UK Finance Response to PSR Discussion Paper: Data in the Payments Industry

Introduction

UK Finance is the trade association which was formed on 1 July 2017 to represent the finance and banking industry operating in the UK. It represents around 250 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our objective is to work with our members to build a more customer-focused and innovative finance and banking sector, cementing the UK's role as a global leader in financial services for the benefit of the wider economy. The interests of our members' customers are at the heart of this work.

General Comments

The Discussion Paper is broad and contains a wide-ranging analysis of data use in the payments industry, and consideration of these issues is both timely and appropriate given the fast-changing nature of the market, and the resulting implications for all stakeholders (including consumers, government, and market participants). We welcome that the PSR has opened this dialogue with industry and indicated that it is keen to gather the views of market players on the issues raised within the paper.

The consistently greater use and sharing of data, both in the present and near future, has wide-reaching ramifications for society and, as part of this, the payments industry. New technologies, regulatory changes and business models mean that the industry and its customers are experiencing change at an unprecedented rate, and in many cases data use is at the core of these changes. UK Finance therefore welcome this opportunity to provide feedback on the PSR's Discussion Paper and to engage further with the PSR as it considers the findings and determines its future policy. But additionally, we would encourage the PSR to be aware of the extensive market changes that are currently underway within the payments landscape (including the design of the New Payments Architecture). Within this implementation period, the PSR should operate by monitoring the market changes and working with the industry to help tackle any emerging challenges, allowing time for the market to develop and respond to consumer-led demands.

The paper references a broad range of issues, from the potential impacts of the PSR's objectives, spanning potential definitions of what may constitute payments data now and, in the future, for example where data in a payment message field may be attached for a completely different purpose than processing the payment message, and moving to consider whether ancillary services such as transaction data analysis could safely be opened up on a competitive basis. We have sought to address these issues in our response, but they constitute complex topics, and set against the changing data regulatory environment, we have focussed on best practice legal ways to permit data sharing, which we believe should form the basis of PSR's approach to these issues

In addition, we feel that developing specific and concrete use cases for the issues discussed in the Paper would be a positive next step.

The Discussion Paper refers to data protection law but as this work and thinking progresses, we believe it would be beneficial for further analysis of the relevant data protection requirements to be undertaken (possibly led by the PSR), and for this to be applied to assess different use cases. We suggest that key data protection requirements and issues that should be factored in are:

- The need for a consistent and nuanced definition of 'personal data'
- Further consideration of which actors are 'data controllers' and which are 'data processors' – for the current payment systems this tends to be understood but will become potentially more complex with the introduction of the NPA and the adoption of the new message standard
- The need for a 'basis for processing' as distinct from 'consent'
- The difference between 'consent' under GDPR and 'consent' in a more conventional contractual sense (like under PSD2)
- The requirement for a specific purpose and the minimisation of data to match this
- The overarching need for 'fairness' in data processing
- Accommodating and facilitating the exercise of GDPR rights by individuals over their personal data

(More detailed commentary about these requirements are annexed to our response.)

In line with our earlier comments, we note that determining what is possible and to ensure compliance with data protection requirements would be aided by the establishment of clear uses cases. The use case will impact the basis for processing, the applicable data subject rights and how to facilitate the exercise of these, how to ensure fairness, how to ensure that data is minimised, and the approach to any 'further processing' beyond the purposes originally explained to data subjects.

One particular area where we would seek additional clarity within the Paper is the extent to which the PSR has made any assumptions of the new services which it envisages will be 'opt in' for data subjects, and to what extent firms might be expected to share the data without consulting data subjects (though at a minimum the new processing would need to be explained).

At the July PSR workshop, we understood that both options were being considered, with the possibility discussed of having PSPs simply update their T&Cs to enable wide data sharing. Although this kind of broad approach might be possible for initiatives intended to achieve public policy goals like fraud prevention, broad sharing to enable private firms to develop as-yet unknown commercial products would require careful consideration, for example to ensure transparency and fairness. We suggest the PSR continues to broaden its consideration of data protection requirements and is mindful of the nuances involved in 'consented' data sharing as it develops its work in this area.

Similarly, we would request further clarity from the Paper as regarding what kinds of institution the PSR would like to see gain access to the data, though we understand that the PSR is interested in seeing access be as wide as possible. The more widely shared the data is, the greater the data protection compliance challenges will be.

As the PSR progresses its thinking, we recommend that a Data Protection Impact Assessment (DPIA) is completed, working closely with the ICO. Although the PSR would not likely be the data controller, the DPIA process would help identify and manage the privacy risks and ensure compliance with GDPR of the overall proposals. In addition to (or as an alternative to) an overarching DPIA, a DPIA will likely be

needed for each potential use case or overlay service, in co-ordination with the ICO. The actors, data flows and necessary controls will no doubt be very different for each.

Our members are very conscious of their own roles as data controllers under both data protection laws and other privacy / confidentiality obligations and would in all cases require to undertake their own Data Protection Impact Assessments (DPIA). These might be supported by, as in the development of the Confirmation of Payee service, at NPSO, a legal taskforce to consider the Legitimate Interest Assessment for this proposed data exchange. In the context of Confirmation of Payee, data minimisation has been favoured, both from a data protection perspective and to maximise the customer experience.

Finally, we note that cybercrime, cyber resilience and fraud risks will need to be carefully considered in the preparation of use cases. This will need to include consideration of new data breach reporting requirements under GDPR. Given the constant and evolving threats from cybercrime, and the continued risks of IT failures, it is likely that data breaches will continue to occur in future.

In the following section we will provide responses to the questions set within the Discussion Paper.

Collection and Classification

Do you agree with PSR's assessment of:

a) types of data in the payments industry that are relevant for this Paper?

- The PSR's examples by payment system appear to accurately reflect the difference in system data messages, and what is provided by the end user and between system participants. As such, the definition used in the document of "the totality of information collected by PSPs and other third party-providers in the process of providing core payment services to end users" is appropriate, but by including the caveat that the relevant data is "not limited to" this definition, the meaning becomes less clear and the in-scope data set substantially broadened.
- Characterisation of 'personal data'
    - In paragraph 2.4 the Paper observes that data protection law does not apply to data relating to corporate entities, only natural persons. This is correct, but it should be kept in mind that corporate data can sometimes be personal data pertaining to individual staff, directors and shareholders.
    - As outlined in the annex, 'personal data' is data that *relates to* an identifiable individual. However, throughout part 4 of the Paper, the assumption seems to be that only the data points that directly *identify* the individual are captured. For example, in 4.25 the Paper states that the date and amount of a Bacs transaction are not personal data, but in fact they would be if that information is associated with an identifiable individual.
    - The Paper might be intending to refer to these specific transaction data points in isolation from any other data (i.e.: irrevocably separated from the payer/payee data), but this is not clear.
- 'Special category data'
    - It is arguable that payment records could contain 'special category personal data' (SCPD), for example: does a payment to a health services provider imply information about the payer's health, and does a payment to a trade union or political party indicate information about political opinions? There is not necessarily a clear answer to this and the PSR should discuss it with the ICO. If SCPD are present, the data protection challenges to data sharing will be considerably greater.

- Processing SCPD can only be processed under strict conditions, primarily where there is a specific legal permission to do so in the Data Protection Act 2018, or where the individual has given 'explicit consent'. 'Explicit consent' has a particular meaning under the GDPR and is a very high standard, requiring granular explanation of the data and how it will be used. (See also annexed comments on 'consent' under GDPR.)

b) types of data collected by different entities in the industry?

UK Finance broadly agree with this assessment but notes that it does not cover Direct Debits and the position of indirect PSPs. Additionally, some of the data listed in Section 4 is not strictly payments transaction routing data and may not appear in the NPA global data sets.

c) different ways that payment data can be classified?

See comments above and in the annex on 'personal data'.

Use of Data

Do you agree with our assessment of the different points in the value chain where data could be used to generate benefits for payment system participants? Are there any other points where data could generate value?

No comment.

Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

The current uses of payments data identified are broadly correct. However, there are some complexities that will need to be worked through in due course as the PSR develops its thinking:

- The fact that a firm 'has' a dataset does not mean that it can use the data freely.
  - 'Data processors' are not able to determine the purposes of processing (see annex).
  - Any personal data processing requires a 'basis for processing', as detailed in the annex, and the processing must be fair, with data collection minimised. 'Legitimate interests' is the most flexible basis for processing but requires a balancing of the controller's interests against those of the data subject. Furthermore, when legitimate interests are relied on, the data subject has a right to object to the data processing and force the controller to reassess the balance of interests. Where the processing is for marketing purposes, the data subject has an absolute right to block the processing.

PSR Policy Issues

End-User Willingness to share data

The Discussion Paper asks whether there is a mismatch between consumer trust in established brands and new third-party providers, and whether this could lead to reduced competition. In part, UK Finance believes that this mismatch should be viewed alongside the issue of consumer trust as a whole. Data breaches (particularly where these are very public), cyber incidents and IT failures will impact consumers' trust and their willingness to share their personal data. All stakeholders have a role in reducing data breaches, and clear guidelines and assistance from regulators should be provided to assist firms put in place procedures to resolve any breaches in a timely, more uniform and efficient manner. This would assist in increasing consumer trust across the market.

In general, consumers should be equipped with relevant information to help them to make safe decisions. Both incumbent and challenger firms have the ability to clearly, openly and accurately state how they will use consumers' data; a PSP that does so may reap the benefits of consumer trust and

engagement. Ensuring that consumers understand how their data is being used and who has access to it will be key to consumer confidence, along with secure and safe management of that data. These issues will require careful consideration as the PSR develops more specific use cases.

Regarding the 'incumbent firm v new firm' trust concerns, we would encourage the PSR to undertake further research on this topic to understand how customers feel about allowing new firms access to their data, and how this varies as compared to their attitudes towards firms with more established brands. This could help newer firms understand what they can do to help consumers trust them and engage with their services.

Customers are more likely to engage with new services when they can see clear benefits in using these services. This can take time, with new products generally being taken up quickly by early adopters and allowing other customers to move at a more considered pace. As Open Banking and PSD2 mature and come into full operation, it is likely that innovative new players, offering useful and relatable products to the open market will receive more attention. The PSR should take stock of how the market develops and monitor uptake of 'new v old' services, in order to determine if and where a trust mismatch occurs.

Access to global datasets

The Discussion Paper is not clear on the exact definition of a 'global data set'. In the July workshop, hosted by the FCA, the PSR stated that this referred to 'global transaction data', for example all FPS transaction data, including sort codes, account dates and associated information; the data in question does not include 'ancillary data', which was understood to refer to location, but it was acknowledged that richer data could be included in the future. If this definition is correct, then it would be beneficial for the PSR to consider this further in its follow up activity and clarify the status of the various data types.

Within the Paper, and in the workshop, the PSR stated that they wished to broaden access to global datasets to prevent firms with existing access to such data having a monopoly over any associated services. The Paper asks if the NPSO could be mandated to consider how to open access to these data sets to other firms. However, it should be noted that the controllers of such global datasets do not always have open access to the data for other purposes. They do not have permission to utilise the data in ways outside as was permitted by the user and other members of the payment chain (within PSD2 and Open Banking customers must explicitly agree to the data being shared)

Even if such expanded processing is permitted, for example to support deeper fraud analytics on transactions and potentially other data, this would require careful risk assessment. A Legitimate Interests Assessment would also be needed to ensure that there is an appropriate basis for processing under GDPR.

It is also difficult to estimate the types of data overlay services that may emerge without a concrete definition of what the 'global transaction data' includes, and some example end-use cases to ascertain what is intended. However, we recognise that it is possible that anonymised global data could assist anti-money laundering efforts and could be an early detector of other forms of financial crime. Opening up the datasets, using an API system as is suggested, could be beneficial by reducing the "single point of contact" risk. However, opening any data set comes with accordant risks of having more players who need to be vetted and monitored. If this approach is progressed, the PSR will need to effectively and closely monitor and regulate all activity in this arena.

It is difficult to fully assess the regulatory hurdles to widening the sharing of 'global transaction data' without greater clarity as to the data to be shared, the level of individual consumer control and the recipients of the data. As use cases are developed, in respect of *personal data* we think it would be productive for the PSR to consider how these map onto GDPR requirements, especially those set out at the beginning of this response. In particular, the following will need consideration:

- The basis for processing

- How to ensure fairness for customers
- The precise purpose, and whether / how any 'further processing' can be justified
- Given the purposes, how will the requirement for data minimisation be met?
- How data subject rights will be facilitated.

Broadly speaking, data protection risks will be higher (and GDPR compliance more difficult) if data sharing:

- is not part of the provision of the core service requested by the customer,
- is not an optional addition that customers can opt into, or
- is not for the purposes of regulatory compliance (such as fraud prevention).

Widened access to data will therefore have to be considered for each overlay service, rather than as a generic requirement on firms to make data available for unspecified purposes.

As noted above, at the July workshop we understood the PSR to be considering an approach by which account providers would update their terms and conditions to enable sharing of personal data with a wide range of recipients for the purposes of developing innovative products. Such a 'consent process' would be unlikely to meet GDPR requirements; the consent would not likely be valid, and 'fair processing information' needs to explain (among other matters) the purposes of the processing and specify who the data controllers are.

Developing new industry-wide fraud and anti-money laundering (AML) prevention measures

Is there tension between the development of industry-wide transaction data analysis tools and data protection requirements? If so, what technical requirements and consent processes would be needed to address this issue?

A shared analytics tool to help firms detect and prevent fraud, money laundering and other crime would be a useful innovation. In some cases, such as the Transaction Data Analytics, a fair funding model would also be necessary to recognise the costs of capturing, storing and processing the data. There would also need to be central assurances (including regulation) of providers who have access to the global data sets, and a clear governance model to process any disputes.

This proposal will require further development and, as highlighted above, the impact of data protection requirements will depend on the exact nature of the use case. Again, insofar as personal data is in scope, we think it would be helpful for the PSR to consider in particular:

- The GDPR basis for processing
- How to ensure fairness for customers
- The precise purpose, and whether / how any 'further processing' can be justified
- How data subject rights will be facilitated
- The level of individual consumer control over access to their personal data

In terms of 'consent processes' – 'fair processing information', explaining how customer data is used and who the data controllers are, would need to be provided to all data subjects. If the tool would share personal data with a wide or open-ended group of data controllers, this would need careful consideration in order to achieve transparency and fairness. Those controllers without direct contact with the data subject would not readily be able to provide a privacy notice. Some kind of central privacy notice might be possible but would need to be able to accommodate frequent changes to the relevant controllers.

Similarly, if personal data is shared with a wide group of firms, it will be difficult for data subjects to exercise their GDPR rights. Individuals need to be able to identify who the data controllers are and be able to contact them, so they can request information about the personal data held, correct errors, object to processing, etc.

In any event, it is unlikely that 'consent' would be the basis for processing for fraud or money laundering prevention processing, unless this were intended to be an optional service of some kind that individual customers could choose not to participate in. 'Legitimate interests' or conceivably 'legal obligation' would be a more likely basis.

Realising the benefits of enhanced data

During the Workshop, the PSR specified that the enhanced data in question would follow the Bank of England's work on ISO20022 message, and would contain more remittance information, more identity on receipts, information on all the PSPs in a chain, purpose codes within CHAPS, and space for LEIs (with the possible mandation of inclusion for this within CHAPS). The enhanced data will also be able to contain links to other data. As we have stated in our interactions with the Bank, UK Finance is supportive of the use of enhanced data where possible.

However, inclusion of enhanced data must be done in such a way that ensures it is still of a high quality. For example, consumers who do not understand the benefits of adding such data may do so without due care and attention, possibly making mistakes or omitting data points. Enhanced data must be of a high quality to ensure any benefits are realised. As the PSR continues in their discussion on data, it would be beneficial for a wider consideration of the data issues surrounding enhanced data to be considered (including the implications of enhanced data being held remotely from the transaction e.g. by data warehouse providers)

As the Paper states, the adoption of enhanced data may be slowed in some points by operational issue e.g. the need to update technology. However, whilst the PSR may wish to encourage adoption, we would advise caution before mandating any action in this area. The payments market is currently in a period of unprecedent change, and these changes should be allowed to play out fully before any more modifications are mandated. The new ISO messaging standard, alongside the changes of the New Payments Architecture, mean that there will be large increases in the amount of additional data made available (Additionally, it could be beneficial to explore if the NPA can be designed to accommodate data sharing capabilities, rather than the possible need to retrofit in future.) The outcomes of these developments should be seen before introducing more change.

Other payments data-related issues

The Discussion Paper refers to issues such as smaller PSPs having higher fixed costs of data management than smaller firms, and that larger PSPs have a wider ability to offer cross-selling due to their wider consumer base. These are concerns that may well be valid, but it is unclear what role the PSR may seek to have, or should have, in business realities that are distinct from payments systems themselves.

In addition to understanding the access regulatory position, there is a need for greater understanding of the operational and information security implications of having more parties with access to the global data sets in the central infrastructures. It would be of benefit if the PSR undertook further analysis to map the business case, cost, operational and resilience implications of this access and processing significantly large data messages, in addition to the capture, storing, retrieving and presentation of enhanced data.

The complications of enhanced data should also be considered by the PSR. For example, optimal interoperability and ubiquity of Confirmation of Payee requires consistency of naming convention, or the ability to link related data that may have considerable differences in presentation. Many data led initiatives can have their design, build and implementation complicated by inconsistent data management.

Privacy and trust concerns of consumers are likely to be key to ensuring they can benefit from new services. The PSR should focus on assisting firms to maintain high standards of data protection, and

providing effective regulation, ensuring that any and all breaches are dealt with efficiently and safely. In addition, the PSR should be mindful of the high amount of activity and change currently underway in the payments industry and allow current changes to “bed in” before suggesting more. The NPA, for example, should be introduced and allowed to mature before any reassessment of requirements in terms of data are undertaken, and the PSR should work in conjunction with the NPSO to ascertain the NPA’s functionality in regard to any future Enhance Data and TDA (Transaction Data Analytics) requirements

Annex – key GDPR requirements

- Definition of 'personal data'
    - The Paper contains varied definitions of 'personal data'. E.g. in 2.4, the Paper refers to personal data as information that "could be used… to identify a living person". This definition is much narrower than the GDPR definition. The definition in 4.15 of the Paper more correctly characterises personal data as data that *relates to* an identified or identifiable living individual. It is not clear which definition the PSR is applying throughout the Paper. See also comments under Question 1.
    - If a data set does not directly identify an individual, it will still be personal data if the firm holding the data has access to other data which, in combination, will identify an individual. As such, certain data might not be personal data when held by one firm but *could be* personal data when held by another firm with access to additional relevant data.
    - Pseudonymising data is a protective measure that firms can implement to reduce data protection risks. However, contrary to page 63 of the Paper, pseudonymised data is still typically personal data and therefore subject to GDPR. See ICO guidance here.
- Controllers vs processors
    - GDPR distinguishes between two types of firm:
        - A 'data controller' is a firm that determines the purposes and means of personal data processing. Controllers have most of the responsibilities under the GDPR.
        - A 'data processor' is a firm that is engaged by a controller to process personal data on its behalf. A processor must only process personal data in the manner requested by the controller, except in the case of additional processing required by law (e.g.: to comply with a warrant or data request from law enforcement, or to comply with legal obligations under payments law).
    - The Paper does not make this distinction, but many firms involved in processing payments act as processors. Although a processor might 'have' a dataset, it is not able to determine the purposes of data processing. Further analysis of increasing the availability of payments data will need to consider which parties are controllers in each circumstance, and which are processors.
- 'Consent' vs 'basis for processing'
    - GDPR states in Article 6 that personal data can only be processed if one or more of six 'bases for processing' apply. These are (broadly):
        - Where the data subject has given consent
        - Where the processing is necessary to perform or enter into a contract
        - To comply with a legal obligation
        - To protect the vital interests (life) of the data subject
        - When in the public interest
        - Where the controller has a 'legitimate interest' in processing the data, provided this interest is not outweighed by the rights of the data subject.

- Under GDPR, 'consent' has a specific meaning and is only valid in very particular circumstances. Generally, in the area of payments, 'contract', 'legal obligation' and 'legitimate interests' will be much more likely than 'consent'.
- Very broadly, consent is only appropriate where the data subject has a genuinely free choice as to whether the data will be processed and will not be denied access to a service if they refuse. More detail is available from the ICO here, and from EU regulatory authorities here.
- PSD2 requires 'consent' from the account holder before an ASPSP can share data with a third party. However, this is not the same as the basis for processing and is more a kind of 'contractual consent'.[1]
- Though firms would seldom ask for consent (in the GDPR sense) when providing payment services, firms must explain to data subjects how their personal data will be used at the time they gather the data and will often need a contractual form of consent in order to comply with PSD2 and contract law requirements.
- The Paper mentions the need for a legal basis in 4.19, but in other places seems to assume that personal data processing in the context of payments (currently, and under potential future arrangements designed to facilitate data sharing) will be based on the consent of the data subject. See for example 4.12. It is unclear in the Paper when 'consent' is being used in the GDPR sense, and when it is being used in a more general, contractual sense as per PSD2.

- The need for a clear purpose and data minimisation:
  - Under GDPR, personal data must only be collected for clear purposes. Personal data collected must be limited to what is necessary for those purposes.
  - Further processing for new purposes is only possible if:
    - The new processing is compatible with the original purposes, requiring an assessment of numerous factors set out in GDPR Article 6,
    - The data subject has consented to the processing (as noted above, consent is only valid in specific circumstances), or
    - The processing is necessary for the controller to comply with a legal obligation.
  - Efforts to 'repurpose' personal data will need to meet one of these three tests.
- Fairness:
  - Article 5 requires personal data processing to be fair. The ICO explains: "In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them."[2]
- Data subject rights:
  - Under GDPR, data subjects have rights over their personal data. Specifically, they have rights to:

[1] See for example the view of EU data protection authorities here: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

        - be informed about how their data will be processed and who the data controllers are (see definition above)
        - access their personal data
        - correct any errors
        - restrict the processing of their personal data, in some circumstances
        - have their data erased, in some circumstances
        - a right to receive their data in electronic form (portability) in some circumstances
        - be informed as to how their data has been shared
        - object to data processing (when the basis for processing is 'legitimate interests' or 'public interest')
    - An initiative to share individuals' personal data with more firms will need to be designed such that data subjects are able to exercise these rights effectively.
- 6.63 states that GDPR prohibits automated decision-making with legal / significant effects unless the data subject has given explicit consent. In fact, GDPR also permits such automation where the processing is necessary for entering into or performing a contract, or where there is an authorisation in law.