “authenticate itself in an unequivocal manner”. This is not technically possible unless there are different authentication measures in place for payment initiated or not via a TPP, which would be both costly for the providers and burdensome for the users.

Article 58.2 should therefore be modified as follows:
“2. To provide payment initiation services the third party payment service provider shall:

(a) Be authorized by the payer to provide the service;

(b) Agree [bilaterally or multilaterally] with the account servicing payment service provider the procedures and standards necessary for the secure authentication of the third party service provider , the communications between the two service providers and the transmission to the account service payment service provider of the consent of the payer.

(c) authenticate itself in an unequivocal manner towards the accountservicing payment service provider of the account owner, for each transaction according to the provisions of (b) above and shall therefore not use the personalised security features of the payer for the purposes of this provision

Art. 58.3: the words “availability of funds” should be replaced by “presence of funds” knowing that no payment guarantee is provided, so the availability of said funds cannot be guaranteed.
The account holding PSP might not know the TPP or its address. Therefore, the account holding PSP should only be forced to communicate with its on customer which is the PSU.

The text of Article 59 includes the terms “third party payment instrument issuer” as well as “payment card services” which have not been defined in the proposal. These terms should be clarified in Article 4 otherwise the article will remain unclear as to its proposed scope and aim which it is to achieve.

At present, the account-holding PSP agrees with the PSU on the payment card(s) attached to the account taking into account the credit risks involved. In any case, it has to be ensured that only the account holding PSP has the right to decide about the payment instruments that the PSU may use to authorise payments from his or her account as every payment instrument bears risks of misuse.

Therefore, information on availability of funds can be given to the payee (merchant) as agreed with the account-holding PSP, not to another card issuer. Article 59, as proposed, leads also to several problems related to the account-holding PSP’s liability for unauthorized payments, loss or unauthorized storage and use of personal data.

Articles 60 – 65

Liability rules seem neither clear not logical: As pointed out previously, all these articles (and particularly 60.2, 62.1, 63.2, 65) cannot be applied correctly in case a TPP intervenes in a transaction and the above mentioned requirements would not be fulfilled.

The responsibilities, evidence and burden of proof on those cases should indeed be considered separately for TPPs and account-holding PSPs, and not be interrelated. This principle is rightly set down in Recital 52: "Rights and obligations of the payment service users and payment service providers should be appropriately adjusted to take account of the **TPP involvement** in the transaction whenever the payment initiation service is used. Specifically, a balanced liability repartition between the payment service provider servicing the account and the TPP involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are **under their control** and clearly point to the responsible party in case of incidents."

Unfortunately this sound principle is not reflected in the text of the relevant articles of the Directive as it should be (e.g. articles 65,80 and 82).

TPPs should be fully and directly liable to users, without account-holding PSPs being obliged to refund users in a first place and then to exercise their right to recourse vis-à-vis TPPs.

Without a contract between the TPP and account servicing PSP how may the financial compensation to the account servicing PSP by the Third PSP be applied? (article 64.2)

Art. 65 – *PSP liability for unauthorized payment transactions*

Art. 65.1: In addition to the previous comment, it is noted that unfortunately, this article does not address one of the most debated issues raised by the PSD, related to the timing of refund. Experience has shown that a minimum level of checking is needed in order to discourage and indeed block unfounded/fraudulent attempts at requesting refund. Therefore we suggest that the word "immediately" is changed in "without undue delay" in order to take account of a "*de minimis*" investigation which must be carried out by the PSP in order to discard totally unjustified or fraudulent refund claims.

Art. 65.2
In relation again to TPPs, we strongly object to paragraph 2, as refund should be requested to TPPs when they intervene in the transaction and not to the account-holding PSP. This principle is rightly introduced in Article 80. It is important to note that according to the present text of the proposal, the AS PSP is neither able to control nor allowed to prevent the use of payment initiation services. It is the decision of the PSU – not the AS PSP- if payment initiation services are used and which provider (TPP) will be requested / selected to provide the services. Therefore, it is not appropriate that the AS PSP would run the insolvency risk of the TPP which was chosen by the PSU.

We suggest the following wording:

"2. Where the unauthorized payment transaction is originated by a payment order transmitted by a third party payment service provider the account servicing payment servicing provider shall inform the payer accordingly and the third party payment provider shall restore the debited payment account to the state in which it would have been had the unauthorized payment transaction not taken place."

Art. 66 – *Payer's liability for unauthorized payment transactions*

The new draft of this article worsens one of the highly debated points of the PSD, which is the amount of losses that the payer may be obliged to bear before notification. Indeed we consider that further reduction of such amount to 50€ (from the already low level of 150€) represents a disincentive to cautious and diligent behavior by users, with respect in particular to notify loss or misappropriation in a timely manner. This seems also being aggravated by the fact that the PSD (and PSD2) puts the burden of proof on PSPs, and that the experience so far has shown that it is generally impossible to prove negligence by the user.

In such a way, the PSD2 risks fostering careless and/or fraudulent behavior by users, and is not in line with the ECB Recommendation for the Security of Internet Payments, which conversely points to the need of increasing customer awareness.

Liability rules should ensure that all parties have the right incentives to behave- we believe the new threshold of 50 euro does not achieve this.

Articles 67 - 68 – *Refund and request for refund*

The redrafting of these important articles appears to have a twofold objective:

- on the one hand, aligning the provisions of the law to the *practice* introduced in the EPC SDD "Core" Rulebook of a refund on a "no-question asked basis", and therefore grants "*unconditional right for refund"* and,
- on the other hand, ensuring that such right is not exercised in cases *"where the payee has already fulfilled the contractual obligations and the services have already been received or the goods have already been consumed by the payer".*

To this regard we note that:

a) the long refund period allowed by the PSD has generated uncertainty for the creditors and had severe adverse impact on the credit extended to them in anticipation of expected flows of collections, which not only are not final until after 8 weeks from debit date but where finality ultimately depends on the PSP-debtors' agreements unknown to the creditor and its bank as well as on the debtors' behaviour (which can also abuse of the refund rights);

b) an unconditional right to refund coupled with such a long refund period risks exacerbating the instability of the direct debit market to the detriment of creditors, and ultimately the appeal of the direct debit instrument to them. If creditors would no longer be willing to use direct debit, this would also be to the detriment of consumers. We would therefore suggest reconsideration of the 8 weeks period for the unconditional refund right;

c) there is a need to clarify the cases *"where the payee has already fulfilled the contractual obligations and the services have already been received or the goods have already been consumed by the payer";*

d) in any case, the PSP cannot be requested to play any "mediator" role between creditor and debtor in relation to the underlying obligation. At a minimum the request for additional information by the PSP shall not be mandatory but only optional. The underlying commercial contract must stay legally separate from the payment transaction. Who is entitled to make a judgement whether the services or goods have already been consumed? Certainly not the PSP. The factual details of consumption of services and / or the receipt of goods are outside of and disconnected from the customer-to- PSP relationship.

It is noted that the last sentence of the fourth subparagraph of Article 67.1 is not readable and that clarity is sought with regard to Article 67.3: to what kind of transactions/situations does this § apply?

In summary, Article 67 needs thorough rewriting for SEPA Direct Debits to continue to be viable and used after entry into force of the Directive.
Unintentionally certainly, the way in which this article is written transforms an unconditional right to refund into a conditional one with the conditions impossible to determine precisely. This is a real decrease in consumer protection and will have an impact on the use of Direct Debits.

The banking industry will provide suggestions in due time. Our reasoning is that there should only be one default situation in the law, whilst recognizing that parties may agree otherwise in the framework contract

The default situation should be: always a right to refund, but parties may agree in the framework contract that the payer is not entitled to a refund in case the payee has already fulfilled his contractual obligations and the services or goods have already been consumed.

CHAPTER 3 – Execution of payment transactions

Art. 71 - *Irrevocability*

Paragraph 2 of this article should be reconsidered, as the concept of "irrevocability" as being linked to "receipt of the payment order" by the PSP is no longer applicable in relation to TPPs intervening in the transaction. In such cases the payment order that is received by the payer's PSP has not been provided by the payer but by the TPP and hence a different set of liability and revocability provisions should apply.Indeed the account-servicing PSP has no knowledge of the exact moment when the payer gave his consent to the TPP. And what should the ASPSP do if he receives an opposition from the payer before or at the same time of the reception of the message of the TPP transmitting the payment order?

Art. 74 – *Payment transactions to a payment account*

It is noted that the last sentence of par. 1 should read "this period" (and not ("these periods"). Further, Article 74(3) remains unclear as to its application to card transactions. Incorporating the wording of the Commission's own guidance in respect of this issue from the PSD Q & A's would have provided the desirable clarity and legal certainty.

Art. 80 – *Non-execution, defective or late execution*

As indicated in the section "General remarks", the liability in connection with the presence of TPPs has to be reviewed in order to ensure proper balance of responsibilities between TPPs and account-holding PSPs.

Specifically, it is not conceivable that the account servicing PSP could be under any circumstances held liable for non-executed or defective payment transactions and should refund the user in the first place if the TPP is liable for non-execution or defective execution. In such cases, the transaction falls under the TPP's responsibility and the TPP shall refund the user.

Article 80 (1), second §, last sentence, should be rephrased to foresee a liability of the AS PSP only towards the payer – not the payee – for the correct execution of a payment transaction. It would be

more coherent (in accordance with the principles of the present PSD) if the payer's PSP remains liable to his contractual partner i.e. the payer himself – instead of being liable to the payee.

Moreover if the account-holding PSPs *"shall make immediate efforts to trace the payment transaction and notify the payer/payee of the outcome",* it is clear that this activity shall be remunerated either by the TPP or by the user.

Art. 82 - *Right of recourse*

The way this article relates to the role of TPPs and unclear as well as whether TPPs are "intermediaries" or not, as there is no definition of "intermediary" and TPPs are defined only by their activity in Annex 1.

CHAPTER 4 – DATA PROTECTION (Article 84)

We note that the provision previously present in Article 79 of the PSD, explicitly allowing the exchange of data "*necessary to safeguard the prevention, investigation and detection of payment fraud",* has been withdrawn from the proposal.

The EBF considers that detecting and preventing fraud is of significant importance, not only to financial institutions and payment systems, but can help to protect consumers *inter alia* from identity theft. Therefore, a concrete reference to fraud and financial crime prevention and detection as a legitimate interest to process data was very much welcome in the PSD as it provided the right legal basis for this type of processing.

We wonder whether new Article 84, making reference to Directive 95/46/EC and to the national rules transposing Directive 95/46/EC and Regulation (EC) No 45/2001, will achieve the same effect.

Given that the current EU data protection legal framework is currently under review, clarity is needed as to how the prevention and detection and investigation of payment fraud can still be performed under full legal certainty by financial institutions and payment systems.

CHAPTER 5 – OPERATIONAL AND SECURITY AND AUTHENTICATION (Articles 85-87)

These articles incorporate some of the ECB Recommendations for the Security of Internet Payments. Specifically, the Recommendations concerning incident monitoring, reporting and risk control and strong authentication are incorporated to some extent. However, given the importance of the ECB Recommendations, we believe that all of them should be introduced in this Chapter of PSD2 in order to ensure maximum harmonization in their implementation in all Member States.

The applicability of these articles in the event a TPP intervenes in a transaction is a perfect demonstration that the requirements for TPPs outlined in our introduction are absolutely needed, because otherwise these articles cannot be complied with.

Specifically, Article 87.2 should specify that the TPP should use "strong authentication" towards the account-servicing PSP and that authentication of the TPP should occur "***before initiating a transaction on behalf of the user".***

According to Art. 87 "Authentication" the account servicing payment service provider (PSP) as well as the third party payment service provider are obliged to apply strong customer authentication when the payer initiates an electronic payment transaction. It is not clear how this would work in practice and how the security features of both methods of authentication would interrelate.

We thus suggest that each PSP has to rely on its own authentication methods and therefore each party is liable for the quality of these methods. There would not be a level playing field, neither under security nor under cost aspects, if some market participants would get the right to use the others' infrastructure for free. Therefore, TPPs should not be allowed to use the account holding PSPs authentication instruments unless there is an agreement on this (including costs and liability) between the two PSPs.

Furthermore, it is necessary to include a precise definition of "strong authentication" in Article 4 – Definitions.

Articles 85, security requirements and incident notification and 86: implementation and reporting: refer to Directive NIS which puts obligation primarily on the Member States to establish a required framework and has not been adopted. The creation of a high interdependence between both Directives is not desirable given the uncertainty related to the final shape of the NIS Directive or its subsequent national implementation. Therefore these articles cannot be applied as such and should be deleted from the proposal for the PSD2.

Article 90: *Internal resolution of disputes*

We suggest to extend the total period for dealing with complaints from 15 business days to 30 calendar days. This extended period is necessary for an appropriate review and assessment of all relevant facts.

Role of the European Banking Authority

The PSD2 suggests a central role to be played by the European Banking Authority (EBA) in the implementation and reporting provisions of the proposal.

The allocation of responsibilities between EBA and the Securepay forum author of ECB Recommendation for the Security of Internet Payments could be further clarified.

In particular, the EBF fears a lack of clarity as to how the forthcoming guidelines to be issued by EBA will be coordinated with the Securepay forum recommendations.

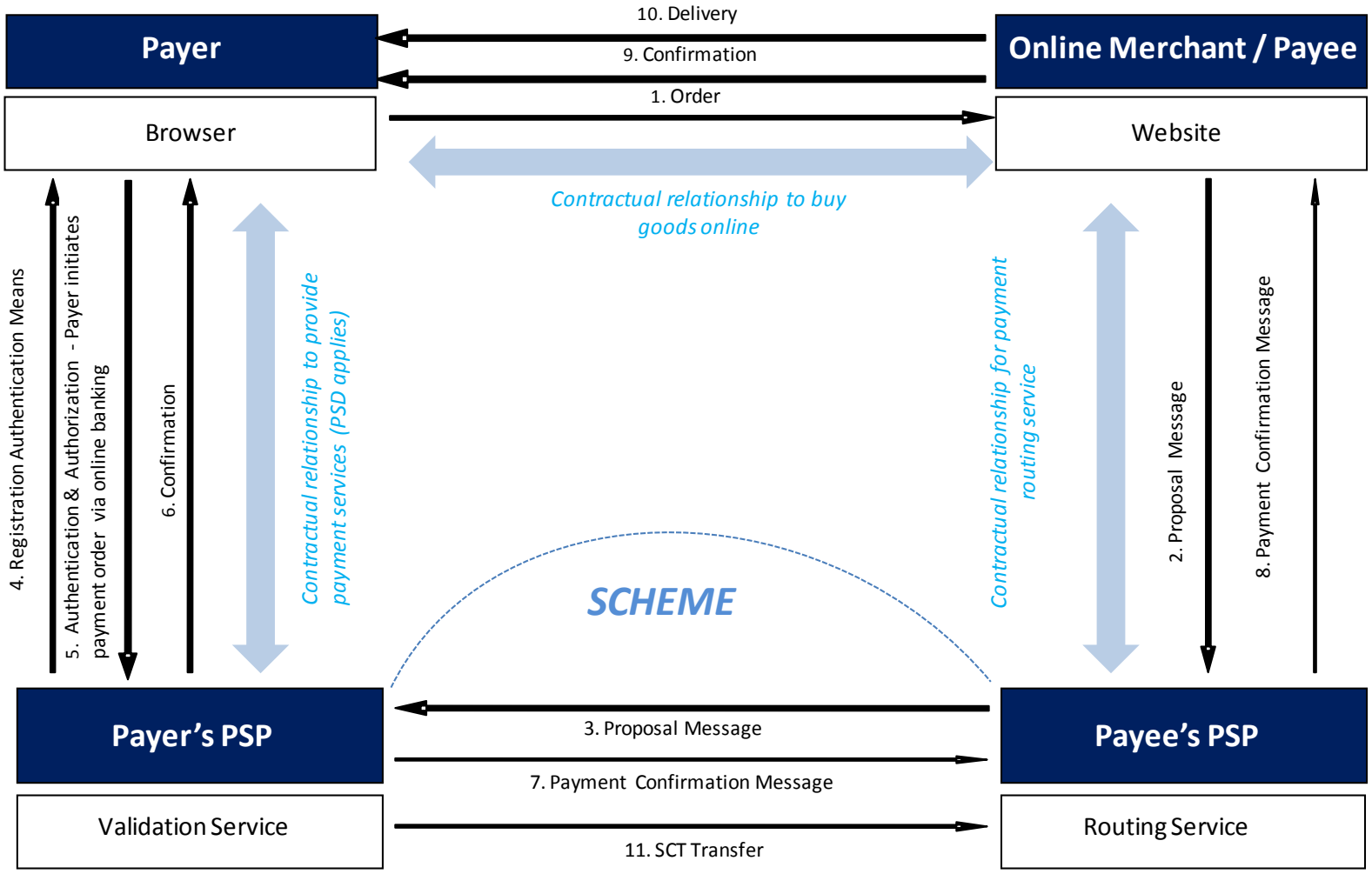
The EBF believes that the tasks conferred to EBA should not lead to any regulatory overlap and unnecessary duplication of successful standard setting exercises.

Contacts:

Patrick Poncelet: p.poncelet@ebf-fbe.eu
Séverine Anciberro: s.anciberro@ebf-fbe.eu

Annex I: TPP Process Flow Diagrams

a. Four Corner Process Flow l: Customer Initiates Payment Order

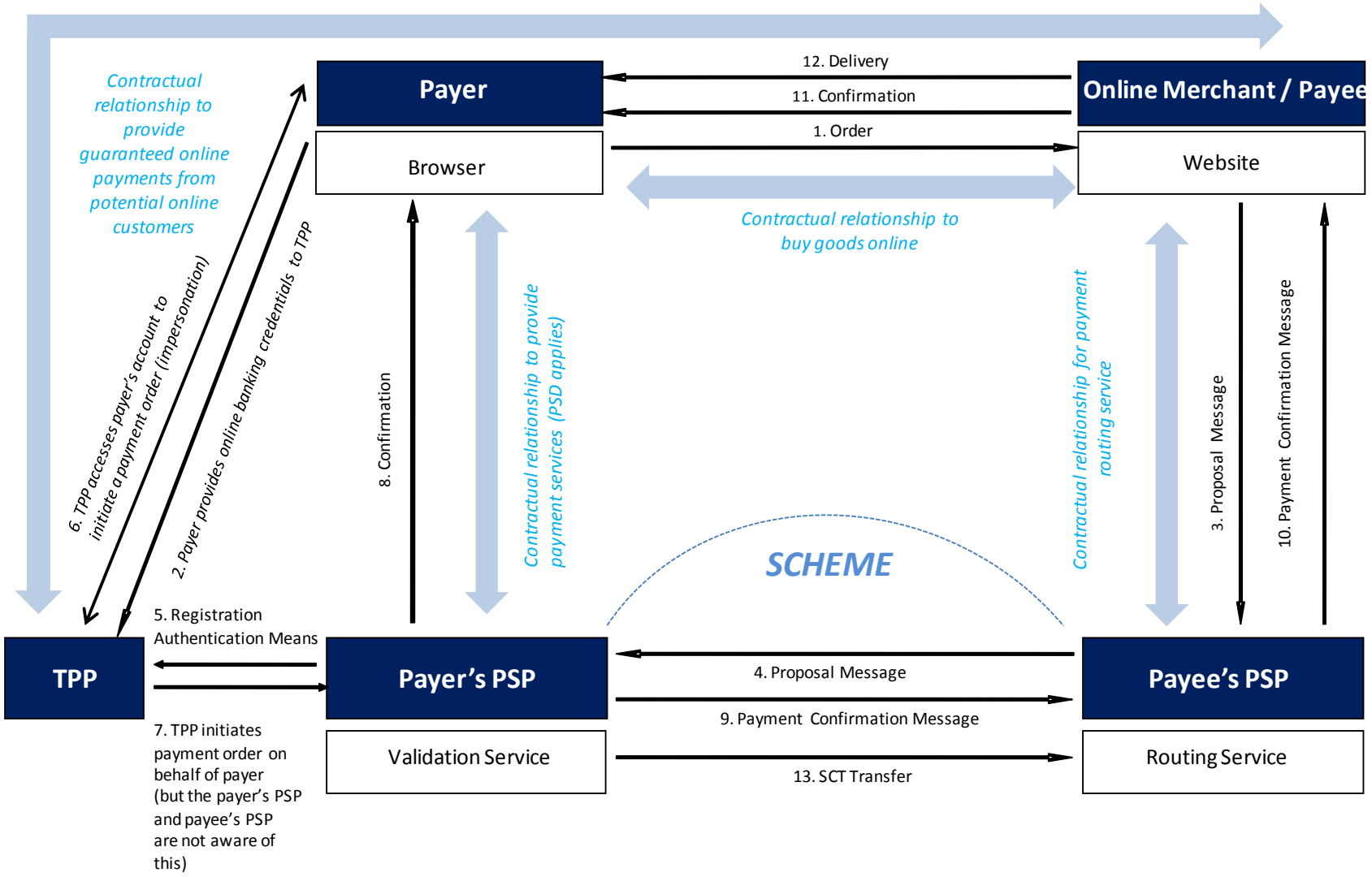


EBF a.i.s.b.l
ETI Registration number: 4722660838-23
Avenue des Arts 56, B-1000 Brussels
+32 (0)2 508 37 11 Phone
+32 (0)2 511 23 28 Fax
www.ebf-fbe.eu

Process flow description:

1. The payer using an Internet browser accesses the merchant's (payee) website to buy goods online.
2. A proposal payment message is sent from the payee to the payee's PSP (or routing service provider).
3. The proposal message is sent from the payee's PSP (or routing service provider) to the payer's PSP (or validation service).
4. The payer is redirected from the payee's website to an authentication screen offered by the payer's PSP (or validation service).
5. The payer authenticates itself and initiates a payment order via its own online banking.
6. The payer's PSP (or validation service) verifies the authentication credentials provided by the payer and confirms the result to the payer.
7. The payer's PSP (or validation service) sends a payment confirmation message to the payee's PSP (or routing service).
8. The payee's PSP (or routing service) forwards the payment confirmation message (when validated) to the payee.
9. The payer is routed back to the payee's website where a confirmation of the payment is presented.
10. The payee delivers the goods to the payer.
11. The payer's PSP creates and sends a SEPA Credit transfer message to the payee's PSP.

b. TPP Process Flow: TPP Initiates Payment Order



Process flow description:

1. The payer using an Internet browser accesses the merchant's (payee) website to buy goods online.
2. The payer is asked at check out to provide its online banking credentials to the Third Party Provider (TPP) as part of the proposed payment process.
3. A proposal payment message is sent from the payee to the payee's PSP (or routing service provider).
4. The proposal message is sent from the payee's PSP (or routing service provider) to the payer's PSP (or validation service).
5. The TPP is directed from the payee's website to an authentication screen offered by the payer's PSP (or validation service).
6. The TPP accesses the payer's account and uses the payer's credentials to authenticate itself (impersonation).
7. The TPP initiates a payment order on behalf of the payer. However, both the payer's PSP and the payee's PSP are not aware of this and assume that the payer initiated the payment order.
8. The payer's PSP (or validation service) verifies the authentication credentials provided by the TPP and confirms the result to the TPP.
9. The payer's PSP (or validation service) sends a payment confirmation message to the payee's PSP (or routing service).
10. The payee's PSP (or routing service) forwards the payment confirmation message (when validated) to the payee.
11. The payer is routed back to the payee's website where a confirmation of the payment is presented.
12. The payee delivers the goods to the payer.
13. The payer's PSP creates and sends a SEPA Credit transfer message to the payee's PSP.

Source: European Payment Council