ETPPA Position Paper on PSD2 review

About ETPPA

ETPPA is the leading EU fintech trade association for bank independent Third Party Providers ("TPPs") under the EU's second payment services Directive ("PSD2") and beyond. ETPPA represents TPP interests on the key payment forums in Europe, such as the ECB's Euro Retail Payments Board, the board of the European Payments Council and several European Commission expert groups, in support of creating an innovative and competitive level playing field for Account Information and Payment Initiation Service Providers ("AISPs & PISPs").

Position Summary

ETPPA believes that:

- Out of PSD2's three main objectives (improving payments security, innovation and competition) only the first one (security) has been achieved, and arguably over-achieved.
- Unfortunately, PSD2 governance has not fostered any innovation and competition.
- PSD2 has opened the market in Member States, where banking was closed before, but it has not been as impactful as was originally intended, and it had the opposite effect in others, where banking was more open before.
- ASPSPs and TPPs have invested huge sums of money and time in trying to make a regulatory approach work.
- Both were unnecessarily "forced" to develop and use dedicated interfaces based on new (API) technology, which in most cases was badly implemented either on purpose or by ignorance.
- Enforcement of "good APIs" under the current regime has not proven to be effective. The customer interface should always be accessible to TPPs to ensure availability and to encourage good APIs, which TPPs want to use.
- Open banking (and open finance) will work much better with less regulation and more industry-driven approaches, e.g. SEPA API Access Scheme, now SPAA MSG.
- The vast majority of the EBA guidelines, opinions and Q&As have been to the advantage of ASPSPs and therefore hindering innovation and competition by TPPs.
- The EBA interpretation on the SCA rules, which can be performed only for the ASPSP and not by and under the responsibility of the TPP, impacted in a negative way the AIS business.
- Overall, we can say that an RTS2 is much more needed than a PSD3. Therefore, many of our suggestions focus on setting a much more progressive and tighter frame for any future RTS. We plan to provide detailed suggestions to that effect.

Main ETPPA asks for PSD2 review:

- PSD2 regulation should not increase in scope, but fix the core issues properly.
- Its governance must change and should involve the competition authorities.
- PSD2 & RTS must become outcome driven and avoid or minimise any technical prescriptions.
- Any room for interpretations, which could lead to detrimental 2nd or 3rd-level legislation, must be avoided.
- Both banks and TPPs must be given a choice for their interaction
    - The ASPSPs choice of providing a dedicated interface or allowing the use of their user interface(s) (whether API-based or not) must be reciprocated by giving the TPPs the choice of using the dedicated interface or the user interface(s)
- This simple principle would have avoided the vast majority of problems we have had over the past 3 years, because:

    - TPPs have numerous genuine reasons for preferring API-based dedicated interfaces if they adequately perform
    - However, ASPSPs must be incentivised to provide good APIs, by allowing alternative access.
    - This would enable much more competition from TPPs most of which act cross-border
    - It would allow innovation on a broader perspective rather than what is offered by narrow APIs
    - It would increase transparency and allow data parity, when ASPSPs cannot hide behind a too narrow API
    - It would provide more choice for users on the whole range of banking services
- Account access SCA should not be required or at least just the exception, not the norm.
- PISPs must be allowed account access prior to finalising a payment initiation to allow non-execution risk mitigation.
- It must stipulate a good outcome for PSUs as an overarching principle.

Main PSD2 problems encountered by ETPPA members

PSD2 was meant to foster innovation, competition and security in the payments industry. The outcome of that to date depends heavily on the country being looked at. Where banking was rather closed before, e.g. UK, France and Southern Europe, PSD2 has played an important role in removing some barriers to innovation in retail payments and fostering competition, although it has not been as impactful as was originally intended. Where banking was already quite open beforehand, e.g. Germany, Austria, Nordics, we see a big step backwards.

The outcome also varies depending on the maturity of a TPP, and in particular whether it existed already before PSD2 or not:

Existing PISPs (pre-PSD2)

- high cost for implementing new API technologies
- high cost of maintaining legacy technologies due to APIs not working properly
- uncertainty cost due to complex and unclear legislation that is generally interpreted in a way that protects ASPSPs at the expense of TPPs.
- Increased friction leading to lower conversion rates due to bad redirections
- increased risk due to reduced data access, which disabled non-execution risk mitigation
- licensing burden
- on the positive side: wider reach, due to EU-wide access

New PISPs

- the dedicated interfaces provisions have given hundreds of TPPs the ability to enter the market and provide payment initiation services to consumers
- new API technologies not sufficiently well implemented and maintained by ASPSPs, and alternative access is too costly to develop
- no payment certainty (no access to risk mitigating data via APIs)

Existing AISPs (pre-PSD2)

- high cost for implementing new API technologies
- high cost for maintaining legacy technologies due to APIs not working properly, and because it is required to access non payment data, which AISPs typically require.
- uncertainty cost due to complex and unclear legislation that is generally interpreted in a way that protects ASPSPs at the expense of TPPs.
- 25% reduction in conversion rates due to the introduction of undocumented and untested SCA at the customer interfaces which is required to be overcome by the legacy technologies whilst APIs do not work properly.
- Significant reduction in the functionality and data available through APIs
- Increased complexity due to not all payment data being in scope of PSD2 in all countries (i.e. credit cards or savings accounts)
- on the positive side: wider reach, due to EU-wide access

New AISPs

- the dedicated interfaces provisions have given hundreds of TPPs the ability to enter the market and provide account information services to consumers
- new API technologies not sufficiently well implemented and maintained by ASPSPs, and alternative access is too costly to develop

PSD2 governance and supervision

Neither the EBA nor the National Competent Authorities are mandated to foster innovation and competition. Therefore, they have focused solely on PSD2's third objective, which is the improvement of security. Some PSD2-NCAs are also in charge of the prudential supervision of credit institutions, which even causes a conflict of interest with the competition objective.

Prudential supervision and the fostering of innovation and competition must be clearly separated to avoid that the former is always prioritised over the latter. Non-bank PSPs (PIs, EMIs and TPPs) are fundamentally different from credit institutions and should be supervised in a different way and by different entities.

In our experience, there appears to be good collaboration amongst some NCAs and the EBA, but not amongst others. Hence, there are significant differences to be seen in the markets, which are leading to serious discrepancies. It would be preferable to strengthen the central authority and give it more influence to ensure a more harmonised approach across the EU.

We, therefore, need a fundamental change of PSD2 governance, whereby either the mandates of the EBA and NCAs are brought in line with all PSD2 objectives, or other entities are given this role. Our preference is clearly for the latter, because changing mandates can be done overnight, but changing mind sets typically takes a generation. The Open Banking approach in the UK has shown that it might be beneficial to involve the competition authorities in a more decisive manner.

PSD2 scope

The inclusion of AIS in the last minute was not done with enough understanding and foresight of such services. Most of our AISP members believe that there is insufficient justification for being considered as a payment service at all.

However, some of our members fear that de-scoping AIS could lead to the blocking of access by ASPSPs and would rather accept their PSD2 obligations in return for the PSD2 rights they are given. That said, it should go without saying that any data holder in any industry (including banking) cannot be allowed to block real-time account access by the data owner or a third party acting on their behalf, if technically possible.

Data access and data sharing

The openAPI model has enabled many new companies to enter the market, but the implementations by the EU banks have been poor, with very few exceptions. The vast majority of them have taken a minimal compliance approach and have not even achieved that, because most of them still contain numerous obstacles, and we are still waiting for the EU authorities to enforce compliance with their minimum requirements.

The situation is particularly difficult for TPPs which existed before PSD2 and which were forced to change their existing (and well-working) "direct access" technology to low-quality, low-performing API implementations.

Banks/ASPSPs were given a choice of developing and implementing additional dedicated interfaces or just simply allowing access via their existing user interfaces with minimal effort and cost. Please note that TPP-identification is mandated on TPPs, not on banks, and can be done unilaterally by TPPs without changes in the user interface. TPPs, however, were not given that choice, but were forced to integrate and use these dedicated interfaces, where they were made available. Almost all ASPSPs chose to do that, despite the much higher cost and lack of compensation, which can only be explained by the fact that they saw other benefits for that under the regulatory circumstances. Given the low quality of most APIs and the number of obstacles built in, this was obviously done to create a bottleneck so that TPPs could not compete on par with the ASPSPs' own services provided via their user interfaces.

In addition, it must be noted that the implementation cost for TPPs was disproportionately higher, because:

- many APIs had to be implemented within a relatively short amount of time
- sandboxes were practically unusable and had no resemblance with the final API, so that most integrations had to be done twice or even more often
- ASPSPs abused TPPs to do their alpha and beta testing (they did very little testing of their own, and instead let the TPPs discover all the problems and report them)

And even after all this work, it was not possible to replace the pre-existing direct access technology due to the API underperformance, so that TPPs now have to maintain both technologies.

Furthermore, the SCA for access to bank accounts, which the EBA said could only be performed by banks and not TPPs, impacted in a negative way the customer journey, with no impact on fraud rates, as there was no fraud linked to access to bank accounts. Instead, this required TPPs to add yet another (mobile) direct access technology to avoid customer presence for the SCA, as provided by the RTS Art. 36(5b). Consequently, many TPPs now have to support not one, but three account access technologies, which has increased their cost base dramatically.

This situation is untenable and must be remedied as soon as possible. Free access via user interfaces must always be an option (being able to use “the stairs if the lift is not working”), so there cannot be any fallback exemption, to:

- avoid monopoly pricing of any chargeable interface
- ensure data parity between all interfaces
- ensure redundancy, as even the best of all APIs will fail one day

Given the cost of direct access, and the many reasons why TPPs favour APIs over browser-based user interfaces, there is sufficient room for ASPSPs to make a sufficient margin on their APIs, if and when they want them to be good.

This situation also explains why the initial growth of TPPs in some countries has slowed down considerably and while it has never materialised in some other countries, in particular in the South of Europe, where API exemptions are the norm, not the exception, despite their significantly under average quality.

API standards

API technology is good in principle for the provisioning of dedicated interfaces as defined in PSD2, but the banks’ use of this technology has been dismal, generally speaking. Most API implementations are performing poorly and have a significant number of obstacles built in. Most TPPs had to use alternative technologies to access the payment accounts via the banks’ user interfaces, which are performing at a much higher level.

One problem with many APIs is that they venture outside of how APIs typically work. APIs typically exist to facilitate the exchange of data (only) whereas PSD2 APIs implemented by ASPSPs often also involve user experience (user interface) requirements, e.g. that the user should be redirected to the ASPSP’s domain as part of the payment journey. We need to have APIs that are more narrow in scope (exchange of data only) but do that very well (speed, stability, load-wise).

There is not much advantage in further standardisation of the APIs, as different ASPSPs have different core banking systems and different data and online banking products offered to the users. A narrow standard would imply a “least common denominator” approach which would have adverse impact in terms of functionality, stability and competitiveness of the API. Rather, we need a great API provided by each ASPSP which can then be integrated by multiple TPPs.

Some API standards have been extended with so-called premium API standards so that they can be used beyond the scope of PSD2. Some others have stuck to their minimalistic approach.

Going forward, we are advocating for an industry-led, commercial approach, which can and must use such premium APIs that will allow competitive services - see SEPA API Payment Access (SPAA) scheme.

One should not forget though that "User Interface" technology is the most rapidly moving goal post in our industry. APIs are state of the art today for text based data, but voice interfaces, augmented reality, virtual reality, metaverse interfaces will come rapidly.

We must avoid and remove any technology dependency from PSD2 and the RTS. Neither APIs nor any other technology should be given any preference, let alone being mandated. And please note the difference between an API and dedicated interface. There are different types of interfaces, e.g. user interfaces or (TPP-)dedicated interfaces, and then there are different technologies to provide these interfaces, e.g. online browsers, mobile apps or APIs. We can expect more and more user interfaces becoming API-based, too.

SCA and risk under PSD2

The security improvement objective of PSD2 has been achieved mainly by regulating TPPs and by introducing the concept of SCA, which is largely shouldered by the end user. Any unnecessary use of SCA results in pure inconvenience without any risk mitigation, which is for example the case in many if not most ASPSP APIs, which require two or more SCAs in one flow or session. It makes sense to require 2 keys (factors) for a stronger authentication, but it does not make sense to require the same 2 keys twice or multiple times.

Unsurprisingly, the inflation of SCAs is leading to an "SCA fatigue", whereby consumers are using simpler factors and paying less attention to the process, which is an important other reason for avoiding any unnecessary SCA.

Alternative approaches, involving more risk management on the payee side, are hardly recognized. Going forward, it would be desirable to shift the security overhead from the end user to the corporate entities in the ecosystem by enabling more SCA exemptions, especially risk-based ones.

AML and categories of PSP's

There is a consensus among regulators that the use of AIS and PIS does not increase the risk of money laundering or terrorist financing to any significant extent. The EBA has recognized and highlighted that "AISPs are not involved in the payment chain and do not hold customer funds", and "PISPs do not themselves execute the payment transactions or any transfer of funds or enter into the possession of any funds". ETPPA therefore believes that AISPs and PISPs should not be brought into scope of the (ongoing proposed) AML Regulation as their services are entirely contingent on accessing just a subset of the data available to the banks and are, by their very nature, ancillary to the payment services provided by banks.

Furthermore, it must be understood, that Customer Due Diligence/KYC obligations resulting from AML regulation, for the "acquiring of payment transactions" can only relate to the payee (the merchant), and not the payer also when one and the same entity acts both as PISP and acquirer of the payments. We must not allow a situation, where payers would have to be subject to customer due diligence as part of the payment flow, no matter how often they are using a PISP for single payments.

The listing of AIS and PIS in PSD2 Annex 1, has brought them into scope of AML directives and the proposed new AML regulation, because the "payment services" listed in this Annex 1 are referred to from the annex of the Credit Services Directive. It is therefore important to remove AIS and PIS from PSD2 Annex 1 and create a separate Annex for them.

In addition, PSD2 Art. 45(2) should be changed, because it should not be a necessity for PISPs to provide or make available their business information to the payer. Otherwise, PISPs could not effectively compete with card payments, where neither the card acquirers nor the card processors have such obligations, and consumers would never need nor request such information.

Definition of a 'payment account' and 'online payment account'

The CJEU decision of when a savings account is a payments account makes sense, but there should not be any discriminate legislation, which would unnecessarily restrict any customer accessing their data no matter what type of account it is in.

The solution for this is not to bring more account types into the scope of PSD2, which is and should be limited to payments, but to ensure that any horizontal data access legislation, e.g. GDPR, is not discriminating any industry sector and type of data or account. Data Owners, both private and corporate, must be able to use their data no matter where and by whom it is stored. If it is accessible online, e.g. via a user interface, this access cannot be restricted to manual use. Automated access by the owner or an authorised third party cannot be blocked independent of the technological nature of that user interface, be it based on APIs or not.

Of course, any Data Holder storing and using private or corporate data is free to offer additional, dedicated (and potentially commercial) interfaces, which may allow mutual benefits, but these cannot be given a monopoly status, i.e. Data Owners must be able to access their data in alternative ways.

The CJEU case law explains what a payment account is, but does not say what an 'online' payment account is. Some ASPSP (at least in France) use a protocol (called EBICS T) to allow their clients to access payment accounts without any SCA. This protocol (with no SCA) competes with the PSD2 AIS activity, where the SCA is mandatory. ASPSP's surprisingly argue that the access to the payment accounts through EBICS are not 'on line' access to payment accounts. However, from a technical point of view, this protocol is an Internet access (https) similar to AIS PSD2 API access. ETPPA is in favour of a definition of an 'online' payments account, in order to have the same SCA rules applied for the same activities (access to payment information).

PSD2 consent management

The level 1 text must make it fully clear that it is the TPP that handles the consent of the user and that this is done without involvement of the ASPSP.

PSD2 consent management seems to have a number of discrepancies with GDPR, which must be resolved. The EDPB has provided guidelines to the interplay between PSD2 and GDPR, but these are not acceptable from the payments industry perspective, hence another solution is needed.

Therefore, PSD2 must be fully brought in line with GDPR and should not use the term consent in any incompatible way. For example, GDPR allows several legal grounds for processing PSU data and all of them must be allowed from a data consent perspective, including the use of "explicit consent" rather than stipulating contracts.

The concepts of consent, authentication and authorisation must be clearly distinguished.

Rules regarding framework contracts and single payment contracts

With PSD2 there have been some improvements to both framework and single payment contract stipulations required, but most importantly it must be clarified that some service providers can act without any contract requirements on the payer side at all. There are currently different views on whether that is possible, in particular for (merchant-facing) PISPs, which are leading to competitive disadvantages compared to Card Acquirers and Card Processors.

Payments can be initiated by the payer or by the payee and since PSD2 also by a PISP, who can act on behalf of the payer or (in the merchant-facing case) on behalf of the payee. Merchant-facing PISPs need consent from both the payer and the payee/merchant to initiate a payment between the two, but they are acting solely on behalf of the merchant and a contractual relationship is only needed there. In this case, only the payee can instruct or insist on the initiation, not the payer. On the payer side, it is therefore sufficient to obtain (GDPR-type) consent without the need for a single payment contract.

This is different for the "execution" of the payment, which does require a single payment or (more usually) a framework contract between the payer and the payment executer, i.e. their ASPSP, and this does also define the execution authorisation, e.g. via SCA. Hence, in the end it is always the payer who has control over the execution of a payment, even if it was not initiated by them or on their behalf. The change of framework contract conditions should require the active acceptance of the PSU. Implicit (silence means agreement) acceptance should not be allowed.

PSD2 clearly differentiates between the payer, the payee and a PSU, who can be either or both, which is indeed very important. It would be similarly important to better differentiate between the initiation and execution of a

payment, and clarify that PISPs are a) only involved in the former, and b) can do this on behalf of any PSU, not just payers.

PSD2 and the move to open finance

Payments have a high risk of fraud so that the movement of funds must be protected specifically over and above other types of transactions. PISPs do not execute any transactions, i.e. do not move any funds, and must be clearly distinguished from other "payment services" which do move funds and therefore should be in scope of AML. However, PISPs do initiate payment transactions, which does warrant their inclusion in an appropriate vertical regulation as defined by PSD2.

In contrast, account information access, where payments are not initiated, let alone executed, i.e. where money is not being moved at all, does not create any risk, which would not occur in other industries as well. Health data, location data, email data, tax data, investment data must be protected in the same way as payments data - no more, no less.

Data protection, and that includes data access, is a horizontal issue, across all industries and is (heavily) regulated by GDPR. Any sector specific regulation can lead to unfair differences. An example of that is the current need for payment account access SCA, at least every 90 days, which is not required for any other type of account. This restriction is not justified by any evidence of risk or fraud reduction and should be removed.

Health data, location data, email data, tax data, investment data must be protected in the same way as payments data, savings data and credit data - no more, no less.

Furthermore, the term "data sharing" must be avoided completely in the context of PSD2. PSD2 is about safeguarding payments and payments data, whereas the term "sharing" implies the opposite and has therefore become extremely toxic. PSD2 has nothing to do with data sharing. It allows users to unlock their payments data held by their bank so that they can use value-added services based on that data and provided by 3rd parties rather than being limited by the offers of their bank.

The use of TPP services is about "Unlocking & Re-using My Data for Myself", which means:

- Enabling MYSELF to use value-added (3rd party) services
- Granting access as needed for the service, whereby the 3rd party requires my explicit consent
- I may have to provide access keys if needed, but keep full data ownership and full control
- 100% confidentiality is required and 100% safeguarding is imposed
- I am NOT "sharing" any data whatsoever
- An analogy would be giving your keys to the neighbour
    - to water the plants and empty the mailbox
    - not to share anything with them!

In contrast, "Sharing My Data with Others" means:

- Enabling OTHERS to use my data
- Giving away the control over my data and usually, giving away data ownership
    - e.g. selling data for money, exchanging data for a service or for other data, or donating data for the public good, etc.
- For this, I would not provide any confidential data, let alone any access keys
- There is either no confidentiality required or guarded by a contract, i.e. no trust needed
- Analogy would be a Garage/Yard sale
    - taking your household goods outside
    - sell them to others