



Electronic Money Association

Crescent House

5 The Crescent

Surbiton

Surrey

KT6 4BN

United Kingdom

Telephone: +44 (0) 20 8399 2066

Facsimile: +44 (0) 870 762 5063

www.e-ma.org

Treasury and Financial Policy

State Secretariat of Economy and Support of
Entrepreneurship of the Ministry of Economy,
Industry and Competitiveness

Submitted by email to:
audiencia@tesoro.mineco.es

10 April 2018

Dear Sirs

**Re: Consultation on implementation of the Revised Payment Services
Directive (PSD2) in Spain**

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

Please find below EMA's response to the consultation. I also attach our PSD2 Position Paper setting out our views on a number of issues related to the implementation and interpretation of PSD2 at national level. Please feel free to contact us should you have any question or require further information.

I would be grateful for your consideration of our comments and proposals.

Yours faithfully

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Exemption from certain authorisation conditions – small PIs and small EMIs (Article 32, PSD2)

One of the objectives of the ‘small’ institution regime is to allow prospective payment service providers to offer a limited service, under certain controls, and to assess the viability of the business. A proportionate supervisory approach is therefore also appropriate, and minimising reporting requirements, except where these are essential, is preferred. We support a light touch approach to registration, enabling innovative payment startups to enter the market and test their products.

Thresholds for low value payment instruments (Articles 42(2) and 63(2), PSD2)

We propose the introduction of the higher limits, which continue to be low in relative terms, and enable the offering of low value payment products to users without giving rise to significant risk. The products benefiting from this exemption generally have low profit margins, so this lighter regulatory regime allows them to be commercially viable for issuers, which in turn means they can be purchased by consumers. These products are valued by wide range of consumers, including:

- The financially excluded, who do not have the facility to make online payments;
- Those who might wish to protect their main payment account by limiting its online use for certain goods, or for day-to-day expenses;
- Those who desire privacy when making purchases;
- Those who wish to limit the amount that can be spent – for example parents giving their teenage child a card with pocket money;
- Travellers seeking an alternative to cash.

As the derogation only disapplies a limited number of provisions, the consumer will continue to benefit from consumer protection measures set out in the remainder of the relevant titles and PSD2 as a whole.

Appendix: **EMA PSD2 position paper – Nov 2017**

1. Interpretation of the commercial agent exclusion and its application to business models, article 3(b)

1. In relation to article 3(b) PSD2, the European Commission has indicated that in the case of e-commerce platforms, the exclusion can still apply if there is a third party (a PSP) handling funds for one of the parties (either the payer or the payee); in this case the commercial agent would only act for one of the parties for the purposes of the exclusion so the exclusion would apply. We would welcome confirmation that the same approach will be taken.

2. Examples of when a payment service may be ancillary to another business activity as well as factors to help determine whether a payment service is ancillary would be useful.

3. We would also welcome clarification and examples of when the commercial agent is regarded as acting only on behalf of the payer or the payee, as opposed to when the commercial agent is acting on behalf of both the payer and the payee.

2. Limited network exclusion, article 3(k)

1. The European Commission position is that the addition of 'very' was not intended to change the interpretation of the exclusion, but rather to clarify its scope. We would not therefore expect the interpretation to change in a significant way.

Given the Commission's intention not to amend the scope, can you confirm that exempted products that meet PSD1 criteria for limited range of goods and services can be assumed to continue to meet the new criteria under PSD2?

Examples of products that are currently regarded as qualifying for exemption are fuel cards that enable the purchase of fuel and other items from a petrol station, or event gift cards that enable the purchase of tickets as well as goods or services associated with the event. Are you able to provide comfort that such products continue to benefit from exemption?

Other limbs of the exclusion relating to the issuer's premises and a limited network of service providers have not changed materially and would be expected to continue to be applied in a similar manner to current exemptions under PSD1.

We would, however, welcome guidance on the meaning of the terms '*premises*', '*limited network*', and '*range of goods*' in the context of goods and services offered online.

We suggest recognition of the equivalence of online and physical means of reaching consumers, and explicit provision for online stores to be capable of meeting the geographic limb of the exclusion.

2. There is currently no definition of a 'professional issuer', nor of a 'direct commercial relationship'. It may be helpful if these were addressed by way of guidance. It will be important that 'direct relationships' would include arrangements where 'direct' contractual obligations

could be created by way of agency, reseller and similar intermediaries acting on behalf of the issuer. Similarly, a professional issuer needs to be defined to include all commercial providers of such services.

3. When is the notification required:

(i) In relation to the limited network exclusion notification requirements, and following a request for clarification, the European Commission has indicated to the EMA that notifications would be expected to commence 12 months following the implementation of PSD2, and that the first notifications would be expected in January 2019. Existing products would not therefore report in relation to the period prior to implementation of PSD2. This is to ensure that PSD2 is not implemented retrospectively. We would welcome confirmation that the same approach will be taken.

In order to allow existing service providers to adjust to the revised limited network obligations, we propose a 12-month transition period, which should commence at the time of implementation of PSD2 into member state law.

The EMA has entered into discussions with the European Commission, and this appears to be consistent with the intention of the legislation.

(ii) We suggest that there is little benefit in annual notifications and suggest that further notifications should be made only if the product proposition has materially changed in nature so as to impact the competent authority's original conclusions (following the first notification). Annual notifications would create an annual period of uncertainty, and a significant burden for competent authorities. We suggest the competent authority set out any boundary conditions in relation to exclusion in its response to the first notification, and the issuer can then notify if these boundaries have been breached or appear likely to be breached.

The uncertainty created by an annual notification process would likely have a chilling effect on business and discourage many potential offerings.

(iii) Additionally, guidance is required on the timelines for a response from the competent authority, provisions for an appeal procedure, timelines for transitioning to a regulated framework where possible and the process for winding up of product offerings that are not viable under the regulatory environment.

(iv) We propose that service providers should have certainty with regards to a time period by which they would be informed of the outcome of the review. A time period should be specified, after which the service provider can assume the relevant authority has no objection to their interpretation of the exclusion.

Industry would benefit from the setting out of a period of time after notification when the product notified could be regarded as not having given rise to any objections. Service providers need certainty with regards to the time period within which they will receive the outcome of the decision of the relevant competent authority. There should therefore be a specified time period for the competent authority (“**CA**”) to respond, after which the service provider can continue

to offer the service under the limited network exclusion and assume the relevant authority has no objection to the service being excluded from PSD2. This time period could be two months, which is consistent with other time frames set out in the legislation.

3. Electronic communication network (ECN) exclusion, article 3(l)

1. We suggest that a ‘subscriber’ is a person with a contractual relationship with the ECN provider, and could include a user with multiple contracts; could relate to work, personal and joint contracts. ECN providers should be encouraged to look out for abuse of the provision for criminal purposes, but this should not limit the number of contracts a user can legitimately have with an ECN provider.

2. The EMA regards the exclusion as extending to intermediaries in the transaction chain so as to take account of the role of aggregators and other parties that enable the payment service to be delivered. Any other interpretation would amount to the support of a particular business model over another, and would discriminate against business models that included an intermediary by requiring regulation for what amounts to the same purchase. The responsibility for tracking spending should, however, rest with the provider that holds the consumer relationship, as it is the only party in a position to track spending and implement appropriate controls.

3. We would like guidance to address the scope of the exemption in relation to ‘ticketing’, a widening of permissible services that can be purchased under this exemption and clarifying that ‘ticketing’ should not be used as a proxy to enable the purchase of physical goods.

4. Periodic reporting for payment institutions with agents or branches in host member state territory, article 29(2)

Reporting obligations will already be in place with the home country CA, and these will be undertaken periodically. It would be simpler to seek such data from the home country CA. Firms could distinguish data relating to business performed in different member states to aid in its dissemination. This would be preferable to firms having to report to multiple CAs in all member states where they have agents. In this respect, there is a significant distinction between agents and branches, where the volume or nature of activity may suggest a more direct relationship with the host member state CA.

5. Creation of central contact point for payment institutions with agents under the right of establishment with the head office in another member state, article 29(4)

1. We do not think that PIs operating under the right of establishment should have to set up a central contact point for the purposes of communicating with the host state regulator. Such a requirement would introduce an unnecessary administrative burden that would be unlikely to add any value.

(i) In practice, the CA is more likely to communicate with firms – and particularly smaller PIs – remotely (by email or by telephone). This is likely the case for firms that are authorised with the home Member State (“**MS**”), as well as those passporting inwards.

(ii) Firms’ data and internal systems are located centrally and are accessible at the head office of the firm. There is usually a compliance officer overseeing the payment product/service in all member states where it operates: this compliance officer is usually the most knowledgeable about, and familiar with, the product and the relevant compliance requirements. It is therefore more effective for this person (or team) to be known to the CA. If the CA wished to meet them in person, they could of course travel to the CA’s offices. Employing another person to simply be present in home MS for compliance purposes will be very costly and will not necessarily ensure greater compliance. It will rather increase cost and administrative burden with little demonstrable benefit. This is particularly difficult for smaller innovative PIs.

(iii) If needed, firms can provide the name and contact details of a specific person with whom the CA can communicate and who will act as the contact point within the firm at its head office.

6. Exemption from certain authorisation conditions – small PIs and small EMIs

One of the objectives of the ‘small’ institution regime is to allow prospective payment service providers to offer a limited service, under certain controls, and to assess the viability of the business. A proportionate supervisory approach is therefore also appropriate, and minimising reporting requirements, except where these are essential is preferred. We urge to create a light touch approach to registration, enabling innovative payment startups to enter the market and test their products.

7. Safeguarding funds and segregation in relation to fees paid by users

1. Payments where fees are paid by the payee: users making payments understand that part of a payment will relate to a fee for the service, but may not be aware of the fee component where the fee is paid by the payee; their payment obligation will relate to the entire amount including the fee. Segregation of the entire amount is therefore more consistent with legislation as the obligation to credit the payee does not arise until the next business day; in other words, on the first business day, the funds continue to be in transit, and could be claimed back by the payer.

2. Payments where fees are paid by the payer: other payments such as money transfer payments where the payer may pay a fee for the transaction should recognise that the payment executed by the payer will always comprise of the principal and a fee component. It would be unreasonable to ask the payer to make two separate payments in order to separate out the components, and to route the different components to different accounts. This was never the intention of the legislator. PSPs should be able to receive the entire payment into a segregation account, and to extract fees as they fall due. In other words, to recognise that the payer made a

payment for the entire amount and to seek to protect that. Once the PSP seeks to identify and apply a fee, then it is at this time that the obligation to separate out the fee becomes due.

3. It will of course always be the case that whatever is held in the segregation or safeguarding accounts will form part of the asset pool, irrespective of any potential fee component.

We would welcome confirmation that the above approach will be taken.

8. Distributors and agents

1. We distinguish the role played by an agent – which by definition acts as agent of its principal, and that of distributor. In most cases distributors resell e-money as principal, and may additionally undertake activities on behalf of the issuer. Where they act on behalf of the issuer, then the responsibility will lie with the issuer, but where the distributor acts in its own capacity, then the issuer is not responsible. Distributors do not undertake regulated activities, and there is no obligation to register distributors in PSD2.

2. Under current arrangements, where distributors are part of a network or group, the issuers have notified for the group as a whole and not individual retailers. This avoids the submission of excessive data, and the need to continually update changes to the group.

We would welcome confirmation that the above approach will be taken.

9. Definition of ‘sensitive payment data’, Article 4(32) and obligation not to store sensitive payment data, Articles 66, 67, 73(2)

1. The data covered by the definition of “*sensitive payment data*” in Article 4(32) should be limited to personalised security credentials (“**PSC**”) and should not include individual transaction data, payee whitelists and Personally Identifiable Information that are collected in the course of the customer due diligence process. There is, however, a difference in the scope of sensitive payment data that can be stored by a payment initiation service provider under Art. 66(3) or requested by an account information service provider under Art. 67(2). A PISP should be allowed to store transaction data for the transaction initiated through its platform; an AISP should be allowed to request a wider set of transaction data to present to its customer.

2. The PISP should be allowed to store adequate data to allow the PISP to demonstrate that “*the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown ... linked to the payment service of which it is in charge.*” (Art. 73(2)). This should not include PSCs issued by the account servicing payment service provider or transaction data for any transaction that was not initiated by the PISP.

10. The way/form of the explicit consent to a payment, in the context of the use of a payment initiation service, to be given, expressed and recorded, Article 66

1. Customer consent – to a payment initiated through a PISP – should be provided in a format that allows the PISP to demonstrate to the ASPSP that it has obtained legitimate customer consent for the attempted payment. The format can vary to reflect different inter-payment service provider communication models. These formats can include, for example, a customer electronic signature accompanying a transaction initiation request, or a software token delivered to the PISP by the ASPSP after the PISP customer has been authenticated by the ASPSP that manages the underlying payment account. The consent provided by the customer should be recorded by the ASPSP and the PISP to facilitate future dispute resolution procedures.

2. The restriction on storing sensitive payment data could be problematic if PISPs were to be subject to AML legislation; this will need to be considered. It is also important to evaluate the impact of existing data protection requirements on processes that can facilitate the sharing of customer behaviour-based characteristics. PSPs may find it difficult to demonstrate to external parties that they have complied with strong customer authentication requirements by using certain inference elements, if they are prevented from sharing such elements with external parties due to applicable data protection regulations.

11. Account information services (“AIS”) and payment initiation services (“PIS”)

1. Additional services currently provided that may be brought into PSD2 scope under a broad reading of the PSD AIS/PIS definition may include:

AIS Services:

- (i) Services that compare product features of different payment accounts based on an analysis of payment transaction data as well as product related information,
- (ii) Services that can execute transaction scenario analysis to identify transactions that can maximise savings (or minimise costs) for the payment service user (“**PSU**”) based on the current PSU financial position or the PSU profile held by the AIS. *The results of such analysis are presented to the PSU that may choose to authorise the execution of such transactions,*
- (iii) Access to a PSU’s identity information held by the ASPSP, as a means to confirm identity information within a risk based approach to mitigate the risk of financial crime
- (iv) In summary, any service whereby an AIS service providers provides added value information services based on access to the PSU’s transaction and personal information data.

The scope of AIS services contemplated at the time of drafting of PSD2 was limited, and focused on the aggregation of information from different sources. Increasingly, the opportunities offered by AIS services are focused on data analytics and automated decision making.

PIS Services:

- (v) Payment (credit transfer) initiation to execute transactions – previously identified by an AIS - that maximise returns for the PSU,
- (vi) Merchants, marketplace operators, merchant acquirers, and other PSPs establishing their own PIS to allow them to complete credit transfers from/to their customers’ payment accounts.

2. We would like to distinguish bilateral and contract based arrangements between a PSP and a partner that may involve the use of APIs to initiate payment transactions. Such arrangements are part of current product functionality offered by a PSP and should not bring the partner into the scope of legislation. Such partners could comprise platforms that enable their customers to initiate transactions through a contracted PSP.

12. Payment accounts ‘accessible online’, article 65

1. Some of these accounts only provide account status information online, others provide balance or transaction history details. However, the existing functionality of some of these accounts would not always be adequate to service an AISP or card based payment instrument issuer (“**CBPII**”) access request. For example, displayed account balance information may not be updated quickly enough to provide a real-time, updated picture of the account to allow these TPPs to offer their services.

2. CBPIIs would require ASPSPs to provide confirmation of availability of funds within 2-3 seconds of receiving the transaction authorisation request. We suggest CBPIIs are provided access to a process of notifying the competent authority if they continue to be prevented from offering their services due to lack of responsiveness by specific ASPSPs.

3. We stress the importance of ensuring that AISPs and PISPs are correctly identified as authorised and registered very quickly after they are authorised so that they can receive access to ASPSP payment account data.

4. We request that the competent authority clarifies how ASPSPs are expected to treat TPP payment account access requests in the period after PSD2 implementation and prior to the application of the RTS on SCA and common & secure PSP communication, particularly where TPPs do not identify themselves to the ASPSP in a secure manner.

5. We are of the view that it is important that the PSD2 transposition into local law ensures that:

- direct access can continue for non-payment accounts without restriction, and
- AISPs & PISPs do not risk their PSD2 license when continuing access to non-payment accounts.

13. Form, content and timing of notifications that must be provided where access has been denied to providers of AIS and PIS

1. We imagine that in many cases the blocking of all access to customer accounts by the ASPSP would be disproportionate and cause major disruption to the PISP/AISPs service. There should be an opportunity for the PISP to work with the ASPSP to reassure the provider, and address any issues, before they experience a total denial of access.

2. It would be helpful if the information in the notification form would be made available to the AISP or PISP in question. Greater transparency will facilitate the prevention of anti-competitive behaviour.

I4. Professional indemnity insurance

1. There is serious concern that the requirement for TPPs, PIs and EMIs to hold Professional Indemnity Insurance may (i) hinder the market for such services as the supply of such services is very limited if at all present, and (ii) create a distorted playing field if the cost is significant, as this will in effect create an additional transaction cost for such providers compared to credit institutions.

In order to increase the likelihood of insurers offering suitable product the CA is requested to define the scope of risk that is being insured, and to define this narrowly enough to enable insurers to assess and offer suitable cover. In the absence of such specification, the ability of insurers to offer suitable products will be limited, and where they do, these will be excessively expensive.

In the event of PII insurance being only made available at significant cost, the CAs should consider the means available to remedy the uneven playing field that will exist between credit institutions and other providers of TPP payment services.

2. We would welcome guidance regarding the specific characteristics of comparable guarantees and the criteria for their implementation.

We believe the existing own funds requirements for PIs and for EMIs under PSD2 and EMD2 are sufficient guarantees to cover any liabilities. We do not believe the ongoing capital requirement imposed on credit institutions for the offering of payments business is significantly different in quantum to that which results from the calculation of own funds for EMIs and PIs under EMD2 and PSD2.

The main difference is initial capital requirement, but Recital 35 of PSD2 states that PII is required because it would be disproportionate to impose an own funds requirement on PISPs and AISPs, and not initial capital.

Accordingly, we propose that PIs and EMIs should be excluded from the requirement to have PII when they offer payment initiation and account information services because they are already subject to own funds requirements.

This interpretation is not inconsistent with the provisions of level I text in PSD2 at Article 5(2) and (3) that refers to PII requirement when an entity applies for authorisation or registration to undertake PIS or AIS business. This text can reasonably be interpreted as applying to applicants seeking 'sole' authorisation for AIS and PIS services.

The rationale for such an interpretation and approach is the creation of a level playing field between Credit Institutions, EMIs and PIs offering such services. Sole providers of PIS and AIS

services that are not subject to ongoing own funds requirements, on the other hand, would be required to obtain PII cover.

15. Data protection requirements, Article 94(2)

1. Article 94(2) requires that a PSP obtain explicit consent from a PSU to process the PSU's personal data for purposes of providing payment services. Given that a PSP cannot provide a payment service without the explicit consent of the PSU to process his/her personal data for that purpose, this means when a PSU withdraws his/her consent he/she is ending the provision of the payment services by the PSP.

2. Under Article 7(3) GDPR the withdrawal of consent by a data subject does not affect the lawfulness of data processing by the data controller based on the consent before its withdrawal. This approach is not explicitly stated in the Data Protection Directive (95/46/EC) although the need for legal certainty means that it is implied under the current data protection regime.

3. We seek confirmation that, during the period from 13 January 2018 (when PSD2 is implemented) to 25 May 2018 (when the GDPR is implemented), the revoking of consent by a PSU for a PSP to process their personal data for the purposes of payment services will not invalidate the payment service user's consents/authorisations for all payment transactions initiated prior to the revocation of the consent. Please note that this request for confirmation does not relate to the revocation of individual payment transactions in accordance with the applicable framework contract.

16. Implementation of complaints handling requirements; Alternative Dispute Resolution, Article 101(2)

The PSD2 provisions provide a helpful means of creating a harmonised regime across the EU. Our members offer services in most EEA member states and therefore prefer the implementation of a single approach across the single market. We, therefore, support adoption of the PSD2 requirements.

17. Thresholds for low value payment instruments, Articles 42(2), 63(2)

We propose the introduction of the higher limits, which continue to be low in relative terms, and enable the offering of low value payment products to users without giving rise to significant risk. The products benefiting from this exemption generally have low profit margins, so this lighter regulatory regime allows them to be commercially viable for issuers, which in turn means they can be purchased by consumers. These products are valued by wide range of consumers, including:

- The financially excluded, who do not have the facility to make online payments;
- Those who might wish to protect their main payment account by limiting its online use for certain goods, or for day-to-day expenses;
- Those who desire privacy when making purchases;

- Those who wish to limit the amount that can be spent – for example parents giving their teenage child a card with pocket money;
- Travellers seeking an alternative to cash.

As the derogation only disapplies a limited number of provisions, the consumer will continue to benefit from consumer protection measures set out in the remainder of the relevant titles and PSD2 as a whole.

18. Providing for more favourable termination provisions for payment service users in relation to framework contracts, Article 55(6)

PSPs operating across the EU rely on the harmonised rules in PSD2 in order to be able to manage their compliance costs. PSD2 rules on termination already protect the consumer by not allowing the notice of termination to be longer than one month and by making sure it is free of charge subject to limited exceptions. In practice, in order to compete by making their product (and the T&Cs) more attractive to potential customers, many PSPs already offer more favourable terms to consumers by allowing them to terminate without notice and free of charge. We support the approach to avoid provisions for more favourable termination and that competition on such issues should be left to market forces. Providing for harmonised terms and conditions across the EU helps firms offer their products in all member states simultaneously, and ensure better consumer service is delivered.

19. Information for the payer/payee on individual payment transactions, MS options in Articles 57(3) and 58(3)

We propose a broad interpretation of provision of payment services to allow for new and innovative ways, for example, through apps. We would like the interpretation to include any action by the PSP, which allows the user to print or save the information. For example, a pdf provided on a website, information provided through a secure online account or in-app information. Using another example, we would argue that providing information in an online account (e.g. transactional information) is the same as sending it by email since both require the PSP to send the information to a particular user. The user has to open his email account to see the information in the same way he has to open his online secure account. Having to send an additional SMS just because the information is in the secure online account adds an unnecessary layer of obligation that does not give any additional benefits for the user, especially if the framework contract stipulates that the information will be provided in the user's online account.

We would like to propose that providing a pdf copy of the framework contract online during the registration process for printing or saving by the customer would also amount to providing it on a durable medium as the customer is able to save or print the framework contract. The online environment requires more flexibility with regards to how the information is provided. Furthermore, in any case, the customer can request a copy of the framework contract at any point during the contractual relationship free of charge.

If the transactional information is routinely provided to the user, e.g. online every time before execution of a transaction, where a payment order is initiated by the payer, we suggest that this would meet the requirement to provide the information at the user's request.

20. €50 maximum liability for unauthorised transactions, Article 74(I)

We are in favour of a harmonised approach (€50), as this simplifies customer support and dispute resolution, ensuring the best customer outcome. The low value may act to encourage users to protect their payment instruments and their means of authentication, and is therefore helpful without being onerous.

21. For national payment transactions, member states may provide shorter maximum execution times than provided for in Title IV, Article 86

Current execution times are harmonised across the EU and act as a minimum requirement. PSPs will act to offer faster execution times as part of their competitive service offering. There is a move across the EU and within the SEPA framework to instant payments, and once this is introduced, industry will deliver more rapid execution times to meet consumer expectation. We are of the view that there is no need to legislate for this outcome.

22. PSPs' access to payment account services

1. The provisions consider individual responses to applications for payment accounts by PSPs. We would like to see competent authorities take a more global view of the market and also collect and review data that would indicate the status of access in the market generally, and to act if the aggregate position did not result in a competitive market for such accounts.

2. We would welcome guidance on what would be considered reasonable time for CIs to respond to an application.

3. There is a concern that some credit institutions will try to create a pre-application process by which they would not treat pre-applicants as potential applicants. We would welcome guidance on how CAs will prevent this and ensure the intention of the provision (i.e. to provide access) is followed.

23. Reporting of statistics on fraud relating to different means of payment

We would encourage the competent authority to consider the similar fraud reporting requirements that apply to all PSPs that want to benefit from Transaction Risk Analysis-based exemptions to the PSD2 requirement to complete SCA. These requirements are detailed in Art. 16 of the final version of the *EBA PSD2 RTS on SCA and common & secure PSP communication*. It would be very useful if the scope/frequency of these fraud reporting requirements to competent authorities is aligned across these documents to avoid confusion and duplication of effort for PSPs.

24. Transitional provisions

We strongly support the grandfathering process as the new regime is approximately equivalent to the existing regime. Where there are departures, these can be implemented by providers as part of their adoption of the requirements of PSD2 more generally.

25. Application of Title III (provision of information by the PSP), Title IV (provision and use of payment services) and ADR procedures for the benefit of micro-enterprises, Articles 38(2), 61(2), (3)

We do not think micro-enterprises should fall under the same regime as that for consumers. Business-to-business contracts (regardless of whether there is a micro-enterprise involved) should be left to the parties to negotiate. This will allow the market to adapt and PSPs to compete in offering payment services with enhanced benefits and protections to micro-enterprises.

List of EMA members as of April 2018: <http://www.e-ma.org/our-members>

Advanced Payment Solutions Ltd	One Money Mail Ltd
Airbnb Inc	Optal
Allegro Group	Park Card Services Limited
American Express	Paybase Limited
Azimo Limited	Payoneer
Bitstamp	PayPal Europe Ltd
BlaBla Connect UK Ltd	PayPoint Plc
Blackhawk Network Ltd	Paysafe Group
Boku Inc	PPRO Financial Ltd
CashFlows	PrePay Solutions
Citadel Commerce UK Ltd	R. Raphael & Sons plc
Clearsettle	Remitly
Coinbase	SafeCharge UK Limited
Corner Banca SA	Securiclick Limited
Ebanx	Skrill Limited
eBay Europe Sarl	Starpay Global Ltd.
Euronet Worldwide Inc	Stripe
Facebook Payments International Ltd	Syspay Ltd
First Rate Exchange Services	Transact Payments Limited
Flex-e-card	Transact24 (UK) Ltd
Flywire	TransferWise Ltd
GoCardless Ltd	TrueLayer Limited
Google Payment Ltd	Uber BV
IDT Financial Services Limited	Valitor
Imagor SA	Vitesse PSP Ltd
Intuit Inc.	Viva Payments SA
Ixaris Systems Ltd	Wave Crest Holdings Ltd
Merpay Ltd.	Wirecard AG
MuchBetter	Wirex Limited
Nvayo Limited	Worldpay UK Limited