



OFA Position Paper on the Payment Services Regulation and the third Payments Directive (PSR/PSD3)

October 2023

Summary

The Open Finance Association (OFA) welcomes the European Commission's [proposal](#) on payment services in the internal market and amending Regulation (PSR) and the [proposal](#) on the third Directive on payment services and electronic money services in the Internal Market (PSD3).

We support the Commission's approach of a 'natural evolution' to the current rules in the second Payments Services Directive (PSD2). They hold the potential to further empower consumers and businesses by enabling them to use more of their financial data and account functions via regulated third parties.

OFA supports a more consistent and uniform application of rules for digital payments in the EU which fosters clarity and brings a harmonised regulatory approach across the Member States. This will create an environment more conducive to achieving the European Commission's vision for an integrated, modern and safe EU payments market.

OFA believes the key focus areas for the PSR/PSD3 are:

- **Improving open banking** through better APIs and establishing a minimum, uniform functionality for data and payment initiation services.
- **Improving SCA implementation** by focusing on removing obstacles and enabling higher quality user experiences.
- **Ensuring a consistent application of the rules** through a more active and engaged supervisory model and increased transparency.

Why the proposed changes in the PSR matter

We welcome the increased focus on open banking compared to PSD2.

PSD2 introduced groundbreaking rights for consumers and businesses to access their transaction data and initiate payments through regulated third parties, using secure dedicated interfaces. It led to investment and innovation benefiting consumers and businesses across the EU.

PSR is an opportunity to enable further innovation and competition in digital payments. It promises to address some of the inconsistencies in how these rules have been applied, which has resulted in a fragmented rather than coherent single market for open banking services, and constrained the growth of market entrants. A clearer definition of baseline requirements for both data and payments



services, together with more robust enforcement, will unlock more innovation by open banking providers, and stimulate adoption by giving more European consumers and businesses access to AIS and PIS-based services.

Together with the changes to the Instant Payments Regulation (IPR), the EU has the opportunity to develop an open, pan-European, real time, account-to-account payment method that will be compelling for both merchants and consumers, providing a competitive alternative to card payments, and will help to drive the growth of the EU's digital economy.

We look forward to working together with EU institutions and with our industry partners to achieve this shared vision of an open, innovative, and balanced payments ecosystem - and beyond into open finance through the Financial Data Access regulation.

Contents:

- [Open banking](#)
- [Strong Customer Authentication](#)
- [Security and fraud](#)
- [Enforcement and supervision](#)
- [Definitions](#)
- [Re-authorisation for payment and e-money institutions](#)
- [Access to payment systems for non-bank PSPs](#)

Open banking

1. An API-only approach

OFA welcomes the API-only approach of PSR, where the priority is creating excellent AIS and PIS connectivity via the dedicated interface (see recital 61 and article 35.2).

PSD2 included the obligation for most ASPSPs to effectively maintain two separate interfaces. Usually, they implemented an API as the dedicated interface and a fallback interface, often a modified customer interface (MCI) based on screen scraping. The obligation to have two separate interfaces took away resources from financial institutions as well as focus from delivering excellent API connectivity.

The PSR removes the obligation to permanently maintain another interface as fallback for the purpose of data exchange with account information and payment initiation service providers (AISPs and PISPs). This reform will ensure ASPSPs focus more on well performing APIs and consistent baseline functionality – helping to address the twin challenge of variable performance and functionality that AISPs and PISPs have struggled with up to now.

PSR also introduces the concept of ‘latency parity’ with customer interfaces in Art. 36, requiring the response times of dedicated interfaces to be at least as good as the response times of customer interfaces. Fast API response times are essential, as PSUs will cancel or abandon payments if the redirection or loading screens take too long. While the parity approach may lead to some improvement in response times, relative to the current situation, we are concerned that it may also have the unintended consequence of leading to downgrades in performance, where customer interfaces are performing more poorly than PSD2 APIs are today. For open banking payments to compete successfully, the latency of APIs must compare favourably to the latency inherent in card payments.

Furthermore, the articles on statistics regarding APIs availability and performance are more detailed and prescriptive in PSR. We welcome the intention of increasing transparency around API use by requiring ASPSPs to publish regular statistics on the number of total and successful AIS and PIS requests, as well as the overall PIS transaction volume. However, we believe a centralised monthly reporting cadence, as is the [case in the UK](#), would shine a more powerful light on market trends, to help public authorities assess how the market is developing and act where performance is lagging. These statistics should be compiled and closely monitored by NCAs or an appropriate central body.

OFA supports that the use of exemptions from the API requirements should be extremely narrow in order to make sure that the objectives of PSR are fully achieved.

OFA recommendations:

OFA supports the overall PSR focus on improving API connectivity and performance. We would like to see a narrow definition of exemptions from implementing dedicated interfaces.

Regulatory technical standards should establish clear guidance and criteria as to what API response times (Art. 36. 1, c) should be, which should not be defined by parity with the response times of customer interfaces but by parity to other competing payment methods such as cards.

ASPSPs should provide monthly statistics on the total and successful AIS and PIS requests, as well as the overall PIS transaction volume and value - instead of quarterly.

NCAAs should aggregate and closely monitor API availability and performance data from their respective ASPSPs.

We also recommend clarifying that the provisions of Art. 36.1 are explicitly in scope of the EBA regulatory technical standards according to Art. 89. Clear requirements for API response times will ensure a consistent level of service among all ASPSPs.

2. Contingency measures

PSR recognises that the fallback mechanism has been a distraction from creating the highest quality of API connectivity, and also that it encouraged less secure and less versatile methods like screen scraping.

The contingency mechanism under PSD2 requires a TPP to have the capability to screen scrape or to reverse engineer a customer interface (or to reverse engineer bank application APIs). The majority of TPPs, which entered the market after PSD2, do not access accounts via screen scraping or reverse engineering. Instead, they have focused on API connectivity, which is a more secure, pro-competition, and versatile method. Therefore, the fallback mechanism does not function as a viable contingency mechanism for most TPPs – in fact it creates an unlevel playing field.

PSR narrows the scope for TPPs to use screen scraping or reverse engineering-based methods for accessing accounts, but does not create a viable fallback method for most TPPs. We believe a combination of escalating incident reporting to NCAs by ASPSPs experiencing outages, real-time updates from ASPSPs to TPPs about outages, and the possibility of supervisory action against ASPSPs in the case of major outages, would be more effective.

OFA recommendations:

Instead of a contingency mechanism:

- ASPSPs should be required to open incident reports with their NCAs when their APIs become unavailable, similar to the process that ASPSPs would follow if their customer interfaces become unavailable for PSUs.
- Major API outages (beyond one day) should be reported to NCAs by ASPSPs as major incidents.
- NCAs should be required to monitor the duration of the outage and take supervisory action against ASPSPs for outages longer than one day.

- During the course of the incident, TPPs should be able to receive real-time updates on the issue so that they can communicate appropriately with their customers. These updates should be provided ideally through an API.
- NCAs should be required to make a dedicated contact available to TPPs for escalation of issues where the ASPSP is non-responsive to TPP enquiries relating to potential non-compliance with dedicated interface requirements (such as performance or functionality).

3. **Baseline functionality: beyond parity**

The “data parity” principle in PSD2 has been useful but has also shown its limits, for example where TPPs are not able to receive useful information after the payment initiation stage (and thus not able to provide a “complete” payment service by informing their customers about causes of payment rejection), or where basic information like the name of the account holder is not made available in the API because it is not displayed on the front page of the online banking portal (the EBA has clarified that the name of the account holder is not sensitive information - this must be reinforced in PSD3 or the SCA RTS.)

ASPSPs should not be required to provide new products in order to meet the minimum functionality, however there should be a requirement to provide sufficient functionality to enable account information and payment initiation services that can provide value to PSUs.

OFA recommendations:

PSR must go beyond the PSD2 concept of ‘parity’ to ensure consistent access to basic payment functionality and account information.

OFA supports the introduction of a PIS and AIS baseline functionality in Art. 36 which will constitute a significant step forward towards consistency and will encourage user adoption.

For AIS, we support the minimum functionality in the draft PSR, which includes the ability to request and receive information on payment transactions, and see the account’s unique identifier, associated names of the account holder, and the currencies available to that PSU. The baseline should also include the **full** account holder name, regardless of how it is displayed on the customer interface, to enable account verification and provide certainty.

For PIS, we support the minimum functionality list under Art. 36.4. We also strongly support the goal behind Art. 36.5 and Art. 37.3 to provide PISPs with information about payment execution after the payment has been initiated. The ability for a PISP to receive a payment status from the ASPSP to confirm to the merchant whether a payment has been executed or rejected is essential for a minimum level of PIS service.

We also note there is an emerging commercial space through the [SEPA Payment Account Access Scheme \(SPAA\)](#). Industry initiatives with premium functionality going beyond the PSR requirements will be an important complement to the PSR and will help drive adoption of open banking-based

data and payments services. We support premium functionality such as Dynamic Recurring Payments or payments to multiple counterparties being made available through industry schemes. The European Commission should monitor the adoption of the SPAA scheme and consider measures to encourage participation.

4. API access model: prohibition of contracts

We support the approach taken by the PSR proposal, and justification in the accompanying impact assessment, of maintaining the prohibition of contracts approach of PSD2 (art. 34.1).

Under PSD2, ASPSPs are required to provide access to their customers' payment accounts to PISPs at no cost and without needing a contract between the bank and the PISP. This model has stimulated competition and market entry, and has kept the cost base for open banking providers low. In turn these providers are able to offer cost-effective payment initiation and account information services to PSUs.

Removing the free model for API access "would be a total reversal of the approach taken in PSD2 and applied since 2018, risking significant upheaval possibly with a detrimental impact on the open banking sector. It could also harm competition as many smaller TPPs would probably be obstructed by this financial barrier" ([PSR and PSD3 Impact Assessment Report, 2023, page 47](#)). It risks creating an expensive and inefficient system that replicates card payments, severely hampering competition.

According to the [Study on the application and the impact of PSD2](#) the combined costs of the banks for the construction of PSD2 API interfaces built by ASPSPs were estimated by ASPSPs themselves at EUR 2.2 billion. This is not an exceptionally high cost if divided across the number of EU banks providing payment accounts, or if measured against the overall banking sector profit since PSD2 entered into force.

Overall cost of API implementation	€2.2bn
Number of EU banks	5441
Number of EU banks with PSD2 APIs	1000 (est)
Cost per bank	€2.2m

		Cost of PSD2 APIs vs profits
Overall cost of API implementation	€2.2bn	
EU banking sector profit 2022	€158.1bn	1.4%
EU banking sector profit 2015-2022	€981.7bn	0.2%

Requiring TPPs to enter into contractual agreements with hundreds if not thousands of ASPSPs would also be unrealistic and would cause severe disruption to the market, as the Impact Assessment Report again notes.

Therefore, we welcome the European Commission's approach to maintain the current prohibition of contracts in PSR.

Premium open banking services

Beyond the baseline open banking services outlined in the PSR, there is ample room for industry collaboration towards added-value, commercial services, both bilaterally and through multilateral forums like the European Payments Council's (EPC) SEPA Payment Account Access (SPAA) scheme.

OFA has closely supported and contributed to the development of the SPAA scheme. We believe SPAA has the potential to deliver enhanced open banking functionality on a commercial basis and to act as a template for broader future premium open finance services (as envisaged under FIDA). Version 1.1 of the SPAA rulebook was published in June and detail on the default business conditions, including fees, is expected to be published shortly. It is critical that these fees are set at a level that enable all ecosystem participants to deliver commercially competitive propositions to their customers.

OFA recommendation:

The PSR must maintain the current approach of free API access with no contractual requirement.

This emerging model, with a free and clearly defined baseline (or "compliance") functionality and separate, commercial space for value-added open banking services that go beyond the PSR baseline, is the foundation for a sustainable European open banking ecosystem, and will deliver the most benefits for both businesses and consumers.

Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) has been a positive force in building trust and increasing security in the digital payments market and in the broader economy.

In open banking, SCA applies each time a user accesses their payment account online, initiates an electronic payment transaction, or carries out any action which may imply a risk of payment fraud or other abuse. It is built into open banking payments, and is always performed by the bank with which the user has a payment account.

1. Obstacles to open banking and the importance of user experience

The application of SCA is a key part of the payment journey and an important element of the overall user experience. It varies between banks and between Member States, and significant obstacles remain in place resulting in users defaulting to more familiar methods like cards. Many open banking journeys continue to require unnecessary manual input (for example, consumers having to type in their own name or IBAN), numerous consent screens, and even multiple authentications. This discourages use and limits overall adoption.

Unfortunately, many of these obstacles, which were identified by the European Banking Authority in 2020 in its [Opinion on obstacles under Article 32\(3\) of the RTS on SCA and CSC](#), continue to exist

despite the EBA's guidance that National Competent Authorities should remove them, and they impose artificial limits to the uptake of open banking payments.

OFA recommendations:

OFA welcomes the intent behind Article 44 of PSR which lists and prohibits obstacles to open banking. However, the list should be non-exhaustive and should be able to capture new types of obstacles that would arise in the future. We recommend that Art 44.1 is amended to include the explicit mention that: "Prohibited obstacles shall include **but not be limited to** the following" (...).

We support prohibiting the restriction of payment initiations to or from domestic unique identifiers only. However, the PSR must also account for more subtle cases of **IBAN discrimination**, where so much friction has been put in place that in practice it becomes extremely difficult for the payer to complete the payment journey. The PSR should reinforce the current requirements in the SEPA Regulation and prohibit making cross-border SEPA payment journeys more difficult than domestic payments.

We also recommend establishing a central registry of reports coordinated by the EBA, relating to problems with ASPSP dedicated interfaces and obstacles to SCA, including public identification of the ASPSP in question, whether such problems have been resolved, or are still open, and tracking how long they have been open for. This transparency would incentivise addressing the issues in a timely manner.

We welcome the EBA's remit to develop regulatory technical standards which enable "the development of user-friendly, accessible, and innovative means of payment" (PSR Art. 89, 2). Customer experience guidelines can work well to standardise and improve customer journeys, and to promote trust and adoption of open banking. We think an explicit focus of these RTS should be driving more consistent and harmonised end-user open banking journeys.

The PSR should explicitly prohibit embedded SCA flows for open banking. Such approaches are inherently less secure than other approaches (such as decoupled and redirect), and are both confusing to consumers and limit consumer appetite to engage with open banking (given confusion and/or concern about providing their banking credentials directly in the TPP domain).

In addition, we recommend more monitoring of 'conversion rates' by the EBA i.e. the proportion of customers that complete an open banking journey. This is a performance criteria that can be used to ensure bank authentication screens are good enough to be used for AIS and PIS.

2. SCA for AISPs

Article 86, 4 of PSR prescribes that:

*"Unless the ASPSP has reasonable grounds to suspect fraud, **AISPs shall apply their own strong customer authentication** when the payment services user accesses the payment account information*

retrieved by that AISP, at least 180 days after the last application of strong customer authentication [...].”

Currently, only ASPSPs are able to apply SCA. Changing the requirement would impose a significant burden on AISPs if they are required to issue SCA credentials themselves for reauthentication, as opposed to the simple reconfirmation of consent.

PSR also introduces consent dashboards to give consumers additional control and overview over their AIS and recurring payments consents. This additional visibility and control for the PSU means that the 180 day reauthentication requirement is no longer needed.

We therefore support requiring AISPs to periodically obtain a simple reconfirm from the PSU, without the requirement to perform a Strong Customer Authentication.

OFA recommendation:

Art 86.4 should clarify that AISPs only need to obtain a simple reconfirm from the PSU every 180 days, as opposed to performing their own SCA or being asked to re authenticate every 180 days .

3. SCA exemptions

Under PSD2, PISP-initiated payments are meant to have SCA exemptions available to them where applicable. In practice, however, exemptions are rarely applied and PISPs do not have visibility about where they exist and may be available. Current implementation does not allow for low value or low risk open banking payments to be exempt from SCA.

Examples of exemptions under PSD2 that are not commonly applied for PIS include low value transactions, transactions to trusted beneficiaries, or B2B payments.

If the ASPSP applies SCA exemptions to customers using the customer interface, they should apply the same exemptions when the customer accesses accounts via an AISP or PISP.

Art 36, 2 (c) states that TPPs shall “make use, in a non-discriminatory manner, of any authentication exemptions applied by the account servicing payment service provider”.

Article 85 of PSR also establishes that exemptions from the application of SCA need to be designed by the EBA, also according to Article 89. Under PSD2, there are a number of exemptions that TPPs should benefit from, but they are not applied by the ASPSP more often than not.

OFA recommendation:

All applicable SCA exemptions must be made available consistently to payments initiated by PISPs.

We support Art. 36.2 which states that TPPs shall be allowed “to make use, in a non-discriminatory manner, of any authentication exemptions applied by the account servicing payment service provider.”

To realise this in practice, ASPSP dedicated interfaces for TPPs must support both flows where SCA is applied and where an SCA exemption is applied and SCA is not applied.

PISPs must be able to request information about available SCA exemptions from the ASPSP via the dedicated interface, including reasoning about any refusal to apply.

NCA must actively supervise the implementation of SCA exemptions to ensure alignment with the PSR provisions. Evidence of support could be monitored through augmentation of ASPSP fraud reporting requirements, which currently require ASPSPs to report total SCA exemption usage across credit transfers and cards. Requiring separate reporting of total SCA exemption usage on PISP-initiated payments would show where ASPSPs were supporting exemptions in a non-discriminatory manner.

4. SCA parity

PSR (Article 86, 2) sets the requirement for ASPSPs to allow PISPs and AISPs to rely on the same authentication procedures provided by the ASPSP via the customer interface. This “SCA parity” exists under PSD2, however it is often not applied. There are many examples of banks implementing best practice SCA for the customer interface - for example automatic app to app redirection and frictionless biometrics - but not for AIS or PIS, which need to rely on outdated and less secure methods such as card readers or one time passwords.

OFA recommendation:

We support the PSR obligation for ASPSPs to allow PISPs and AISPs to rely on the same authentication procedures provided by the ASPSP via the customer interface.

ASPSPs offering redirected authentication with biometrics to PSUs accessing accounts or initiating payments directly via the ASPSP must also enable their PSUs to use redirection with biometrics to authenticate with the ASPSP when using the services of an AISP or PISP. This is in line with [EBA Q&A 2023_6767](#).

Security and fraud

OFA supports PSR’s focus on measures to fight financial crime and fraud.

1. IBAN/name matching

IBAN/name matching is useful in combating authorised push payments fraud (APP) or preventing misdirected payments, where the payer can, by mistake or as a result of fraud, send a payment to an unintended payee.

When customers choose to pay a business using open banking, they are not usually required to manually enter any payee details. This removes human error, and the risk of customers being tricked into sending the money to a fraudster. The open banking provider controls where the money goes: to a safe merchant with which they have a contractual relationship and that has passed due diligence checks.

OFA recommendations:

We support the approach taken in the draft PSR on IBAN/name matching, which will strengthen protection for some open banking payments where a payer needs to input the recipient's account details.

In cases where the PISP provides the payee details and has carried out appropriate due diligence on the payee, they are already responsible for correctly providing these details in the payment order. Applying an IBAN/name check in this case would duplicate the checks already performed by the PISP, with no additional benefit. We therefore welcome Art. 50.7 which states that the matching "shall not be required where the payee did not input himself the unique identifier and the name of the payee."

In addition, IBAN/name check provisions in the PSR must be aligned with those in the final Instant Payments Regulation to ensure consistency and harmonisation of rules.

2. CDD obligations & interaction with the AMLR

Merchant-facing PISPs are already required to undertake Customer Due Diligence (CDD) on their merchant customers. ASPSPs are also required to undertake CDD on their account-holding customers. Both the payer and the payee in PIS have been subject to CDD.

As a result, requiring PISPs to apply CDD to both their own customers (merchants) and on the account-holding end-users from whose accounts they initiate payments, is duplicative and unnecessary. In fact, it places merchant-facing PISPs at a considerable competitive disadvantage to other PSPs such as card acquirers, who do not have to apply CDD to people paying their merchant customers by card.

OFA recommendation:

The AML Regulation, being negotiated in parallel to the PSR/PSD3, must only require that PISPs apply CDD to their merchant customers. Recital 34 of the AMLR must remove PISPs from scope or

explicitly state that merchant-facing PISPs should only be required to perform CDD on the payee (their merchant customer) and not the payer (as the ASPSP has already undertaken CDD on them).

Enforcement and supervision

One of the main challenges under PSD2 has been the uneven enforcement of open banking rules. OFA welcomes the extra powers and responsibilities granted to the EBA and to NCAs in this regard.

OFA recommendations:

We welcome the increased focus in PSR compared to PSD2 on enforcement and supervision via empowering NCAs. The effectiveness of the open banking provisions will in part depend on enforcement and supervision.

Closely related to this, cross-border obstacles amounting to IBAN discrimination remain widespread. Their removal depends on NCAs interpreting and enforcing rules consistently and effectively.

In the longer term, we believe that the right solution will be creating an EU Authority tasked with supervising the implementation of open banking and open finance rules.

Definitions

Payment initiation service: PSR rightly addresses a shortcoming of PSD2 and recognises that payment orders can be placed by PISPs on behalf of the payee, not just the payer. Many TPPs have a business relationship with the merchant accepting the payment, not with the end user making it.

Re-authorisation for payment and e-money institutions

A significant change in PSD3 is the merger of the licensing and authorisation regimes of PSD2 and the E-Money Directive (EMD2). In the new framework, former Electronic Money Institutions (EMI) are a subcategory of Payment Institutions (PIs). Both the EU Commission and the European Banking Authority consider that payment services and e-money services are very similar in nature and risks, and therefore should have almost identical legal requirements when it comes to authorisation and requirements for safeguarding and initial capital.

The changes should create a clearer, simpler framework for e-money and payment institutions.

As a result of these and other changes, current PIs and EMIs will also need to apply for re-authorisation from their NCAs.

OFA recommendations

OFA welcomes the creation of a streamlined process for re-authorisation of payment institutions (PIs) in order to not create unnecessary administrative bottlenecks.

We suggest establishing a clear path to simple re-authorisation under PSD3 for existing PIs which are demonstrating compliance with PSR/PSD. PIs should not be obliged to re-submit information already shared with the NCA.

Access to payment systems for non-bank PSPs

OFA supports granting PIs the right, under proportionate, objective, and non-discriminatory criteria, to directly access payment systems, via amending the Settlement Finality Directive (SFD). We also believe that this outcome should be achieved as soon as possible so that non-banks will be able to get the benefits of direct access and foster competition in the payments industry.

Contact

Join us and be the voice of Open Finance in the EU and UK.

info@openfinanceassociation.org | www.openfinanceassociation.org

