# FDATA submission: Implementation of the revised EU PSDII

16th March 2017

# FDATA submission:
# Implementation of the revised EU PSDII

## 1. Introduction

1.1 The Financial Data and Technology Association (FDATA). We currently have 19 members who provide innovative financial applications and services to empower customers to make better decisions and take fuller control of their financial lives across all their accounts, credit cards, loans and investments. The fintech sub-sectors we now cover include:

- ➔ Personal finance management
- ➔ Price comparison
- ➔ Challenger banking
- ➔ Credit reference
- ➔ Lending
- ➔ Technology provision
- ➔ Accountancy
- ➔ Identity verification
- ➔ B-2-B financial advisers
- ➔ Customer-led data marketing

1.2 We seek to work with government, regulatory authorities and financial industry stakeholders in our mission to open up the UK's financial sector to the benefits of financial data and technology.

1.3 Our Membership Charter follows:

*As Members of the Financial Data and Technology Association (FDATA), companies and their representatives agree to endorse and to follow the aims and values of the Association. They agree:*

- *that by empowering consumers to leverage their financial data, through services of their choosing, they can make better financial decisions and achieve better financial outcomes;*
- *that all companies offering these services have obligations with respect to the security and privacy of their customers' data and that these are best serviced by participating in the creation and widespread adoption of rules that promote consumer confidence in our industry;*
- *that from time to time the Association will wish to make representations on behalf of the industry to government, authorities and stakeholders and as a Member we agree to play a full, productive and constructive part in that process;*
- *that when operating on behalf of the Association we will speak for the Association and the industry, being cognisant of all views, and that we will not use any opportunities created through Membership of the Association to attempt to achieve commercial advantage solely for our own company.*

1.4 Our current members, in alphabetical order, are:



















## 2. Our submission

*Question 1: Do you agree with the government's proposed approach to implementation of the PSDII? Bearing in mind the maximum harmonising nature of the PSDII, do you think the structure of the regulatory regime will allow the UK's competent authorities to enforce the regulations in a fair and equal way towards all payment service providers?*

We are broadly aligned with the Government's implementation of PSD2, and fully supportive of the Treasury's enthusiastic support for the expansion of open banking for the benefit of UK consumers.

However we would raise a flag that the Government, in its role at the head of the regulatory regime which includes CMA and FCA, ensures that the outcome of the two current open banking processes - PSD2 and the Implementation Entity - creates the market conditions for innovation and expansion but also ensures that the solid foundation laid by the 'live market' over the last 10 years is not carelessly broken.

This will require careful and complete alignment with the FCA's implementation of PSD2 and the implementation of the CMA-mandated API.

*Question 2: A consultation stage impact assessment of the proposed changes will be published before the end of the consultation. Do you have any comments on the impact of the PSDII set out in the impact assessment?*

The critical issue surrounding the impact of PSD2 is that it helps to create the market conditions for innovation and expansion but also ensures that the solid foundation laid by the 'live market' over the last 10 years is not carelessly broken.

In this respect, the fate of the data aggregation process known as screen-scraping is critical. The majority of the live market uses this process to obtain, with the permission of consumers, financial data. Were this process to be banned, without the simultaneous ability to obtain same data in unredacted format via another technology such as an API, the current live market would face drastic consequences.

Perversely, it would have the opposite effect of that intended by Treasury and the CMA, in that it would dramatically reduce the size of the open banking market rather than helping it expand. This shows the critical importance of ensuring that the data scope of the CMA-mandated process is *at least* as ambitious as that of PSD2.

*Question 3: Do you agree that the government should continue to exempt the institutions listed above from the PSDII?*

As a rule, we are not generally in favour of exemptions, because we believe all consumers are ultimately best served by maximum openness of financial data. That remains our position, although we appreciate that there may be valid reasons for the government to consider these institutions carefully.

*Question 4: If you intend to make use of the electronic communications networks and services exemption, how do you intend to track the €50 and €300 spending limit?*

FDATA is a trade association. This question relates to a business model and would therefore be best answered by individual members.

*Question 5: Is the approach on cascading useful to intermediaries given the limits on the exemption and the potential need for authorisation or registration for other services provided? What types of business models would benefit?*

FDATA is a trade association. This question relates to a business model and would therefore be best answered by individual members.

*Question 6: Do you agree with the government's interpretation of the limited network and commercial agent exemptions? Which business models do you think may now be brought into scope that were previously exempt?*

As a rule, we are not generally in favour of exemptions, because we believe all consumers are ultimately best served by maximum openness of financial data. That remains our position, although we appreciate that the particular exemption has already been narrowed and there may be valid reasons for the government to consider these transactions carefully.

*Question 7: Do you agree with the proposed change to safeguarding to ensure funds can be deposited with the Bank of England?*

FDATA is a trade association, the majority of whose current members are third party providers rather than payment institutions. We have therefore not yet formed a view on this, but we expect our membership to expand and we will form a view on such matters in due course.

*Question 8: Do you agree with the government's proposed approach to access to payment systems and payment account services?*

FDATA is broadly in support of the government's approach. Insofar as there are concerns about safety and security, we think it is important that the government restricts access only in those cases where the agreed requirements for regulation or whitelisting are not met. In the instance of a provider which passes all the required legal and regulatory tests, we do not believe that data holders should be able to restrict access (or the quality of that access) on the basis of security or safety concerns. That is the job of regulation.

*Question 9: Do you agree with the approach to continue to exercise the SPI exemption, with the same conditions as under the PSD?*

FDATA is a trade association, the majority of whose current members are third party providers, so this question is not currently within our locus.

*Question 10: Do you agree that the government should extend the right of termination to overdrawn current accounts?*

FDATA is a trade association, the majority of whose current members are third party providers rather than banks. We have therefore not yet formed a view on this, but we expect our membership to expand and we will form a view on such matters in due course.

*Question 11: Do you agree that the Title III provisions should continue to apply to transactions involving micro-enterprises in the same way as those involving consumers?*

FDATA is a trade association, the majority of whose current members are third party providers rather than payment institutions. We have therefore not yet formed a view on this, but we expect our membership to expand and we will form a view on such matters in due course.

*Question 12: Do you agree with the government's proposal to maintain the thresholds set for low-value payment instruments in the PSRs?*

FDATA is a trade association, the majority of whose current members are third party providers rather than payment institutions. We have therefore not yet formed a view on this, but we expect our membership to expand and we will form a view on such matters in due course.

*Question 13: Do you think PSPs should be required to provide monthly statements to payers and payees?*

FDATA is a trade association, the majority of whose current members are third party providers rather than payment institutions. We have therefore not yet formed a view on this, but we expect our membership to expand and we will form a view on such matters in due course.

*Question 14: Do you agree with the government's proposal to provide access to out-of-court procedures (in the form of the FOS) only where the complainant would usually be eligible to refer a complaint to the FOS?*

This question is not within FDATA's remit.

*Question 15: Do you agree that the prohibition on surcharging should be limited to payment instruments regulated under Chapter II of the IFRs?*

This question is not within FDATA's remit.

*Question 16: Do you agree with the proposal to maintain the thresholds set for low-value payment instruments under the PSRs?*

This question is not within FDATA's remit.

*Question 17: Do you agree with the proposed approach to consent, authentication and communication?*

The overall picture remains confusing, in part because of the lack of clarity within PSD2 itself and in part because of the additional layer of complexity created by the Implementation Entity.

There are several important facts which must be established before the combination of the FCA and the Implementation Entity, with input from CMA and Treasury. Primarily, if screen-scraping is to be banned for payment accounts within the scope of PSD2 (we presume for these purposes that PSD2 has no locus to ban screen-scraping for financial accounts outwith PSD2's scope), we must understand whether the ban applies only to those financial data sets which are available through a dedicated interface (API), and/or to those providers which have chosen to switch to an API.

Should the answer to that question be that the ban is in place for all data-sets within PSD2 scope (irrespective of whether those data sets are available via the Implementation Entity process through a dedicated interface, unredacted and matching precisely data available online) the government must seek a solution which mitigates the risk to the live market. It is likely that this will require maximum alignment between the data scope of the Implementation Entity and that of PSD2, so that all data to which the screen-scraping ban is applied is available through an open API offering 100% unredacted data.

Furthermore, it will be the shared responsibility of governmental and regulatory actors to create some form of transitional arrangements to allow live market participants to onboard customers to a new platform in an orderly fashion which does not result in market-threatening disruption.

*Question 18: Do you agree with the information and payment functionality that will be available to AISPs and PISPs?*

We are accepting of the scope of financial data within PSD2 and, furthermore pleased that the Implementation Entity has been persuaded to expands its own data scope to provide alignment with PSD2.

However the key issue for government is to plan strategically for the further expansion of open banking into areas currently not in scope for either PSD2 or the CMA remedy, such as mortgages, investments and pensions, for instance.

This is at the heart of the screen-scraping debate. Whilst FDATA does not necessarily share the general view of screen-scraping held by many large banks, we do believe that the third party community would be likely to switch from screen-scraping to API where that API is able to provide the same richness of unredacted data, simply because it would allow for a smoother user experience.

However, it is also our view that, for those data sets outwith PSD2, screen scraping can and will continue. Providers will have no wish to reduce their services offering to consumers by voluntarily ceasing to screen-scrape.

For that reason, any desire to see screen-scraping end can only be met if the government takes the strategic decision that *all* financial data should be available via an API, and provides a roadmap for how and when that will be achieved.

*Question 19: Do you agree with the government's interpretation of the definition of AIS and PIS?*

We note that there is no interpretation of the definition of PIS in the consultation.

As defined in Article 4(15) a 'payment initiation service' means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;"

FDATA is broadly in agreement with the definition of a PIS.

The definition of an AIS in PSD2 is: *"an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider"*

The clarification in the consultation states that: *"The government interprets the definition of AIS as meaning that an AISP uses some or all of the information from one or more payment accounts held by the PSU with one or more ASPSPs, to provide an information service."*

FDATA believes that further clarification is needed around the definition of Account Information Services, especially in relation to the point made in 6.30. We suggest that the scope of an AIS under PSD2 is restricted to generalised services that are available online - this could prevent accountants, financial advisors and legal firms from being in scope.

We feel that the current definition of an AISP is unclear and requires clarification, especially with regard to multi-level business models, as illustrated below.

As defined in Article 4(17) an *'account information service provider' means a payment service provider pursuing business activities as referred to in point (8) of Annex I [i.e. Account information services];*

With this definition an AISP could be any of the following:

1. A service that has access to a PSU's account information
2. A service that retrieves account information **directly** from ASPSPs
3. The branded entity that the end user most closely associates with the service. This entity may not be the same person as 1 or 2.
4. Any combination of the above, and if so, in what combination.

To further illustrate the point we have provided an example scenario that includes a number of participants who each provide different aspects of an account information service and who could all be considered as AISPs depending on how an AISP is defined.

> Company A is a furniture retailer who wants to provide its potential customers (who are PSUs) a budgeting dashboard so that the customer can assess whether they can afford some new furniture.
>
> Company A contracts with Company B to provide a white-labelled financial dashboard. The dashboard is branded with Company A's name and logo, but is hosted and provided by Company B as "software as a service".
>
> Company B builds and hosts the dashboard but contracts with Company C to connect to the APIs of the ASPSPs. Company C connects to the ASPSPs via RTS compliant dedicated interfaces. Company C stores account information of PSU's and provides it to Company B via an API.
>
> A user registers with the website of Company A, as part of this process they agree to terms and conditions that refer to Company A, Company B and Company C. They then click on a link to the financial dashboard hosted by Company B, but in Company A's colours. The user then clicks "Connect my bank accounts" and after giving consent are redirected by Company C to their bank's' website where they authorize the bank to share their data with Company C. Company C shares this data with Company B. Company B then provides the dashboard to the user in Company A's branding.
>
> If an AISP is defined as a service that has access to a PSU's account information, then both Company B and C would be required to register as AISPs. Company A would be required to register as an AISP only if they also had access to the account information (either via an interface provided by Company B, or if the software was hosted in Company A's data-centre rather than being provided as software as a service). This interpretation would offer a good level of protection to consumers, as all participants who are holding the PSU's account information (which will include sensitive data) are regulated, and raises the barrier to entry only very slightly for smaller entitles who may wish to provide services of this nature.
>
> If an AISP is defined as only the service that retrieves the account information directly from the ASPSP, then only Company C would be classed as an AISP. There could be a concern with this approach as Company B would be unregulated even though it is providing the bulk of the account information service. It would also reduce visibility for the ASPSPs as they would only be aware of Company C. In turn this could make it harder for PSUs have visibility of which companies have access to their data from the ASPSP interface. On the plus side, it would support existing business models and not raise barriers to entry. It is also an established model in other areas - Company C would be absorbing Company B's liability and taking it within its compliance perimeter.
>
> If an AISP is defined as the entity that is most visible to the end user, then Company A would be classed as an AISP. While this may seem to make sense, the reality is that Company A may simply be putting its brand on a white-labelled

system. It may have no access to the PSU's account information and therefore many of the security policies required to register as an AISP would be irrelevant.

The above scenario is further complicated by the requirement that AISPs securely identify themselves to ASPSP(s). How does this work when there are multiple AISPs in a chain? Or alternatively if only Company A is an AISP, how can they securely identify themselves to the ASPSP when Companies B & C sit between the ASPSP(s) and Company A.

FDATA would request that HMT provides further clarification on this in a manner that balances the need to see an orderly transition for the live market and the protection of end-user's data.

*Question 20: What services are currently provided that you think may be brought into scope of the PSDII by the broad reading of the definition of AIS and PIS?*

There are likely to be a number of services currently provided by the live market which the definitions of AIS and PIS may require be brought into the scope of PSD2.

This cannot be an exhaustive list but we would suggest that some obvious examples might be accountants, mortgage brokers, consumer-facing personal finance dashboards and account aggregation API providers.

*Question 21: Do you agree with this description of the rights and obligations for ASPSPs, AISPs and PISPs?*

FDATA is broadly in agreement with the description of the rights and obligations for ASPSPs, AISPs and PISPs. We are concerned, however that ASPSPs may meet with the technical requirements of the EBA RTS but implement a materially worse user experience than is available via the ASPSPs own interface. We suggest that HMT clarify that such an approach would risk the ASPSP being in breach of PSD2 by not providing the same level of access.

We are aware that some parties are promoting the concept of a voluntary layer on top of PSD2. This concerns us, because we envisage a situation where the largest actors (i.e. the banks) are effectively in control of the rules. We worry that there will be confusion for consumers if there are two levels of accreditation - a basic PSD2 layer and an additional voluntary layer.

As well as their obligations under PSD2, AISPs will also be subject to GDPR and other data protection legislation to ensure they safeguard end-users personal data. While ASPSPs can't impose contracts on TPPs, they can define the dedicated interface through which the TPPs connect. The design of the standards for these dedicated interfaces can ensure that there are strong cryptographically assured non-repudiable audit trails for every interaction between ASPSPs, TPPs and PSUs. We therefore believe the line of thought promoted by some in the industry that PSD2 will usher in a "wild-west" of ill-intentioned participants is baseless. Assertions that without a voluntary scheme there will be huge regulatory costs are also founded on weak assumptions.

We believe that PSD2 with the EBA RTS will actually improve the security and audibility of online account access and payment initiation.

*Question 22: Do you have any comments on the initial period of implementation, before the EBA RTSs are fully in force?*

FDATA is fully supportive of the intentions of HMT on the initial implementation. However, we would suggest that this will require further complex discussion to ensure that it can work in practice, particularly to establish where the so-called 'CMA9' banks would fit into such a process. Furthermore, we have uncertainties over some of the stated PSD2 provisions; without the RTS, they can be vague and it is therefore difficult to establish recourse in the event of non-compliance.

Although the EBA RTS is not finalised, the fundamental principles have been known from the time of the first consultation and are highly unlikely to change. We therefore support HMT's view that *"During this period both ASPSPs and AISPs/PISPs will be undergoing a learning process and will be expected to work closely across industry, and where appropriate with the FCA, to overcome challenges that emerge and ensure that users have the ability to use AIS or PIS."*

We reject the idea of a delayed roll out and believe the industry can meet the challenge of a January 2018 initial implementation.