Payment Systems Regulator

Data in the payments industry

Responses to our discussion paper DP18/1

September 2019

Contents

Names of individuals and information that may indirectly identify individuals have been redacted.

Association of Independent Risk and Fraud Advisors (AIRFA)

Dear Sirs

BACKGROUND
This email is a response to the request for views from the PSR discussion paper issues in June 2018. It is provided from the Association of Independent Risk and Fraud Advisors (AIRFA). The members of AIRFA are independent advisors to many parties on risk, data, data protection, and other matters relating to payments and the payments industry. AIRFA has commented on papers ahead of the set-up of the PSR, and been party to working groups at the PSR since its inception including those for "Financial Crime" and "Horizon Scanning".

COMMENTS / VIEWS

1. DATA PROTECTION
The views of the Information Commissioners Office (ICO) should be urgently sought, as it is perceived that there are a significant number of statements in this document that are counter to the views and opinions and interpretations of the ICO in respect of the Data Protection laws in place in the past and today. In particular:

a) **Personal Data** can be identified and/or inferred from a wide range of sources and/or brought together from multiple data souces / elements. In this case, there will be data across multiple payments advises, that alone may not be able to identify individuals, but combines / taken-together would breach Data Protection, but moreover fly-in-the-face of the intentions of the Data Protection laws.

b) **Corporate payments data** : cannot be considered to be excluded from data protection legislation. Corporate payments will and do generally involve payments to and/from individuals. Payments made by corporates (e.g. including and especially tax offices and say, utility companies) will contain personal data elements that can and do identify individuals.

c) **Definitions** : The paper uses headline definitions from the Data Protection legislation without assessing the subsequent detail. For example: by defining how the DAP applies "Personal data" - in the discussion paper - in s 2.4(a) of the paper - it automatically ignores the more important elements and the DPA definitions laid down in PART 1 - Section 3, paragraphs 3(a) and 3(b) which then oppose the considerations/conclusions of the discussion paper on how this should apply. i.e. the paper has ignored these sections of the DPA core legislation.

The DPA legislation in one sense is simple, and tries to enshrine some basic principles:
- Our data as individuals should be kept private, we should be able to trust that our data will not be used for other purposes, and we should be able to control what we allow it to be used for, to be able to opt out, and to be ‘forgotten’.
- The personal data can (MUST? - if considered in conjunction with AML legislation), be used to identify financial/other crimes; but when used for this can ONLY be used in relation to identifying the crime, and ONLY by people within organisations whose primary / only role is to prosecute (not in a legal sense) that crime.
- That personal data can be anonymised / conjoined to create statistical ‘high level’ data to show trends in the data (but NOT individual transactions or identifiable data) - e.g, 32% increase in NFC transactions year on year NOT 47 transactions to buy child pornography by people who live in Basildon.

Accordingly, the concept and suggestion of the possibility of "selling the raw data itself" - [see discussion paper: OUR FINDINGS 1.10] - will be unlawful as well as against the principles of the (EU and UK) legislation.

2. INNOVATION & COMPETITION

Using personal data in some of the ways that are proposed / suggested in this paper are likely to breach the underlying core objectives of the PSR of enhancing competition and encouraging innovation.

The Data Protection legislation requires that consumers MUST be able to 'opt out', must be given the opportunity to 'opt out' and that explicit consent always be obtained to use their data, for purposes that are made specific, and provided to them. i.e. "Please provide your consent by opting-IN to the 'data controller' SELLING your data to 'specific company' for the purposes of 'specific reason'. ". Putting aside the complexity of administering this type of arrangement, auditing it and maintaining records of this/all uses of the data:

- Most informed consumers will opt-out automatically and/or object to this.
- No 'explicit consent' could be obtained where corporates use personal data (e.g. utility companies receiving / using personal payments data for individuals).
- The concept of using data in this way contradicts the intention of the Data Protection principles.

Accordingly, individuals/consumers would avoid the use of new payments/products that used their data in this way and avoid automated payments completely, not least because of the suspicion aroused by DP notices. Payment providers and innovators would not be able to create the infrastructures and complex data management systems and options for opt-in/opt-out / choices / measures to comply with the laws.

This overall would then potentially lead to:

- Less trust in the payments systems
- Few new entrants
- Less competition
- Greater payments made / used in/through traditional payments channels (Visa / Mastercard infrastructures) where there are not the 'new' 'big brother' data oversight;
- A migration to cash
- A migration to countries/payments infrastructures that are less bureaucratic and governed ex-jurisdictionally.

3. **Legal use of data -** Data should be combined centrally to provide TWO clear forms of service:
a) Financial Crime and Fraud - but limited to the use defined by the specific clauses of the legislation and ICO guidance. i.e. to aid crime prevention / Investigation through the use of the data in controlled ways and disclosed only to the ' appropriate individuals' in 'closed' circles.
b) Anonymised / collated - i.e. headline statistical data.
c) Within the system itself (NSPO) to identify system problems and anomalies

3. SPECIFIC COMMENTS

a) **Fundamental uses of data**

s1.13(c) - s6.48

- This concept needs stronger involvement of ICO - as the use of payments data is not in the gift of the stakeholders of the PSR. The data protection principles are that the data belongs to the data owners (and can only be used in the ways that they specifically allow on a case by case basis with limitations).

- This is far from an issue about the commercial cost of obtaining / storing / keeping the data.
- Just because some users / innovators / smaller players would like to have access to payments data, does not make it cost effective to provide it, legal to do so, or otherwise. This would indeed, skew the market by providing those parties that use such data at a commercial advantage and the data owners at a disadvantage (i.e. you and I as consumers - who would NOT want this). There is a perception from many smaller players that the 'bigger banks' have use of such data to their advantage: which is clearly NOT the case as the data is not collected today and not lawfully available for these 'big banks' to process today.

b) **Data Collected today - Enhancement thereof**

Data is collected today by UK Payments to report on transactions and fraud. This was organised 25 years ago as a direct consequence of a Home Office review in conjunction with (now) Prof Michael Levi et al. to gather data for the purposes of focusing fraud work / efforts and involved the (then) bank members of (then) APACS providing the data; which they did through / from Mastercard and Visa.

This needs careful rethinking to start to expand this data (as a wider data project) across all other schemes, products and payments types (including and especially) in relation to PISP / AISP data, emerging payment types and other schemes.

A model is in place and needs expanding and this should be placed upon the NPSO as an objective for 2019. It shodul also form part of mandates for licencees of regulated products to provide such data as part of their licence-granting obligations and conditions.

c) Detailed Specifics

4.43 - Include contactless, Mail order, card not present transaction

- Card authenticaiton procedures at the terminal validate the authenticity of the chip card presented.

4.44 - include AVS

- refer to CVC / CVV as those on a) The magnetic stripe and b) Those on the CHIP (ICC)
- what about mail order and telephone order transactions?
- what about 3DS?
- what about geolocation, device fingerprinting, browser checks, IP address, email check, phone number validation?
- Lots of fraud checks are carried out at the Merchant / POS
- Lots of fraud checks are carried out by the acquirer
- At the issuer - fraud scoring, aml, velicity checks, credit check, funds availability, transcaiton permitted to issuer and/or cardholder?

4.45 - Issuers use third parties to undertake many of these tasks

- if not passed issuer responds with a decline message, coded to indicate the decline reason, which is passed to the acquirer/third party and merchant.
- Data held by issuers for different lengths of time depending on many issues.

4.46 - what about cross-currency transactions, multi-currency pricing and DCC?

- disputed transactions addressed via a global chargeback processing service
- what about consumer versus commercial card programmes
- If the checks are not passed - not permitted, insufficient funds, fraud, etc, a decline with reason code is passed back by the issuer / issuer agent
- See also refunds, original credits. debit/credit cards used to fund other payment types, instalments, recurring payments..

- Historically, would give limited indication of what was being purchased other than the merchant name and MCC? Supplementary data can be obtained and linked to the purchase to indicate actual goods/services purchased.

4.48 - what about purchase data, e.g. the specific music track that is captured outside pf payment
- Or manufactured
- Fraud attempts need to be captured too NOT just ACTUAL fraud identified. Attempted fraud is important to learn from, adapt to and make changes to thwart new fraud attempts as they emerge. NB - This is very important in the thinking and seems to have been overlooked here.
- what about all the other 1,000s of data points that are mapped for verification purposes?

Discussion Questions:

1. Do you agree with our assessment of:
a. the types of data in the payments industry that are relevant for this paper? b. the types of data collected by different entities in the industry?
c. the different ways that payments data can be classified?

1a - See above - In some places YES, in other places NO : the paper has been woefully short on consideration ofthe legalities in relation to data Protection principles and Data Protection law; and it is clear that the objectives and specific uses are also unclear and unformed as yet. There is probably a general feel of general 'complaint' that data should be more available without any clear idea or strategy of what is requires / needed / desires. The driving-parties/entities for this project should be held to account for some element or detailed proposal on what should be required, how data should be used etc. It is our belief that there will be little tangible specifics, generalised wish-lists based largely upon a lot of unobtainable data (a. Commercially sensitive, b. Legally (DP) unaccessible, and c. Technically costly and impossible to obtain.)

1b. The paper only touches the surface. There needs to be a lot more detail and clarity of purpose and outcomes, with a lot more investigation into what the outcomes are, and what the legalities are.

1c. No. This needs to be considered carefully in the perspective of how the data will and should be used and how it can be reported and what would be usefully reported.

_____

5.7 - This is already progressing under PISP / AISP - PSD2
5.9 - How data can be used / analysed and extrapolated is interesting (and only in very high-level extract here), but not of any particular use. Such tools and the latest technological advances should always be used and considered as tools: but the fundamentals of the data to be used, and the requirements of the outputs of data to be specified. How it is manipulated will and should form part of the solution once these important aspects are agreed/ understood.
5.9 / 5.10 - elsewhere
- What about bad-debt / collections etc. Errant / fraudulent bad-debt / identity changers etc.
- Account takeover, identity theft
- Why no mention of CIFAS - not profit-making organisation.

5.12 - Mastercard are FAR from the only people doing this. Indeed there are many, many more forward thinking organisations addressing market needs. It is very wrong for the PSR to highlight one such tool from one such organisation who did not even develop this themselves.

Discussion Questions:

2. 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?
3. Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

- See comments throughout - this paper is quite high-level and addresses only some of the issues / challenges.

_____

6 PSR ISSUES

- PSR has highlighted major issues itself with the reluctance of end-users to give consent.
- This is very real
- There are also significant legal issues involved here too.
- The whole issue of limiting data availability to single firms etc., is a major issue: and has unstck the OIX project led by government.
- There needs to be a quantum shift in who and how data identity is managed and how it is stored / owned / controlled with the control as the DP legislation dictates, moved increasingly to US as the data owners as individuals.
- Many aspects of this discussion paper are retrograde in protecting the consumer (Data Subject), where the PSR must be mindful, and also aid in its education of enthusiastic parties within the payments industry (largely new entrants) who want to use private data to their commercial advantage and create costs to the current incumbents in the process as well as compromising al our rights as consumers - i.e. as 'Data Subjects'.

6.5(b) - We must ensure that card scheme data is included (Mastercard / Visa etc.

- "a central utility" - Owned, controlled, managed and regulated by whom? Paid for by whom?
- "KYC information" - This implies a centralise KYC repository. This is a 'hobby-horse' of a small number of challenger banks who want large incumbents to share customer KYC details - to ease their costs. The law (AML) requires organisations to undertake their own due diligence AML validation. KYC validation is costly for ALL to undertake and this should thereby not be provided as a cost to some, and not for others in a commercial world. Moreover, the data protection law is tending to draw us away from centralised KYC as detailed here: TOWARDS 'decentralised solutions' (possibly based upon distributed databases); and **definitely controlled / owned / authorised by data subjects themselves. CARE: DP law again applies here. This all 'feels' like we are pandering to the needs of the few with a generalised complain and non-specific solution ideas based upon old methods and a lack of innovation / competition thinking.**
- **KYC Thinking and legal requirements are complex and rapidly changing. There is NOT a 'one size fits all' solution or possibilities. There is also a significantly varied risk profile for organisations that have to obtain identity information KYC that needs to be addressed by organisations. There is no easy way out for the complainants in this area of interest.**

6.5 (d) - Is it really expected that common-message (data) standards will (or can be) imposed upon the international card schemes (Visa and Mastercard for example), when these are used billions of times a day by 100,000s organisations as an ergo global standard today ISO 8583? This needs a re-think and maybe a separate piece of work and thinking.

It is not a good idea to allow ISO 8583 in the UK for a large part of transactional volume and to impose ISO 20022 for all other types of payments as this will drive more solutions into the easier route standard (ISO 8583) and thereby:

- Inhibit innovation
- Reduce data availability
- Increase crime
- Inhibit competition
- Drive business / innovation / competition outside the UK borders where transactions can be more easily transported.

The principle is nonetheless the right one to adopt, albeit potentially counter-productive.

6.8 - Is this not address with the delivery of SCA and 3DS 2.0?

6.15 - This is potentially the wrong way to deliver security as it is costly and will quickly see a migration of crime/fraud without addressing the liability fundaments. However this has been raised elsewhere in relation to the COP project.

6.39 - "this data" - There is no global data-set: there seems to be a myth out there.

6.42 - What about card data - this would be a better starting point

- The speed of data cahnge , product change and updates to data will need to be coped with to avoid UK Plc becoming uncompetitive, and to allow constant innovation in all areas of development. CARE.

6.44 - It appears to us in our experience of the ICO, and to the ICO itself VERY CLEAR on what data is and can be exchanged, and how and what data can be used and how. It appears that the confusion arises mainly in this discussion paper which has applied only a liberal (and in places in the document non-legal) interpretation of the Data Protection legislation requirements. Accordingly engagement with the ICO is strogly encouraged.

- The Data Protection legislation is there to protect the consumer. It does so well.
- It does not inhibit lawful business, competition or innovation as some may perceive.
- It is clear, but is often seen as unclear when people first address what are complex issues.
- The legislation has 'checks and balances' and allows a lot within constraints that many do not appreciate.
- This discussion paper in places breaches what the ICO would expect to be required under the legislation, and what the consumer would and should expect.

6.48 - AGREE - everything is driven by business cases (that includes both financial and softer benefits (e.g. brand, marketing, relationship, service improvement narratives). This is a GOOD thing. A very good thing. Demand will evolve direct rather than imperative / legislation.

6.64 - Consider Fraud / financial crime

Discussion Questions:

End-user willingness to share data

4. Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

Access to global datasets

5. In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?
6. What models could the NPSO introduce to allow PSPs to get access to global datasets?
7. Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

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

8. 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?

Realising the benefits of enhanced data

9. Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

Other payments data-related issues

10.Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

4. - There are mistrust issues for all participants not just new entries. Banks still have baggage, as do Visa and Mastercard after recent systems issues. Cannot comment on specific questions of who and how to address etc.
5. - Yes: all the marketing and financial services mentioned already - but only on general / trend data: NOT on individual transaction enquiry basis.
6. - Clarity over what datasets are referenced here. Is this reality?
7. - Yes: subject to understanding of processing, security, usage etc. However, much of the proposed access would have to be legal, and it is questionable that this would be the case due to subject access consent etc. Reference to the ICO will be required.
8. - fraud and security provides exclusions for consent, data held for other legitimate purposes. The danger is that this will be exploited as data collected for anti-fraud, anti-credit risk anti-aml, etc may then be used / abused for marketing analysis, creation of innovative products etc., that would automatically breach Data Protection law. The technical issues around consent are

considerable, as it needs to be consent that is specific for specifies usages - so no 'blanket' authority can be assumes. Or expected.

9. - Consideration of UK business collecting and processing data on UK consumers and non-UK consumers.

- No recommendations really offered here.

10. - b2b transcations where the personal data of individuals is processed - name, email, etc. Indeed personal data is collected and transmitted in most / many payment fields - including account numbers / details etc., that would all need to be encrypted and thereby remove much of the benefits.

DEFINITIONS

- What about the other card schemes. CUPS is the worldwide biggest, Amex, Diners, Discover, JCB, WeChatPay / Alipay etc.

RESPONSE ENDS HERE

[redacted]

[redacted]

[redacted]

Barclays

Payment Systems Regulator (PSR)

Discussion paper: Data in the payments industry (June 2018)

Response on behalf of Barclays Bank

3 September 2018

Please note: *This response contains sensitive information, the disclosure of which may harm the legitimate business interests of Barclays Bank plc and Barclays Bank UK plc (together "Barclays"). We understand, therefore, that the information contained in Barclays' response will be treated in the strictest confidence.*

1. About Barclays

1.1. Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

2. Executive summary

2.1. Barclays welcomes the opportunity to comment on the Payment Systems Regulator's (PSR's) discussion paper on the use of payments data. We have also contributed to and support the response submitted by UK Finance.

2.2. The implementation of the revised payment services directive (PSD2), Open Banking and technological advancements have dramatically expanded the innovative opportunities arising from the use and sharing of payments related data.

2.3. It is therefore timely that the PSR is considering these issues, given that these new opportunities are not without risks. Importantly, with any developments it is of critical importance that consumers understand how their data is being used, that their data is held securely, and that their privacy is being respected.

2.4. This is in the context of research showing that consumers across the world consider their financial data to be their most personal and private data.[1] Barclays is acutely aware of this, and strive to ensure that we respect this through adherence to a series of principles that underpin our use of data.[2] [redacted] We want consumers to be in control of their data, and our *digisafe* campaign is at the heart of these efforts.[3]

2.5. We believe that consumers will be willing to share their payments data with new and established third-parties, and many already do so. But, to achieve this at scale, third-parties will need to introduce compelling products and win the trust of consumers. Regulators and industry bodies cannot help third-parties to build a great product, or develop a trusted brand. However, industry can help by coalescing around one common and highly trustworthy approach to data sharing, for instance the secure API based approach of Open Banking. Regulators can help by raising awareness about the protections that they have put in place to make the sharing of payments data safe. We therefore encourage the PSR to work with other relevant regulators to help consumers easily understand the regulatory protections and supervisory landscape underpinning the sharing of payments data.

2.6. Barclays supports the use of payments transaction data from multiple Payment Service Providers (PSPs) to combat financial crime, and Barclays was pleased to participate in the mule insights tactical solution project. However, the process of agreeing to share the data was complicated and time-consuming. We think the industry, via New Payment System Operator (NPSO), could develop a protocol or a framework to make it simpler for PSPs to consent to similar initiatives, while also continuing to respect their legal obligations.

2.7. Barclays believe that it will always remain appropriate for end-users, or the PSPs who have a relationship with the end-user, to have the final say about the use of consumers' payments data. A payment system operator or an infrastructure provider cannot take such a decision. This is because, in the absence of explicit consent from the end-user, it is only the PSP that has an obligation to their customers to keep their data secure.

[1] Page 5, Boston Consulting Group (November 2013), *The trust advantage: How to win with big data*, <http://image-src.bcg.com/Images/The_Trust_Advantage_Nov_2013_tcm9-92206.pdf> [accessed August 2018]
[2] For more information, please see: <https://www.barclays.co.uk/important-information/control-your-data/>
[3] For more information, please see: <https://www.barclays.co.uk/security/digisafe/>

3. The collection and classification of payments data

Question 1: Do you agree with our assessment of:

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

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

c) the different ways that payments data can be classified?

3.1. We do not disagree with the types of data in the payments industry identified by the PSR. However, we have some concerns about the level of consistency of the classifications of payments data proposed by the PSR with existing legislation and regulations. We encourage the PSR to work with Information Commissioners Office (ICO), the competent authority for the EU General Data Protection Regulation (GDPR), to ensure that the classifications the PSR has developed align with those in the Regulation.

3.2. We understand the PSR's desire to introduce the concept of "*global transaction data.*" However, do not consider there is utility in creating new definitions for data that do not have a basis in regulation or law.

3.3. There is a risk that any new definitions will confuse market participants and end-users. For instance, consumers may interpret the use of the term *global* as implying the worldwide sharing of their personal data. Or alternatively, that it includes information regarding international transactions. If consumers do not trust or are confused about what UK payment system operators are doing with their data, it may undermine the confidence they have in those systems.

3.4. The PSR's paper suggests that global transaction data could be aggregated or anonymised. Where there is aggregation or anonymisation, the PSR indicates that this may not contain personal data. We would stress that anonymisation or aggregation does not eradicate the risk of the identification of personal data.

3.5. There are examples of reverse engineering to determine details or traits of the individuals involved. From this personal details may be uncovered. Alternatively, it could be used with other available data already in the public domain to do so. Lubarsky (2018) covers many real-world examples where researchers have identified individuals in data scrubbed of personal identifiers. Examples include Netflix customers, those who used AOL's search engine and New York taxi cabs.[4]

3.6. Similarly, De Montjoye (2015) has shown that anonymous credit card transaction data can be reverse engineered. In 90% of cases the study was able to re-identify individuals using merely the date and location of four transactions. Aggregation of anonymised data did not necessarily help, the study simply needed more data points to identify individuals. With just ten transactions the study was able to identify individuals from aggregated transaction data in 80% of cases.[5]

3.7. Barclays is keenly aware of this. We have developed principles on the anonymisation and pseudonymisation of data. One of the fundamental principles is to test anonymised and aggregated data before disclosure. [redacted]

[4] Lubarsky (2018), *Re-identification of "anonymised data,"* Georgetown Law Technology Review , 1 GEO.L.TECH.REV.202(2017)

[5] De Monthoy, et al (January 2015), *Unique in the shopping mall: On the reidentifiability of credit card* metadata, Science, 30 Jan 2015, Vol 347, issue 6221

4. How is payments data used?

Question 2: 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?

Question 3: Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

4.1. The production of payments data is not the primary purpose of a payment. It is the transfer of value from party to another. The data subsequently produced is useful for the purposes identified by the PSR. But, maintaining the confidence that end-users have in providing data to allow a payment to be made is of paramount importance. We would not wish to make end-users reluctant to use a certain payment method because of concerns about how their data will be used or commercialised. So care should be taken when considering extension of existing uses of payments data.

4.2. The only additional use of payments data not covered by the PSR is the use of the data by Government or public bodies for public policy reasons. For example, HMRC currently collects details about individuals' wages from the Bacs payment system. The purpose of collecting payroll data, known as Real Time Information, is to help ensure that UK taxpayers are paying the correct amount of income tax. HMRC was required to make regulatory and legislative changes to make the collection of this data possible.

4.3. We think that their further public policy uses of payments data are likely. In the Bank of England's consultation paper on a global standard to modernise UK payments, the Bank announced that once RT2 replaces CHAPS it plans to share anonymised transaction level information with the Office for National Statistics (ONS). ONS could then use that data in their statistics measuring the size and health of the UK economy. The Bank acknowledges that any sharing of data would be subject to the relevant data sharing legislative requirements.[6]

4.4. Barclays would like to highlight at this juncture that just because an organisation has transaction data does not mean it can use that data however the organisation holding that data determines. Legal, regulatory and contractual restrictions apply.

4.5. We think there are also ethical considerations regarding the use of payments data. It is vital that organisations have trust in the collection and use of their data. Those collecting and using transaction data must be clear with end-users about what data they are collecting, for what purpose it will be used, and by whom. We think this is particularly the case for financial transaction data. Research by Boston Consulting Group found that across developed countries credit card data and financial data is considered the most private personal data. Both categories of data came above health/genetic information and information about children.[7]

4.6. Research by Which? found that vulnerable consumers were more nervous than any other consumers about data collection and usage.[8] Unpublished research for Barclays by GfK supports this finding. It found anxiety among both vulnerable and non-vulnerable customers about banks using data to make targeted interventions. In addition, payment transaction data may lead to the identification of a customer's vulnerability (for instance excessive gambling) or changing life circumstances that could suggest a risk of vulnerability. Knowledge of such information could lead to supportive activity. But, it could also lead to financial exclusion or exploitation, and some consumers in our GfK research explicitly expressed this concern. These risks and ethical considerations must be borne in mind when considering use of payments data.

---

[6] Page 46, Bank of England (June 2018), *ISO 20022 consultation paper: A global standard to modernise UK Payments*, Bank of England <https://www.bankofengland.co.uk/-/media/boe/files/payments/iso-20022-consultation-paper.pdf?la=en&hash=ED0713BA2B734D21D2485F3F3CC571CE9F9C17CA>, [accessed August 2018]

[7] Page 5, Boston Consulting Group (November 2013),

[8] Which? (June 2018), *Control Alt delete? The future of customer data*, Which?, <https://about-which.s3.amazonaws.com/policy/media/documents/5b5f07fc6be5f-Control%20Alt%20or%20Delete%20report.pdf>, [accessed August 2018]

5. End-user willingness to share data

Question 4: Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

5.1. The PSR notes that *"end-user reluctance to provide access to their* [payments related*] data due to a lack of trust, data protection concerns or aversion to technology could restrict demand for new overlay services."* The PSR proposes that there is a *"range of actions that could be pursued to address this reluctance. One solution could be campaigns to educate consumers about how their data will be used, including the regulations and initiatives that are in place to protect them."*[9]

5.2. An economy where people are more willing to share data with third parties has benefits. However, consumers must still be protected. We agree with the position stated by Department for Business, Energy and Industrial Strategy (BEIS) recently: "*We want to make sure that the markets of the future are designed to encourage competition and innovation, and at the same time ensure that consumers are treated fairly, their data is held securely and used appropriately, and their privacy is respected."*[10]

5.3. So we recognise the PSR's views and description of the potential for consumers to be uncertain about sharing their financial data with new third-party providers. There is often low consumer awareness of new capabilities provided under any legislation. However, we do not think it is appropriate to persuade consumers to use a service if they do not wish to do so.

5.4. Open banking is very new, and the sharing of financial data with third parties is not mature. The revised payments services directive (PSD2) has only just been implemented (January 2018). PSD2 has brought existing third party data sharing services into the regulatory remit of the Financial Conduct Authority (FCA) and, where a customer provides their explicit consent, guaranteeing those third parties access rights to transaction related data for payment accounts. The introduction of Open Banking earlier this year has now made it simpler and safer for consumers to share financial data with third parties. But, it is not clear how the market will develop.

5.5. Over time we expect that more participants will promote new or evolved services that utilise the sharing of payments related data. We believe this will increase awareness of the services and the protections offered by the changing regulations and the implementation of Open Banking. Despite these market developments, we do not think it reasonable to expect exponential growth in the next few years. We expect growth to be observed over a longer timeframe. Providers have to enter the market with products that consumers want to use, and feel safe using.

5.6. Arguably the most significant recent change in how British consumers interact with payments is the introduction of contactless payment cards. In 2007 Barclays introduced the first contactless card in the UK, and approximately 250,000 contactless cards were issued that year and only very few payment terminals could accept those cards. So it is unsurprising that in 2007 only 10,000 contactless transactions were made. [11] However, by the end of 2017, 10 years later, there were

[9] Page 40, Payment System Regulator (June 2018), *Discussion paper: Data in the payments industry*, <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf>, [accessed August 2018]

[10] Page 7, Department for Business Energy and Industrial Strategy (April 2018), *Modernising consumer markets: Consumer green paper*, <https://beisgovuk.citizenspace.com/ccp/consumer-green-paper/supporting_documents/Modernising%20Modern%20Consumer%20Green%20Paper.pdf>, [accessed August 2018]

[11] Page 2, UK Finance (September 2017), *Contactless 10 year report*, <https://www.ukfinance.org.uk/wp-content/uploads/2017/09/UK-FINANCE_Contactless-10-year-report-September-2017.pdf>, [accessed September 2018]

nearly 119 million contactless cards in circulation, and 5.6 billion contactless payments were made.[12]

5.7. The most developed market for the sharing of a consumers' financial data is in the area of personal financial management applications. [redacted] The legitimacy of FCA regulation and efficient and secure transmission of data by APIs under Open Banking will, we believe, accelerate the use of these services by consumers.

5.8. However, consumers are only going to be willing to share their payments related data if there is a compelling product or service. Continuing the analogy with contactless payment cards, the compelling use case of public transport was the catalyst for the growth in contactless payments. Consumers were able to grow accustomed to using their contactless card in a familiar environment, Oyster cards had operated on a similar touch in, touch out basis. This gave consumers the confidence to use their contactless cards for other purchases. Transport for London first introduced contactless payments on buses in 2012, and in September 2014 it expanded contactless payments to tube and rail journeys. At the end of 2015, the London transport network represented 11% of contactless transactions in the UK.[13]

5.9. Trust is also key, people in the developed world view their financial data as more private than their own health or genetic information. [redacted] It is up to market participants to develop the compelling products or services and to the win the consumer's trust that they will keep their data secure.

5.10. The industry and regulators can help stimulate consumer trust by developing and adopting a single, common and highly trustworthy approach to the sharing of payments data. Fragmentation of approach can lead to consumer confusion and damage confidence. For example, in relation to PSD2 and Open Banking we support the adoption of API standards for data sharing over screen-scraping approaches by all market participants.

5.11. Barclays have taken action to help consumers understand the value of their data. We want to put consumers in control of their data. Our *digisafe* campaign highlights how consumers can take steps to ensure that they are not sharing more data than they would like. [14] [redacted]

5.12. In addition to all this activity by market participants and the industry, we think there is a role for the regulatory authorities to raise awareness about the protections that they have put in place to make sharing payments data safe. The authorities, working together, should help consumers easily understand the regulatory and supervisory landscape underpinning the sharing of

[12] Page 10, UK Finance (June 2018), UK Payments Markets 2018, UK Finance, <https://www.ukfinance.org.uk/wp-content/uploads/2018/06/Summary-UK-Payment-Markets-2018-1.pdf>, [accessed August 2018]
[13] Page 3, UK Finance (September 2017),
[14] We have included three examples of marketing material from our *digisafe* campaign with this submission. *Digisafe* television adverts can be viewed here: <https://www.youtube.com/watch?v=RszVPiZbPeg> and here: <https://www.youtube.com/watch?v=vPJ6irUDmHI>

payments data. The purpose of such a campaign is not to make consumers trust a specific participant, but, to give them confidence in the regulatory protections in place.

5.13. We support work by the regulators to raise awareness about the regulatory protections in place for payments data sharing because we saw the benefit from similar industry activities undertaken in relation to contactless payment. The industry created a single, highly secure standard for contactless payments with security standards identical to those in place for any other chip and pin card. The industry then sought to reassure customers about those protections. As the protections are identical to chip and pin payments when the proposition is used responsibly the issuer stands behind the cardholder in protecting against fraudulent use. Hence the contactless innovation in payment experience, optimised for speed and convenience of the user (and merchant recipient) is actually underpinned by the same security standards as its traditional payment counterpart.

5.14. We believe that, as with contactless payments: if compelling services are developed; all participants adopt one common approach to the mechanics of payments data sharing and describe the protections in place in a familiar, accessible and accurate manner; and regulators are clear about the protections they have put in place, then it will stimulate consumer confidence in the new services, whether from new or established providers.

7. Access to global datasets and developing new industry-wide fraud and anti-money laundering (AML) prevention measures

Question 5: In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

Question 6: What models could the NPSO introduce to allow PSPs to get access to global datasets?

Question 7: Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

Question 8: 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?

7.1. As noted in our response to question one, we think the definition of *global transaction data* and by extension *global datasets* could be confusing and unhelpful.

7.2. Regarding the substance of the PSR's questions, we think the PSR's discussion raises some interesting questions regarding access to the data relating to all of the transactions within a payment system. However, we are concerned that the PSR has some misconceptions around that data.

7.3. It is crucial to remember that the data in question relates to the end-user. By making payments, end-users allow their PSP (usually as part of a framework contract) to use that data to, amongst other things, process transactions. With the interbank payment systems, the agreements between the PSPs, payment system operators and any infrastructure providers are explicit on the use of transaction data by those organisations. Those permissions are based on the agreement in place between the end-user and the PSP.

7.4. The PSR acknowledges that payment system operators and central infrastructure providers are only able to use personal data for the purposes agreed by PSPs (and by extension end-users). Therefore, we are confused that the PSR concludes that "*to protect their competitive advantage, the PSOs* [Payment System Operators] *and their central infrastructure providers may not have a strong incentive to make data accessible. For instance, they may perceive that they are better 'protected' from liability if they share less data.*"[15] Ultimately we cannot see how the interbank payment systems or their infrastructure providers have a competitive advantage from holding data that they are only able to use for limited purposes and are not free to exploit for commercial advantage.

7.5. Because data relates to the end-user, who only has an agreement with their PSP, we do not see how it is possible for a payment system operator, or any other related organisation, to share the personal data of an individual for commercial benefit, or the commercial benefit of another third party, without their consent. Regulations and the related contracts are clear. However, if the purpose of providing more extensive access to data is to prevent fraud and money laundering, then we support this and do not believe that there is apparent regulatory tension.

7.6. The GDPR requires controllers to establish an appropriate lawful basis for the personal data that they process, and controllers are likely to be able to rely on the *legitimate interests* condition for processing data for the prevention, detection and investigation of crimes. If the *legitimate interests* condition can be relied upon, there would be no requirements for *consent processes* to

[15] Page 42, Payment Systems Regulator (June 2018)

be established. In such circumstances, an appropriate level of transparency with the data subject would be required. Such content is generally included within PSPs' privacy notices.

7.7. Barclays do support the use of payments transaction data to combat financial crime, with likely resulting benefits to consumers. More extensive use of such data can enhance detection and support prevention strategies. The benefit of a dataset that consists of many PSPs' information is that it can help combat the layering of funds. Layering is a known risk where perpetrators of fraud use multiple beneficiary accounts. Use of numerous accounts hampers tracking and recovery of the proceeds of fraud. Having an automated approach to track frauds may improve our ability to freeze funds for victims of crime, aid repatriation, and support both fraud and scam investigations. This is why Barclays was pleased to participate with other PSPs in the mule insights tactical solution project.

7.8. The mule insights tactical solutions project is an excellent example of the industry collaborating and using payment transaction data to combat financial crime. However, the process of agreeing to share the data was complicated and time-consuming. We think the industry, via New Payment System Operator (NPSO), could develop a protocol or a framework to make it simpler for PSPs to consent to initiatives that seek to use payments transaction data to prevent or reduce financial crime, while also continuing to respect their legal obligations.

7.9. It will always remain appropriate for PSPs to have the final say about how their customers' data is used to combat financial crime. PSPs must be comfortable that the usage of the data, the storage of that data (including geographic location) and the ultimate destruction of that data meets their requirements. It is only the PSP that has an obligation to their customers and, in the event of a regulatory breach, may be found culpable for failing to keep personal data secure.

7.10. We agree with the PSR that nothing in the New Payments Architecture (NPA) design or the agreements between NPSO and infrastructure providers should prevent PSPs or a group of PSPs agreeing to share their data with another third party for financial crime prevention.

7.11. We have no view on how technically to achieve this, whether via APIs as proposed by the PSR or another method. We think the PSR or NPSO should consider all the options and technology available. There may be alternatives to the creation of a central repository of data, or multiple duplicate repositories of that data, that could reduce the risk associated with holding large scale data in one place. De-centralised data models are attractive as the relevant data point can be called as required.

7.12. The PSR noted that allowing third parties to access transaction information would enable "*multiple analytics providers to compete effectively in the market for data analytics services.*"[16] This may well be the case. However, the paper does not mention the security risk of creating duplicate data sets of UK payments data with multiple parties. Or the privacy risks. Once data is released, it is impossible to be sure that it has been destroyed.

7.13. The data concerned is highly sensitive. Security is hugely important. Breach of the interbank payments could release data on every UK citizen or group of citizens. The release of such data could lead to significant detriments. As we noted earlier in this paper, research has shown that even in anonymous data it is possible to identify individuals from very few data points. Data breaches could; inadvertently expose an individual's political affiliations; expose the financial information of notable or vulnerable individuals; undermine confidence in the UK payment systems; or, expose people to a higher risk of fraud.

7.14. The knowledge of transaction details obtained from a data breach or from another source can aid social engineering and so increase consumer susceptibility to scams and subsequent claims for

[16] Page 44, Payment Systems Regulator (June 2018)

reimbursement. Protection of consumers from increasingly sophisticated scams continues to be a core focus of Barclays. So there must be a balance to attain the optimal mix of data sharing and consumer protection.

7.15. In addition to the security and privacy risks highlighted above, there are many practical ramifications arising from the NPSO or other payment system operators allowing third parties to access *global transaction datasets*, whether aggregated, anonymised or not. For instance, who will monitor and investigate potential breaches? Who will test to ensure that aggregated or anonymised data cannot be reverse engineered? Who will provide assurance that the approach of the third parties is safe and secure? Who will contact customers if a breach occurs or provide remediation if necessary?

7.16. We urge careful consideration by the PSR on the proposal made in relation to allowing access to *global transaction data*. We do think it should be easier for PSPs to agree to share their collective transaction data with third parties to combat financial crime. But, we think it will always remain appropriate for end-users, or the PSPs who have a relationship with the end-user, to have the final say about the use of their payments data.

8. Realising the benefits of enhanced data

Question 9: Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

8.1. The creation of RT2 to replace the CHAPS payment system, and NPA to replace the payments systems of Bacs, Faster Payments and the Cheque Image Clearing System, is an opportunity to adopt new and common payment messaging standards (ISO 20022). These new standards will allow the provision of structured data for all wholesale and retail interbank payments in the UK.

8.2. Barclays think the introduction of structured data is a unique opportunity to help PSPs get a better understanding of the parties involved in a payment and the purpose of the payment. PSPs, like Barclays, will be able to automate our processes, make more informed decisions, and reduce the impact on end-users. For instance, we expect that it will minimise payment delays, payment repairs and queries. However, the biggest challenge is to encourage and educate consumers and businesses to use these structured data fields.

8.3. We also think the ability of businesses and individuals to associate more data with a payment or series of payments, known as enhanced data, will also benefit users of the payment systems. In our response to the Payment Strategy Forum's (the Forum) consultation, we agreed with the Forum that enhanced data could assist business in the reconciliation of their payments. We also think it could help make payments personal.[17]

8.4. Like any change, the introduction of enhanced data and being able to exploit enhanced data will involve an implementation cost for businesses, PSP, and third-party services providers. We consider that companies which have already adopted processes or software that enable the reconciliation of their payments are not going to prioritise the implementation of enhanced data. However, newer businesses or businesses upgrading their back-office systems may choose to use the features of enhanced data sooner. It is likely that software providers, such as accountancy packages or cash management products, will upgrade their products to support such services. Users of such packages may also be early adopters.

8.5. Barclays advocate an approach to enhanced data that does not significantly expand the payload of a payment message. Instead, we favour agreeing standards that allow for the association of data with payment and associated rules regarding the storage, security and privacy of that data. This can help ensure that payment messages remain efficient and help stimulate competition. The NPSO will, we assume, be responsible for developing these standards.

8.6. If NPSO develops an approach to enhanced data storage, security and privacy that is inflexible, or where the standards used are lower or not in line with the businesses own standards or applicable legislation Business may be reluctant to use the service. So we encourage NPSO to consult widely on any security standards or storage approach. Overall, we favour an approach that enables companies to express their preference about how their data is stored. Some companies may favour more expensive, more secure approaches. Others may be more price sensitive. This is why we do not favour the creation of an industry-specific data store for enhanced data. Instead NPSO could set minimum standards and expectations of the storage of enhanced data. PSPs and other third parties will then be free to offer enhanced data solutions that meet the requirements of users in a competitive marketplace.

[17] Page 5, Barclays (September 2017), *Blueprint for the future of UK payments – A Barclays response*, <https://implementation.paymentsforum.uk/file/5011/download?token=CNLUcSzX> [accessed August 2018]

9. Other payments data-related issues

Question 10: Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

9.1. We have no further comments to make.

[redacted]

Baringa Partners

A response to the Discussion Paper: Data in the payments industry

September 2018

Introduction

Baringa Partners is pleased to respond to the discussion paper published by the PRA to explore opportunities for advanced uses of payments data to drive increasing value across the industry.

We have responded to selected questions where we believe we have a relevant point of view to offer based on our work across financial services and payments infrastructure providers. We would welcome the opportunity to continue to support further industry developments in this area and are passionate about continuing to develop a competitive and world-leading payments ecosystem within the United Kingdom.

Question 4 – Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

4.1. The number of recent high profile and aggressive nature of reported data breaches across various industries, increasingly topical given GDPR, means that consumers are increasingly alert around how their data will be used. Established financial services firms have largely managed to avoid direct involvement, which has further served to reinforce the trust that consumers have in established firms over new third party providers.

4.2. We do agree that this mismatch could lead to harm in innovation and competition. Initially, we believe that the development of new innovative services by new third party provides (and to a lesser extent, trusted brands) will be tailored more towards the population segments who demonstrate a higher level of comfort with the sharing and commercialisation of their data. However, as with any paradigm shift such as that provided by open data, we believe that with sufficient benefit being evidenced and advertised by the early adopters, usage will quickly extend to more cautious groups of potential adopters. The services provided just need to be compelling enough. The lack of trust in TPPs will slow, but not cease, the innovation and competition in this space. For these more cautious customer segments they will be better served in the short term by trusted financial brands.

4.3. As part of the UK implementation of Open Banking, the industry needs to be assured that sufficient standards for third party participants have been defined and will be enforced. This will require publication to all participants and stakeholders of a set of standards which has been shaped based on robust public consultation. It is imperative that the assessment of third parties against those standards is not just a one-off assessment but that this is supported by a process to ensure ongoing compliance also.

4.4. Communication of safeguard, practices and adherence to agreed standards needs to be very clear at the point of proposal by TPPs. Customers need to know that a set of standards and guidelines exists and be able to identify TPPs which have been assessed as adhering to these. We acknowledge that there were prior discussions at the OBIE around an 'Open Banking kitemark'. Due to a lack of technical feasibility this proposal was stopped, but provision of easy access to a central registry or similar should be considered. This should be

a project conducted between the OBIE and the PSR in close collaboration with established brands in the industry and smaller TPPs who are approved PISPs and AISPs. We acknowledge that the introduction of SCA measures in September 2019 will go some way to supporting this objective.

Question 5 – In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

5.1. We agree overall that global transaction data held in central infrastructure could be used by a variety of providers to develop services.

5.2. Examples of such services could include:

a. Transaction monitoring

- Fraud and AML alert creation, based on a richer history of payments emanating from or to a given entity e.g. identification of layered transfers into a beneficiary
- Fraud and AML alert resolution and triage, supporting investigation and severity assessment of alerts
- Additional customer data for profiling (company data and individuals), to support onboarding, AML and KYC checking
- Additional payer and payee data to facilitate a per-payment risk score

b. Operational

- Use of AI and machine learning services to increase straight-through-processing rates
- Support for reconciliation services – data matching and enrichment

c. Commercial

- Support customer profiling for targeted cross-selling opportunities and marketing
- Identification of demand for services and products to inform investment opportunities e.g. to be able to assess changes in demand in a given geography to inform firm location decisions
- The acceleration of services which are able to categorise and interpret the payment types themselves, particularly those who learn through the use of AI technologies
- Creation of additional services / markets for data which provide more details about the specific products and services underlying the payments and transactions
- Trading services and business models, to inform investment decisions based on the movement of funds and activities

Question 6 – What models could the NPSO introduce to allow PSPs (payment service providers) to get access to global datasets?

6.1. There are a variety of models that can be introduced by the NPSO to allow PSP access to global datasets all of which will need to be managed by the NPSO to ensure access is administered appropriately to authorised PSPs and that access is used for its intended purpose.

6.2. Some of the models below are already in use across the financial services industry with a specific example being the Insurance Fraud Bureau in the UK (and similarly in Canada) with coverage of 97% of all claims data across all insurers to detect and prevent fraudulent activity.

6.3. The underlying prerequisite of harnessing the true value from global datasets is being able to aggregate data across different sources on which entity resolution and network-building can be performed. Only through an aggregate global data set is it possible to generate valuable insights.

6.4. Possible access models include:

d. Pre-defined data extracts generated by the NPSO

- Stand-along data extracts provided periodically by the NPSO.
- Extracts would be the result of insights or improvements in entity resolution and network-building that have been orchestrated by the NPSO.
- For the extracts to be valuable to PSPs would be dependent on the ability of the NPSO to perform value-add analysis to meet specific TPP requirements.

e. Access to data stores via APIs

- Allow PSP access to data stores via APIs to extract the data directly.
- Access can be to either predefined views where analytics has been performed (as per the above) or to subsets of the global datasets for analytics to be performed by the PSP and potentially combined with their own proprietary data within their own environment.
- Data would need to be segregated depending on the purpose of access which will be the challenge of the NPSO to find the balance between allowing enough data scope to provide insight without compromising data privacy or facilitating fraudulent activity.

f. Access to a common "sandpit" environment

- This option potentially allows greater access to data for PSPs as it will be a common environment that will be hosted and managed by the NPSO.
- This would imply greater management overhead for the NPSO however allows greater economies of scale across the industry especially if hosted within a cloud environment.

- Data would be restricted within the environment however there would need to be the provision of analytical tools to support insight generation which can then be shared but also governed by the NPSO.
- There could also be the option to merge PSP data with the cloud environment to allow data-sets to be joined. However, this will need to be within a segregated environment overseen by the NPSO at a cost to the PSP.

6.5. Levels of access and subsequent value to PSPs increase as you progress from an extract only model to a central sand pit model. However, the complexity and governance which the NPSO will need to manage also increases of which a balance must be struck.

6.6. Access management will be a key challenge across all models. Tiered access levels will need to be considered e.g. to allow for greater levels of access for the purposes of AML and fraud investigation versus more commercial purposes. Administering these access levels along with the associated vetting for higher levels of access will also need to be considered and it will be critical to ensure tight controls are enforced for greater levels of access to prevent fraudulent behaviour.

Question 7 – Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

7.1. We believe it critical that all regulated PSOs including interbank and card scheme operations should be required to provide some access to global transaction data sets as this is the only way to enable true insights into fighting fraud.

7.2. In this case the end to end global transaction data set required for fraud investigation would form the most comprehensive view of the payments landscape. To avoid duplicating a similar dataset to service commercial use cases the NPSO will need to be able to segregate sensitive data sets and have the flexibility to administer access to segments based on access levels and purpose. This allows for better economies of scale and avoids unnecessary overheads for ongoing maintenance and support.

7.3. Management of the provision of global data sets across all PSOs will need to be centrally co-ordinated by the NPSO and where required maintain relationships with PSOs not within the direct remit of the NPSO. This will involve defining the commercial arrangement to cover initial development and ongoing operational costs as well as the governance required to ensure the necessary controls are in place to safe guard the data as a whole. Cloud technology will be a key consideration with regards to ensuring current and future operational cost are kept to a minimum.

Question 8 – 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?

8.1. One of the key principles of GDPR is to document what personal data you an organisation holds, where it came from and who you share it is shared with. To achieve this, effective policies and procedures need to be in place. Although it does not fully resolved the potential conflict between the development of industry-wide transaction data analysis tools and data

protection requirements, it this will significantly mitigate the risk and help to comply with the GDPR's accountability principle.

8.2. Under GDPR, it is possible to share data, including transaction data where it is in the vital interest of public or the individual. Financial Crime prevention falls within that category. Organisations would need to notify individuals that the data is shared externally.

8.3. Organisations are not able to share special category data without explicit consent, therefore technical standards would need to clearly define the data that is shared and consider / resolve questions related to special category data that is shared without intention (e.g. does the payment reference data show an affiliation with a political party?). Consent is the only lawful basis that company can use to collect and share special category of data, but you often won't need consent. If consent is difficult, organisations can look for a different lawful basis.

8.4. Another way to mitigate conflict is also to ensure the personal data being processed or shared is adequate, relevant and limited to what is necessary. This complies with the principle of data minimisation under GDPR.

8.5. We also note that GDPR is a real opportunity for companies to build and retain customer trust about how their data are managed, and expect this to be seen increasingly as a source of competitive advantage. By being more transparent and clearer to customers, firms should expect customer to be more willing to share their data if they see a real benefit out of it and trust it will be done in a secured way. This should mitigate some of the risks outlined in the paper relating to customer reticence to share their data.

About Baringa Partners

Baringa Partners is an independent business and technology consultancy. We help businesses run more effectively, navigate industry shifts and reach new markets. We use our industry insights, ideas and pragmatism to help each client improve their business. Collaboration is central to our strategy and culture ensuring we attract the brightest and the best. And it's why clients love working with us.

Baringa launched in 2000 and now has more than 600 staff and 60 partners across five geographies, represented by our four practice areas of Energy and Resources, Financial Services, Telecoms and Media and Consumer Products and Retail. These practices are supported by cross-sector teams focused on Strategy and Analytics, Business and Organisation Transformation, Supply Chain, Programme Delivery, Process and Operational Efficiency, Risk and Compliance, Customer Experience and Information Technology.

In 2017, Baringa Partners was ranked 1st Place in the UK Best Workplaces™ list by Great Place to Work® UK. This is the 11th consecutive year the firm has won an award for its inclusive and engaging company culture. In 2016 Baringa achieved Master status, when it became a 'great place to work' for the 10th year in a row.

[redacted]

Baringa. Brighter Together.

Bank of England (BoE)

BANK OF ENGLAND

[redacted]

[redacted]

UNCLASSIFIED

3 September 2018

Dear Sir/Madam,

We welcome the discussion paper 'Data in the payments industry', which was published by the PSR in June 2018. We are responding to this paper as the policy team within the Bank's Market Services Division (MSD). MSD is responsible for operation of the UK's real-time gross settlement (RTGS) infrastructure, and CHAPS payment system. We are providing comments on aspects of the paper that could impact on these elements of the Bank's responsibilities, as well as potential impacts on the Bank's wider financial stability objectives. For avoidance of doubt, it does not consider issues specifically relating to the supervision of payment systems or their participants.

We would be very happy to discuss our response further, or respond to any further questions or queries.

[redacted]

Bank of England Response to the PSR paper 'Data in the payments industry'

Introduction

1. We welcome the proactive approach of the PSR to promoting competition and innovation as part of the June 2018 discussion paper 'Data in the payments industry'. We are responding to this consultation where we consider that it could impact on our objectives as the operator of the CHAPS payment system and RTGS infrastructure. Note that while this response is also written in the context of the Bank's monetary and financial stability objectives, it does not consider specific issues relating to supervision of payment systems or participants. Nor does it aim to cover issues around consent, liability or charging, which we expect will be provided by participants of payment systems.

2. We note that the focus of the PSR's discussion paper is retail systems.[1] However, we have taken the opportunity to set out our views over use of data in CHAPS[2] as well as retail systems.

3. We are content for this response to be shared publicly, and would welcome further discussion with the PSR on any of these issues.

Bank Response

4. The Bank, in conjunction with the New Payment System Operator (NPSO), recently published a consultation paper considering additional data in payment messages, so-called "enhanced data", as part of the implementation of the new messaging standard ISO 20022 for the UK.[3] Our view is that this enhanced data has the potential to transform the payments industry and we are therefore pleased that the PSR is examining barriers to use of this data and considering how those barriers might be overcome. We hope that this work will feed into the longer-term work across the Bank, NPSO and PSR to drive full adoption of ISO 20022 in the UK to enable the associated benefits. As this work progresses, we would be keen to discuss further how we can best use our respective roles to promote use of the enhanced data across payments systems.

5. The Bank's consultation proposed introduction of a Common UK Credit Message, shared across both CHAPS and the New Payments Architecture (NPA). The consultation also proposed introduction of enhanced data including purpose codes, legal entity identifiers and structured remittance information. We consider that this information will facilitate the

[1] We use the term retail systems to mean Bacs, Faster Payments, cheques (which will all be operated by the NPSO), LINK, Visa and MasterCard.
[2] For avoidance of doubt, the Bank is not subject to regulation by the PSR. For example, the PSR's powers of direction cannot be applied to the Bank as CHAPS payment system operator, nor as an infrastructure provider to CHAPS, nor through our participation in payment systems.
[3] ISO 20022 Consultation Paper: a global standard to modernise UK payments, which closed on 18 July.

detailed payment data analysis that the PSR envisage parties will want to undertake. The Bank is in the process of analysing in detail the responses to its consultation and is therefore unable to provide any further detail at this stage regarding the adoption of these proposals, but cautions that it expects that data enhancements are not likely to be rolled out in respect of CHAPS until 2022-2023, as this is dependent on the delivery of the renewed RTGS system. We plan to publish our response to the consultation in December 2018.

6. The discussion paper states that the PSR is considering whether to require the NPA to facilitate data sharing from the central infrastructure. Whilst we do not object to this requirement in principle, we would like to highlight that in certain (particularly stressed) circumstances, the release of detailed real-time, non-anonymous data could raise financial stability concerns. For instance, the release of real-time information on payment flows could enable the identification of a bank experiencing a withdrawal of retail deposits. If released (or leaked) publicly without sufficient context or understanding, such information has the potential to undermine the Bank's financial stability operations, and potentially magnify financial stability risks. We therefore think that the PSR should carefully factor this in if it designs a regime for access to this information and consider exactly what level of detail of information should be shared with external parties, especially in real time.

7. More generally, we think care should also be taken to ensure that information is not used by third parties for inappropriate purposes. You may wish to consider a regime which imposes different standards based on the data accessed – for example information provided in real time, or containing personal data, should have higher standards attached than anonymised, aggregated or time-lagged data – or where certain transactions can be excluded. We would be keen to discuss this topic with you in more detail as your thinking develops.

8. We are also aware as CHAPS payment system operator, that there is a risk that transactions could migrate from retail systems to CHAPS to avoid their inclusion in the NPA global data set, particularly if retail payment system participants and users are not comfortable or properly informed about the level of detail or degree of control over data shared from the central infrastructure. We would be keen to avoid such an outcome, not only because it would undermine the purpose and benefits of this data project, but because it could also very significantly increase CHAPS volumes, which if unexpected may represent to the smooth processing of CHAPS payments.

9. While it is not explicitly referred to in the discussion paper, we also thought it helpful to set out our thoughts on access to the full CHAPS payments data set, which the Bank holds. At present, the data is only used within the Bank for monetary and financial stability purposes including as end-to-end systemic risk manager for CHAPS. While our analysis of this data may sometimes lead to public statements or articles these never include raw information. Elements of the CHAPS payments data set are obviously highly sensitive. These include CHAPS payments that relate to the Bank's own overt or covert liquidity operations with the market. It is important for UK financial stability that this information is carefully controlled and protected.

10. Nevertheless, our expectation and intention is that the Bank will provide greater access to elements of the CHAPS payments data set once the renewed RTGS system is live, and in particular once enhanced data is available as part of migration to ISO 20022 messaging standards. For instance, we plan to share anonymised transaction level information with the Office for National Statistics (ONS) for use in their statistics measuring the size and health of the UK economy, subject to relevant data sharing legislative gateways.

11. Indeed, the Bank is a key consumer of such national statistics as part of its role in maintaining monetary stability, and we can therefore see value in aggregated retail systems data, including information such as salary payments, being provided to the ONS also. But our expectation is that much of the Bank's analysis supporting both its monetary and financial stability objectives, and also as end-to-end systemic risk manager for the CHAPS payment system, will continue to be undertaken in-house.

12. Payments data ultimately belongs to the parties involved in each transaction. In particular, under the terms of our contractual agreements with CHAPS Direct Participants, in all but limited circumstances the Direct Participants retain control over personal data held in CHAPS messages as data controller. While we use this data for specific purposes, the Bank cannot release transaction data to third parties without the express permission of the CHAPS Direct Participants involved, who in turn would need to obtain their customers' consent. As an example of this, we are considering, as part of the renewed RTGS system, whether the CHAPS payment data could be provided to a third party transaction monitoring service in order to further improve fraud detection and prevention within CHAPS payment flows. However, this would only be with the agreement of each Direct Participant and with appropriate controls around it. Given the sensitivities of the CHAPS payments data our expectation is that express consent would have to be given for each particular use of the data, rather than designing an access regime setting out permissions in advance. We expect that similar issues may exist in retail schemes.

13. There is a suggestion that "public information and education material needs to be made available" to encourage customers to make their data accessible and therefore also realise the benefits of new service offerings. The PSR requests "views on the role of payment schemes in providing customers with such information". The Bank believes that the primary responsibility for providing information and educational material to consumers lies with payment service providers, as they own the contractual relationships with consumers that specify the conditions under which consumers' payment data can be used. Nevertheless, the Bank recognises that there may be an additional role for payment system operators in providing information and educational material, particularly where encouraging the sharing of such data would support the end-to-end systemic risk management of the payment system. For example, we would support any public information or education initiatives by CHAPS Direct Participants that would allow them to share consumer payments data with a trusted third-party fraud monitoring service, in order to help detect and prevent fraud within CHAPS payments.

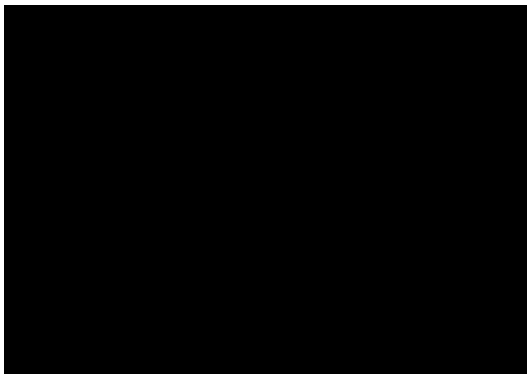
Experian

Experian's response to: DP18/1; Discussion paper:

Data in the payments industry

Payment System Regulator

Response sent 3 September 2018



Introduction

Experian is pleased to offer comments on; Discussion paper, Data in the payments industry.

Background on Experian

Experian is a credit reference and data analytics business, providing services direct to consumers and to businesses across a number of sectors. We provide credit data services to lenders and operate in the price comparison website market.

Experian's data and analytics help people, businesses and organisations protect, manage and make the most of their data, creating better business and consumer outcomes and building stronger customer relationships.

Experian helps people, businesses and organisations to:

- **Lend and borrow responsibly:** by gathering information on past and present credit commitments, such as loans, mortgages and credit cards, Experian helps lenders to understand whether people and businesses can manage their debt repayments, so they can borrow and lend responsibly.
- **Treat people and businesses fairly:** because Experian helps organisations make decisions based on facts, they can treat people and businesses fairly and consistently, which in turn helps people to access credit.
- **Consumer empowerment**: because Experian provides consumers with access to their financial data, we can empower them to use it to make financial decisions through our personal credit information and comparison services.
- **Make better, more efficient decisions to create better business outcomes:** by gathering and analysing information supplied by people and businesses, organisations can make quicker decisions, now taking seconds and minutes instead of days. Organisations need to make fewer manual checks which means less administration and fewer bad debts. This means the cost of extending credit is lower.

Response to Consultation Paper

1. *Do you agree with our assessment of:*

a. *the types of data in the payments industry that are relevant for this paper*?

Yes.

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

Yes, however we believe that some data elements could be missing:

Bacs:

- Do we need to consider customer roll/reference numbers for building society and credit union accounts?
- Should we also consider the payment type, and reference data such as field 10 which may be the direct debit reference, and field 7 - the numeric code used by HMRC for RTI matching.

FPS:

- Do we need to consider customer roll/reference numbers for payments to building society and credit union accounts?
- Should we also consider the payment reference data? For example, the consumer's unique payee reference for a utility bill.

Payment card:

- Should we also consider the name of the merchant involved in the transaction?

c. *the different ways that payments data can be classified?*

Yes, we agree with the classification categories. However, we would challenge the classification of some of the examples:

Bacs, FPS and CHAPS:

- Personal data / non personal data - Are the sort code and account number correctly classified as personal data, do the account details identify an individual?

CHAPS:

- "Potentially address" – if this was a consumer address is it correct to be non-personal data?

Link and Card Payments:

- Cardholder PIN and CVC code, is this personal data, do these details identify an individual? They authenticate the individual. They help to confirm that someone is who they say they are, but can they be used to find out who they are?

Additional comments:

4.48b "While it is unlikely that this data in isolation could identify the customer, or impact the security of future transactions, it is worth noting that if this data is used in combination with other sources of data or viewed in the aggregate level, it could reveal private information about a cardholder's movements or habits"

Today the location of the merchant is considered an identity and fraud indicator, for example, a card payment or cash withdrawal can be stopped if the location is not a typical behaviour; such as using a card on holiday.

Section 4.

Section 4 considers the data available within the current payment systems; in the new payments world, of ISO20022 and open banking /PSD2. Should we consider the potential impact of new overlay services, and the scope for additional data that this presents? The later sections of this paper discuss new opportunities for the use of payments data but do not identify any specific additional data, nor address whether that data should be subject to whatever recommendations come out of the exercise.

2. *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?*

Analysis and Insight on the data help shape and develop applications. Applications can then be used to help improve and correct issues within the data, the cycle starts again. (Ref Figure 6: Value chain of payments data)

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

Errors: are we assuming any data within payments is correct and has already been checked for human error? Could payment data help remove errors before they enter the payment systems?

Identity: Payments data could help PSPs and corporate with Identity and KYC checking. For example, knowing account or transactional behaviour could be used to help check the identity of a consumer.

Affordability: Payments data could help provide informed decisions on a consumer's ability to repay a debt before it is accepted.

End-user willingness to share data

4. *Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?*

Consumer trust is key to the success of delivering any enhanced data. Consumers have been advised not to share personal and bank data with anyone, therefore a mind shift and education needs to take place. This will be built up on trust over a period, as consumers understand and can see the benefit to them of sharing data, more value will be derived.

In terms of addressing this, firstly accreditation should be considered for any provider who has access to data. This accredited list should be publicised with links to industry regulators such as the PSR and possibly the FCA. Consumer can see and understand what accreditation means building trust.

Another possibility would be to develop a central guarantee system, comparable to the Direct Debit guarantee. Consumers had the confidence to begin using Direct Debit because they knew that if anything did go wrong they would be protected under the guarantee system. Although developing a guarantee system could be difficult, it would offer the consumer reassurances that their data will only be used for the agreed permitted purposes. Any use outside of the agreed purposes could lead to reimbursement or compensation for the consumer.

Access to global datasets

5. *In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits*?

If not, why?

Yes, we agree that data held in a central repository / infrastructure would allow accredited organisations to develop overlay services. Overlay service could include Identity checking, fraud prevention and detection, affordability services, insurance scam detection, helping consumers to manage their budgets - for example warning of direct debits due. All these services could help PSPs, corporates and consumers make better informed decisions.

6. *What models could the NPSO introduce to allow PSPs to get access to global datasets?*

Why would only PSPs get access to the global dataset?

Access to the data should be granted via central accreditation. Use cases for the data should be defined centrally, such as Fraud, AML and KYC. Each use case may have a slightly different cut of the data which can be used for that permitted purpose only. The accreditation could then also be linked to use cases and access.

If new use cases or access to the data is required, this would be requested centrally for review. If approved, the new use cases and data and accreditation rules would be centrally created and made the data made available to appropriately accredited users.

7. *Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction* data?

Yes, all data should be included and available for access by accredited organisations. Silos of unshared payments data prevent fraud protection being applied consistently across the payments landscape.

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

8*. 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*?

With the development of pre-defined use cases, accredited companies need to ensure they have valid grounds to process any personal data they access as a result. Data protection compliance could then be managed for each use case and not free form access to the data. For example, a consumer may already have in their current T&Cs with a PSP, appropriate notification that their data will be shared with third parties for fraud prevention purposes.

Realising the benefits of enhanced data

9. Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

Cost and time to implement the new regimes form a barrier to any new development, particularly when the benefit of change depends on data completeness. Essentially corporates and retailers in addition to PSPs will be asked to put additional data into payments. This will require change to existing systems, including gathering new data for historic records. This enhanced data may be of great value, but the immediate value is to the recipients of the data rather than the suppliers of it. And even then only when they have made the investment to make use of it. For all parties, the real benefits of any new system only accrue once everybody is consistently providing the new data. Until then everyone has to rely at least in part on their old strategies. The ROI on such changes are unlikely to make them good candidates for investment. What regulations or rules would be mandated to ensure the enhanced data is populated and complete?

Other payments data-related issues

10. Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

PSPs willingness to share data. Commercial and cost implications of building storage for the data and then sharing. Could it be considered they are giving data away for free for other companies to charge for, even back to the originating PSPs?

Fidelity Information Services (FIS)

Further to my comments on your paper which I made when you presented at the PSR Panel, I wanted to give a little more feedback on your paper titled 'Data in the payments industry'.

4.6 a. End user willingness to share data. (PSR Panel 2 page paper)

Per my comments in the Panel session, the data falls into four broad chunks from a legal basis of processing point of view in my opinion. End users should in my opinion expect 1-3 below to happen, and need to consent for 4.:

1. Data that is required for the transaction to execute (sort code, account number, value etc)
2. Extended data that is required for the execution of a contract (invoice number, invoice detail, other extended information about the contract the payment relates to)
3. Data which isn't required for 1. Or 2. but would be very useful for fraud analytics (IP address, cell tower ID, phone GPS, etc etc etc). In my mind, if this kind of data is collected for the purpose of Fraud screening/trending/analysis, and for that purpose only I would argue Legitimate Interest according to GDPR:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
I would suggest that such data could be stored centrally somewhere, and registered/regulated entities could develop overlay services to consume this data for the purpose of fraud screening/analysis only. This would create a competitive marketplace and value to all participants.
4. Data which may be required for 1.2.3. above but which is being used for another purpose e.g. credit scoring, marketing other processing. In these cases explicit consent from a consumer would be required for the activity being undertaken. Again, the same dataset could be stored centrally, registered/regulated entities could develop overlay services to consume this data for those consumers (data subjects) they have explicit consent from.

Questions in the main paper

1. Do you agree with our assessment of
    a. Types of data relevant
    Yes
    b. Types of data collected
    Yes – but I would add that in the cards industry extra data is also collected in some cases. This is typically for use cases such as fuel cards, and T&E transactions e.g. hotels and may include vehicle registration, mileage, or information about the hotel. These cards can be open or closed loop.
    c. Different ways of classifying
    Yes – but I would add per my notes above that classifying based on usage according legal basis for processing according to GDPR may also be very useful.

3. Have we accurately described…..

I would add that payment firms also use data for

- Onboarding new customers
- Credit scoring
- Finding 'life events' and using them e.g. inferring someone has had a baby as they are shopping at (for example) Mothercare, then sending relevant offers.

4. Do you agree that the mismatch….

It may do, but equally new brands have managed very well to get more data than banks and other FIs hold on consumers and monetise that data without any brand pedigree. Take any social media platform as an example. The key is a fair exchange of value. Consumers are willing to share their personal data if they get something in return. Making that attractive to them is the key – Clearscore would be a good example.

5. In the new payments architecture….

Yes completely agree with that. The only restricting factor is imagination. Obvious examples are around fraud, transaction analytics, enriching other datasets (e.g. social media)

6. What models…..

I would suggest that entities wishing to access such data should have to be registered in some way, and also state for what purpose(s) they plan to use any data. It will then be clear what the legal basis for processing is according to GDPR and therefore how they may be able to access that data. For example, a company finding fraud given a global dataset should be able to use all data under a 'legitimate interest' basis as it is in the interests of both the data subject who has been defrauded, and also other data subjects who (one hopes) would not be defrauded because of the analysis done. I would add that as a result of this, digital rights management will become very important i.e. who can do what with who's data on what legal basis.

7. Should PSOs….

Yes.

8. Is there tension..

As I've mentioned above, I would argue that AML is either 'Legal obligation' according to GDPR under laws a such as MLD4 or if not, then Legitimate Interest. So as long as data is being used for that, and nothing else then that is ok. Technically to manage this correctly, for the central dataset, or subsets of the central dataset, data users would have to establish a legal basis for processing that dataset either as a whole, or for certain data subjects. Consent would only need to be collected in the event that it was being used as the legal basis for processing which in some cases it wouldn't be.

The whole area of digital rights management is an area which I have some knowledge of. I would be happy to have a follow up to discuss how some of these things can be achieved technically should that be useful.

Kind regards,

[redacted]

[redacted]

[redacted].

HSBC Bank PLC

HSBC BANK PLC

PAYMENT SYSTEMS REGULATOR DISCUSSION PAPER DP18/1: DATA IN THE PAYMENTS INDUSTRY

RESPONSE TO DISCUSSION PAPER

3 SEPTEMBER 2018

---

1. Introduction and General Observations

1.1. Following the establishment of the HSBC Group UK retail bank HSBC UK Bank plc on 1 July 2018, HSBC Bank plc is now the non-ring-fenced bank within the Group. HSBC Bank plc customers in the UK include our Global Banking & Markets customers within our wholesale and investment banking division, relevant Financial Institutions, UK Corporate Banking customers and customers of non-UK branches of HSBC Bank plc.

1.2. HSBC welcomes the opportunity to respond to the Payment System Regulator's (the PSR) discussion paper: Data in the Payments Industry.

1.3. HSBC agrees with the PSR that data is an increasingly important part of the UK payments industry. We recognise that the UK payments sector is fast evolving and that data will have a key role in this evolution, and agree with the variety of market, technological, end user and regulatory drivers of change identified by the PSR.

1.4. HSBC supports the PSR in its effort to consider data in the context of their own objectives relating to the opportunities and risks of the changing treatment of data in the payments industry. Our view is that the market is currently undergoing a radical transformation. Some drivers of this transformation are newly live (such as Open Banking and the second Payment Services Directive (PSD2)) whilst others are being prepared for (e.g. the New Payments Architecture (NPA) and industry migration to ISO 20022). Together these changes will open up access to data, bring new players and services with data-driven business models to the market and enable existing payment systems to carry increased volumes, types and complexity of data.

1.5. Given the above, we would support a period of market monitoring to understand how users, and the market more widely, is responding to developments. We suggest the PSR might consider commissioning research to track end user attitudes and to explore how users are reacting to change. For example, this could include engagement with corporates to understand how they are responding to the availability of Enhanced Data (once it is in place), as there is likely to be a period of low take up whilst corporates mobilise their own internal change programmes to use the new functionality. This will enable the PSR to be led by emerging user challenges and requirements.

1.6. Whilst the industry is in this phase of transformation, HSBC believes it is premature for the PSR to implement further regulatory policies or actions and that letting the market develop would not put the PSR statutory objectives at risk. We recognise the issues that the PSR has identified and share concerns, particularly in relation to realising the benefits of Confirmation of Payee, Request to Pay and Enhanced Data, but recommend that the market is allowed to establish itself and respond to customer dynamics.

1.7. Furthermore, we note the sheer volume and complexity of change underway in the industry at present. The regulatory and technological change landscape is complex, interconnected and demanding for Payment Service Providers (PSPs), technology service providers, infrastructure providers, Payment System Operators (PSOs) and, not least, customers. A number of major change programmes have data at their heart, including, but not limited to, the roll out of PSD2 and Open Banking, the Real Time Gross Settlement renewal and implementation of ISO 20022, the NPA as well as implementing Confirmation of Payee, Request to Pay and Enhanced Data.

Further regulatory intervention would touch all of these initiatives and potentially slow the delivery of change.

1.8. In addition to the themes set out in the discussion paper, we believe that cyber security and cyber resilience require careful consideration. The increased use of data and new technologies means new and innovative threats arising from cybercrime (both financial and/or hostile state group) or an IT failure in an owner of data. Threats to data are constantly evolving and ever-present.

1.9. Likewise, the impact of data breaches, both financial and wider, needs to be considered. Media stories about such breaches are influencing customer behaviour and attitudes towards sharing data that in turn, impacts the potential benefits of data sharing in the payments space. One example is the recent coverage around Facebook and Cambridge Analytica. Any market research as described in 1.5 needs to evaluate customer's attitudes and concerns relating to data security.

1.10. Although the discussion paper notes (2.11) that there are a range of regulatory bodies with oversight of the collection and use of data in the UK payments sector, we suggest that the Bank of England (BoE) has a role given that a substantial data breach or failure would be a real risk to the stability and integrity of UK payments.

1.11. More broadly, any action that the PSR is minded to take must be a cross-regulatory approach cognisant of other regulatory frameworks that such PSR action would interact with. We recognise the paper sets out a clear awareness of this factor, particularly in relation to the Information Commissioner's Office (ICO), but it is imperative that others including the Competition & Markets Authority (CMA), the Prudential Regulatory Authority (PRA), BoE, Financial Conduct Authority (FCA), HM Treasury (HMT) and others are involved to ensure a joined-up, end-to-end framework. There may also be a need to take account of non-European legislation given that PSOs, service providers, PSPs and commercial customers may process data outside the European Economic Area.

1.12. The PSR is correct to identify that customers have a greater level of trust for established players compared to new entrants and this has indeed been the finding of a number of research studies. However, we believe this will evolve as the market matures and the presence of trusted players may well support rather than hinder the take up of services by customers, and ultimately the development of the market beyond established players. This is again impacted by the risk of, and actual incidences of, data breaches.

1.13. The PSR proposals also suggest access to 'global transaction datasets.' HSBC agrees that there is significant potential benefit in areas such as fraud protection and Anti Money Laundering (AML), as demonstrated in the Payment Strategy Forum (PSF) work on transaction data analytic solutions for fraud and financial crime prevention purposes. However, the PSR will appreciate that any data sharing needs to be a) secure and b) has to have the appropriate legal justification (e.g. consent, legitimate interests, etc.) in place from individuals regarding the sharing of their data (and also respect the duty of confidentiality and banking secrecy obligations for commercial customers) which therefore requires an effective legislative framework and change. More work is needed to define when such data sharing is appropriate and agree the controls/standards that will need to be in place.

2. Responses to discussion paper questions

Q1. Do you agree with our assessment of:
a. the types of data in the payments industry that are relevant for this paper?
b. the types of data collected by different entities in the industry?
c. the different ways that payments data can be classified?

2.1. HSBC broadly agrees with the assessment and classification of data. However, we have a number of observations in response to Q1. For example, this assessment doesn't look at Third Party Payment Service Providers' (TPP) data sitting over some of these payment systems. Some may be large organisations or have other data sets available to combine.

2.2. We note that the term "global datasets" is defined as a dataset that combines all the data within a payment system. However the term could be construed as impacting non-UK payments which would have a substantial impact as non-UK data legislation would have to be considered. We recommend the term "UK payment scheme dataset."

2.3. The Faster Payments summary should note that many payments require a one-time password (two-factor authentication) to enable a payment.

2.4. The Card Payments section should note the use of 3DS (Verified by Visa / SecureCode) in initiating card-not-present on-line payments.

2.5. HSBC agrees that some data collection is at an aggregated level, but this does not remove the need to consider whether such sharing would be permissible under data privacy laws and whether customers would expect their data to be shared in such a manner. Such data sharing may need to be included within customer documentation such as terms and conditions or data privacy notices, and there needs to be careful consideration as to whether customer consent is required for both legal and transparency reasons and how such consent would practically be obtained and maintained.

2.6. For completeness, it should also be stated that sponsoring banks submit data to payment systems on behalf of agency banks and therefore the data flows for the systems described may be more complex than presented, with agency bank customer data passing via a sponsoring bank before entering the payment system.

Q2. 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?

Q3. Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

2.7. Taking these questions together, we broadly agree with the assessment of different points in the value chain where data can be used for generating benefits for payment system participants. However it should not be assumed that all PSPs are utilising their data in this way, nor exploring its potential. To do so requires significant technological resource and business investment.

Q4. Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

2.8. The PSR is correct to identify that customers have a greater level of trust for established players compared to new entrants as shown in the research cited in the discussion paper. In addition, this has indeed been the finding of a number of research studies on Open Banking (F. Reynolds, 2017; Accenture, 2018; Ipsos MORI, 2018). However, trust levels vary across demographics and are likely to evolve as new entrants gain profile and support from their growing customer base.

2.9. Education and information provision has a supporting role in informing the customer of new services and the benefits of data sharing. However, the impact of this may be limited by the wider environment of concerns relating to data security and data breaches.

2.10. Historically, consumer behaviour has been slow to change in payments (e.g. online banking, contactless card payments) but once consumers recognise the tangible benefit of the service to their own financial management and see others using it successfully, behaviour can change quickly. The research studies cited above, point to the importance of this in the context of Open Banking specifically, suggesting that adoption will be driven by the relevance of the propositions that allow customers to see the benefits outweigh their reservations in data sharing.

2.11. Some new entrants to the market are expected to be established brands from outside the financial services sector which will already have consumer confidence. Likewise, partnerships between new entrants and well-known brands (either within or outside financial services such as retailers) will give scale to new entrants.

2.12. Importantly, established players may provide the trusted environment for consumers to try out the new types of services available and build their understanding, confidence and interest, leading to greater willingness to try out services from other providers. In short, established players may be an important enabler for new players. This is similar to how Transport for London provided a clear use case and trusted environment for consumers to trial contactless functionality on their cards. Likewise, as innovators and FinTechs see the market and consumer appetite grow with established player offerings, it may stimulate new offerings.

2.13. Ultimately, the trust of consumers is gained by seeing a service working well for others, robust security of data and seeing disputes / problems fixed quickly and easily. It is therefore important that both existing players in the banking sector and new entrants are subject to the same levels of regulatory oversight in relation to new data-based services.

2.14. The impact of cybercrime and/or system failures and frequent media stories relating to data breaches (whether including payments data or non-payments data) should also be taken into account by the PSR. Market research during the implementation of Paym highlighted that customers had concerns relating to data security.

Q5. In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?
Q6. What models could the NPSO introduce to allow PSPs to get access to global datasets?
Q7. Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?
Q8. 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?

2.15. As noted above, we recommend the term "UK payment scheme dataset" to avoid confusion. Taking Q5 to Q8 together, the provision of access to global transaction data by regulated PSOs in order to enable innovation that addresses a customer detriment or improves the integrity of the payment systems, is, in principle, a positive development. However, in our view this should not be an open access provision and consideration will be needed on a case-by-case basis determined by the merits and benefits to end users. Given the scale, sensitivity and richness of payment transaction data sets, the use of such datasets should only be for the development of services that will deliver clear benefits for users and therefore enhance the integrity of payment services. Access should not be given for marketing or commercial purposes.

2.16. Such a bespoke model requires strong governance and standards. Parameters will be required to define under what circumstances such access may be granted, in what format, and the standards (such as technology and security) that would need to be met for utilising the data as well as an assurance process that such standards are being met and that usage complies with any relevant data or other financial services legislation or regulation. Any transfer of data must not diminish the security under which data is held. Questions such as whether access should be restricted to PSPs and UK-only entities need consideration as well as whether data analytics to support marketing and / or commercial services is appropriate.

2.17. There clearly is a tension between the potential innovation that access to such transaction data sets may bring and data protection and other legal requirements, especially given the introduction of the GDPR. Even at an aggregate level, data may be commercially sensitive (for example if it indicates market shares), or if combined with other data sets, may be possible to identify individuals. This means access without proper safeguards could give rise to confidentiality or competition law issues, or it may provide inferential data analysis opportunities that can link back to personal data sets. All data must of course be held to the maximum security. A governance body to oversee such applications and a sandbox environment may be the most appropriate way to manage such activity in order to alleviate potential concerns and ensure appropriate standards are adhered and controlled.

2.18. Balancing the benefits of data sharing with the need to respect data protection and other legal obligations is likely to require a joint approach between the different regulators and central government, perhaps seeking derogations from GDPR and other data protection legislation. Indeed, the PSF strategic solution on transactional data sharing for the purposes of detecting and preventing all types of financial crime has identified the need for legislative change if data is to be utilised for this purpose and is working with the Home Office's Joint Fraud Taskforce.

2.19. We have not commented on the technical requirements and consent processes as this is complex and will depend on the nature of the data required and purpose of use. We note though that, in circumstances where consent may be required for the processing of personal data, the GDPR introduces strict requirements in respect of these and in other areas, such as the use of personal data for marketing or further, incompatible commercial purposes. Even where consent might not be required, and reliance on another processing condition under the GDPR is appropriate, factors such as how such further use of data is communicated to individuals in a compliant and appropriate manner must also be borne in mind.

Q9. Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

2.20. Not that we have identified.

Q10. Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

2.21. The increased use of data means is a continuing threats from cybercrime (both financial and/or hostile state group) and an IT failure in an owner of data. It appears that this is a threat that is likely to be evolving and ever-present.

2.22. As mentioned in the introduction, the impact of actual data breaches, both financial and wider, needs to be considered. Media stories about such breaches (even if not directly payments related) are impacting on customer behaviour and attitudes towards sharing data that impacts the potential benefits of data sharing in the payments space.

2.23. Finally, it should be recognised that the growth of data driven payment services is likely to increase the load and velocity in payment systems, which could have system resilience implications.

HSBC UK

HSBC UK BANK PLC

PAYMENT SYSTEMS REGULATOR DISCUSSION PAPER DP18/1: DATA IN THE PAYMENTS INDUSTRY

RESPONSE TO DISCUSSION PAPER

3 SEPTEMBER 2018

---

1. Introduction and General Observations

1.1. HSBC UK Bank plc (HSBC UK) is the new UK ring-fenced retail bank within the HSBC Group, which opened on 1 July 2018. Our customers include HSBC personal and commercial customers in the UK, including those UK Business Banking customers categorised as Non-Bank Financial Institutions, UK Private Bank clients and our other UK retail brands, M&S Bank and first direct.

1.2. HSBC UK welcomes the opportunity to respond to the Payment System Regulator's (the PSR) discussion paper: Data in the Payments Industry.

1.3. HSBC UK agrees with the PSR that data is an increasingly important part of the UK payments industry. We recognise that the UK payments sector is fast evolving and that data will have a key role in this evolution, and agree with the variety of market, technological, end user and regulatory drivers of change identified by the PSR.

1.4. HSBC UK supports the PSR in its effort to consider data in the context of their own objectives relating to the opportunities and risks of the changing treatment of data in the payments industry. Our view is that the market is currently undergoing a radical transformation. Some drivers of this transformation are newly live (such as Open Banking and the second Payment Services Directive (PSD2)) whilst others are being prepared for (e.g. the New Payments Architecture (NPA) and industry migration to ISO 20022). Together these changes will open up access to data, bring new players and services with data-driven business models to the market and enable existing payment systems to carry increased volumes, types and complexity of data.

1.5. Given the above, we would support a period of market monitoring to understand how users, and the market more widely, is responding to developments. We suggest the PSR might consider commissioning research to track end user attitudes and to explore how users are reacting to change. For example, this could include engagement with corporates to understand how they are responding to the availability of Enhanced Data (once it is in place), as there is likely to be a period of low take up whilst corporates mobilise their own internal change programmes to use the new functionality. This will enable the PSR to be led by emerging user challenges and requirements.

1.6. Whilst the industry is in this phase of transformation, HSBC UK believes it is premature for the PSR to implement further regulatory policies or actions and that letting the market develop would not put the PSR statutory objectives at risk. We recognise the issues that the PSR has identified and share concerns, particularly in relation to realising the benefits of Confirmation of Payee, Request to Pay and Enhanced Data, but recommend that the market is allowed to establish itself and respond to customer dynamics.

1.7. Furthermore, we note the sheer volume and complexity of change underway in the industry at present. The regulatory and technological change landscape is complex, interconnected and demanding for Payment Service Providers (PSPs), technology service providers, infrastructure providers, Payment System Operators (PSOs) and, not least, customers. A number of major change programmes have data at their heart, including, but not limited to, the roll out of PSD2 and Open Banking, the Real Time Gross Settlement renewal and implementation of ISO 20022, the NPA as well as implementing Confirmation of Payee, Request to Pay and Enhanced Data.

Further regulatory intervention would touch all of these initiatives and potentially slow the delivery of change.

1.8. In addition to the themes set out in the discussion paper, we believe that cyber security and cyber resilience require careful consideration. The increased use of data and new technologies means new and innovative threats arising from cybercrime (both financial and/or hostile state group) or an IT failure in an owner of data. Threats to data are constantly evolving and ever-present.

1.9. Likewise, the impact of data breaches, both financial and wider, needs to be considered. Media stories about such breaches are influencing customer behaviour and attitudes towards sharing data that in turn, impacts the potential benefits of data sharing in the payments space. One example is the recent coverage around Facebook and Cambridge Analytica. Any market research as described in 1.5 needs to evaluate customer's attitudes and concerns relating to data security.

1.10. Although the discussion paper notes (2.11) that there are a range of regulatory bodies with oversight of the collection and use of data in the UK payments sector, we suggest that the Bank of England (BoE) has a role given that a substantial data breach or failure would be a real risk to the stability and integrity of UK payments.

1.11. More broadly, any action that the PSR is minded to take must be a cross-regulatory approach cognisant of other regulatory frameworks that such PSR action would interact with. We recognise the paper sets out a clear awareness of this factor, particularly in relation to the Information Commissioner's Office (ICO), but it is imperative that others including the Competition & Markets Authority (CMA), the Prudential Regulatory Authority (PRA), BoE, Financial Conduct Authority (FCA), HM Treasury (HMT) and others are involved to ensure a joined-up, end-to-end framework. There may also be a need to take account of non-European legislation given that PSOs, service providers, PSPs and commercial customers may process data outside the European Economic Area.

1.12. The PSR is correct to identify that customers have a greater level of trust for established players compared to new entrants and this has indeed been the finding of a number of research studies. However, we believe this will evolve as the market matures and the presence of trusted players may well support rather than hinder the take up of services by customers, and ultimately the development of the market beyond established players. This is again impacted by the risk of, and actual incidences of, data breaches.

1.13. The PSR proposals also suggest access to 'global transaction datasets.' HSBC UK agrees that there is significant potential benefit in areas such as fraud protection and Anti Money Laundering (AML), as demonstrated in the Payment Strategy Forum (PSF) work on transaction data analytic solutions for fraud and financial crime prevention purposes. However, the PSR will appreciate that any data sharing needs to be a) secure and b) has to have the appropriate legal justification (e.g. consent, legitimate interests, etc.) in place from individuals regarding the sharing of their data (and also respect the duty of confidentiality and banking secrecy obligations for commercial customers) which therefore requires an effective legislative framework and change. More work is needed to define when such data sharing is appropriate and agree the controls/standards that will need to be in place.

2. Responses to discussion paper questions

Q1. Do you agree with our assessment of:
a. the types of data in the payments industry that are relevant for this paper?
b. the types of data collected by different entities in the industry?
c. the different ways that payments data can be classified?

2.1. HSBC UK broadly agrees with the assessment and classification of data. However, we have a number of observations in response to Q1. For example, this assessment doesn't look at Third Party Payment Service Providers' (TPP) data sitting over some of these payment systems. Some may be large organisations or have other data sets available to combine.

2.2. We note that the term "global datasets" is defined as a dataset that combines all the data within a payment system. However the term could be construed as impacting non-UK payments which would have a substantial impact as non-UK data legislation would have to be considered. We recommend the term "UK payment scheme dataset."

2.3. The Faster Payments summary should note that many payments require a one-time password (two-factor authentication) to enable a payment.

2.4. The Card Payments section should note the use of 3DS (Verified by Visa / SecureCode) in initiating card-not-present on-line payments.

2.5. HSBC UK agrees that some data collection is at an aggregated level, but this does not remove the need to consider whether such sharing would be permissible under data privacy laws and whether customers would expect their data to be shared in such a manner. Such data sharing may need to be included within customer documentation such as terms and conditions or data privacy notices, and there needs to be careful consideration as to whether customer consent is required for both legal and transparency reasons and how such consent would practically be obtained and maintained.

Q2. 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?

Q3. Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

2.6. Taking these questions together, we broadly agree with the assessment of different points in the value chain where data can be used for generating benefits for payment system participants. However it should not be assumed that all PSPs are utilising their data in this way, nor exploring its potential. To do so requires significant technological resource and business investment.

Q4. Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

2.7. The PSR is correct to identify that customers have a greater level of trust for established players compared to new entrants as shown in the research cited in the discussion paper. In addition, this has indeed been the finding of a number of research studies on Open Banking (F. Reynolds, 2017; Accenture, 2018; Ipsos MORI, 2018). However, trust levels vary across demographics and are likely to evolve as new entrants gain profile and support from their growing customer base.

2.8. Education and information provision has a supporting role in informing the customer of new services and the benefits of data sharing. However, the impact of this may be limited by the wider environment of concerns relating to data security and data breaches.

2.9. Historically, consumer behaviour has been slow to change in payments (e.g. online banking, contactless card payments) but once consumers recognise the tangible benefit of the service to their own financial management and see others using it successfully, behaviour can change quickly. The research studies cited above, point to the importance of this in the context of Open Banking specifically, suggesting that adoption will be driven by the relevance of the propositions that allow customers to see the benefits outweigh their reservations in data sharing.

2.10. Some new entrants to the market are expected to be established brands from outside the financial services sector which will already have consumer confidence. Likewise, partnerships between new entrants and well-known brands (either within or outside financial services such as retailers) will give scale to new entrants.

2.11. Importantly, established players may provide the trusted environment for consumers to try out the new types of services available and build their understanding, confidence and interest, leading to greater willingness to try out services from other providers. In short, established players may be an important enabler for new players. This is similar to how Transport for London provided a clear use case and trusted environment for consumers to trial contactless functionality on their cards. Likewise, as innovators and FinTechs see the market and consumer appetite grow with established player offerings, it may stimulate new offerings.

2.12. Ultimately, the trust of consumers is gained by seeing a service working well for others, robust security of data and seeing disputes / problems fixed quickly and easily. It is therefore important that both existing players in the banking sector and new entrants are subject to the same levels of regulatory oversight in relation to new data-based services.

2.13. The impact of cybercrime and/or system failures and frequent media stories relating to data breaches (whether including payments data or non-payments data) should also be taken into account by the PSR. Market research during the implementation of Paym highlighted that customers had concerns relating to data security.

Q5. In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?
Q6. What models could the NPSO introduce to allow PSPs to get access to global datasets?
Q7. Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?
Q8. 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?

2.14. As noted above, we recommend the term "UK payment scheme dataset" to avoid confusion. Taking Q5 to Q8 together, the provision of access to global transaction data by regulated PSOs in order to enable innovation that addresses a customer detriment or improves the integrity of the payment systems, is, in principle, a positive development. However, in our view this should not be an open access provision and consideration will be needed on a case-by-case basis determined by the merits and benefits to end users. Given the scale, sensitivity and richness of payment transaction data sets, the use of such datasets should only be for the development of services that will deliver clear benefits for users and therefore enhance the integrity of payment services. Access should not be given for marketing or commercial purposes.

2.15. Such a bespoke model requires strong governance and standards. Parameters will be required to define under what circumstances such access may be granted, in what format, and the standards (such as technology and security) that would need to be met for utilising the data as well as an assurance process that such standards are being met and that usage complies with any relevant data or other financial services legislation or regulation. Any transfer of data must not diminish the security under which data is held. Questions such as whether access should be restricted to PSPs and UK-only entities need consideration as well as whether data analytics to support marketing and / or commercial services is appropriate.

2.16. There clearly is a tension between the potential innovation that access to such transaction data sets may bring and data protection and other legal requirements, especially given the introduction of the GDPR. Even at an aggregate level, data may be commercially sensitive (for example if it indicates market shares), or if combined with other data sets, may be possible to identify individuals. This means access without proper safeguards could give rise to confidentiality or competition law issues, or it may provide inferential data analysis opportunities that can link back to personal data sets. All data must of course be held to the maximum security. A governance body to oversee such applications and a sandbox environment may be the most appropriate way to manage such activity in order to alleviate potential concerns and ensure appropriate standards are adhered and controlled.

2.17. Balancing the benefits of data sharing with the need to respect data protection and other legal obligations is likely to require a joint approach between the different regulators and central government, perhaps seeking derogations from GDPR and other data protection legislation. Indeed, the PSF strategic solution on transactional data sharing for the purposes of detecting and preventing all types of financial crime has identified the need for legislative change if data is to be utilised for this purpose and is working with the Home Office's Joint Fraud Taskforce.

2.18. We have not commented on the technical requirements and consent processes as this is complex and will depend on the nature of the data required and purpose of use. We note though that, in circumstances where consent may be required for the processing of personal data, the GDPR introduces strict requirements in respect of these and in other areas, such as the use of personal data for marketing or further, incompatible commercial purposes. Even where consent might not be required, and reliance on another processing condition under the GDPR is appropriate, factors such as how such further use of data is communicated to individuals in a compliant and appropriate manner must also be borne in mind.

Q9. Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

2.19. Not that we have identified.

Q10. Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

2.20. The increased use of data means there is a continuing threats from cybercrime (both financial and/or hostile state group) and an IT failure in an owner of data. It appears that this is a threat that is likely to be evolving and ever-present.

2.21. As mentioned in the introduction, the impact of actual data breaches, both financial and wider, needs to be considered. Media stories about such breaches (even if not directly payments related) are impacting on customer behaviour and attitudes towards sharing data that impacts the potential benefits of data sharing in the payments space.

2.22. Finally, it should be recognised that the growth of data driven payment services is likely to increase the load and velocity in payment systems, which could have system resilience implications.

Lloyds Banking Group (LBG)

LLOYDS BANKING GROUP PLC

Data in the Payments Industry

Submission Date 03/09/2018

Executive Summary

Lloyds Banking Group (LBG) welcomes the opportunity to respond to the PSR's discussion paper and to contribute to the dialogue regarding the future of data in the payments industry.

We agree that data is an increasingly important component of the UK payments ecosystem. When used in the right way, data has the potential to deliver real customer benefits through innovative new services and propositions that enhance the customer experience, allow customers to better manage their finances and develop improved tools to combat fraud. Nevertheless, data also has the potential to cause significant consumer harm where it is either used incorrectly or is not adequately protected against falling into the wrong hands; for example, recent high profile data breaches.

Initiatives such as the revised Payment Services Directive (PSD2), the General Data Protection Regulation (GDPR) and the delivery of Open Banking in the UK have all brought data and the opportunities and risks inherent in the sharing of data to the forefront of the regulatory agenda. We support the PSR's desire to better understand how data may impact their objectives. We do however recognise that given the importance of data, more than one regulator is interested in or has oversight of how the market develops. It is therefore important for both market participants and end consumers that the role of each regulator is clear. We recognise the need for careful regulatory oversight to prevent consumer harm but this should be carefully balanced to also allow for competition and innovation to thrive in order to deliver real consumer benefit.

The PSR can play a role in supporting this so that new services deliver benefits to customers whilst ensuring that critical services remain safe and secure. Specifically, **the PSR should ensure that the regulatory framework supports the payment system operators (PSO's) and card payment schemes ability to share the data collected over the central infrastructure with authorised third parties**. Additionally, the PSR should take a leading role in ensuring each party has a clear understanding of their rights and responsibilities.

We also believe that there is a role for the PSR in clearly defining what constitutes payments and personal data. Whilst we broadly support the assessment of the data classification types, we think this will be crucial should it be used in any future regulatory text.

Many of the initiatives linked to customer data and data sharing are relatively new to the UK and still require time to bed down. The payments industry is also undergoing an unprecedented level of change. This is recognised in the PSR 2018/19 annual report where the PSR acknowledges they have "*shaken up the market and driven landmark changes in a number of areas across the payments sector over the last 12 months*" with several major initiatives in flight to be delivered over the next three years. Whilst we note the PSR's stated commitment to further explore payments data, we think that the recent comments by the chairman of the Financial Conduct Authority (FCA), calling for a period of stability after coping with the implications of Brexit before any major changes to the regulatory structure are considered, is wise counsel.

The PSR can be an enabler to support the adoption of data services by end-users. LBG was supportive of the PSR Market Review of Infrastructure remedy to move to a common international standard. Migration to ISO20022 will allow for enhanced reference data that enables increased amounts of remittance information to be linked or added to a payment instruction in a structured and standard format

We envisage that **the role of the PSR should be to facilitate evaluation of the marketplace once appropriate time has passed for initiatives to embed and allow for the proposed new services to develop.**

The development of the New Payments Architecture and new services such as Confirmation of Payee and Enhanced Data will naturally increase the data that is available. It is important to help end-users to adopt and make the necessary investments to benefit from this additional data (e.g. Corporates) to ensure the benefits are realised.

Medium and Large Corporates typically have integrated, automated electronic reporting and treasury management solutions, so significant investment may be required for them to both submit payments using IS020022, but also process and leverage the increased amount of data (for example payment receipts). This cost and investment cycles should not be underestimated and therefore it is important that consideration is given to the time that it may take to realise benefits as investment cycles catch up with the Industry changes.

Recent market intelligence suggests that the majority of consumers have little or no understanding of Open Banking. **Clear and simple customer education is key to help deliver consistent messaging across the market to ensure that customers understand how their data is being used and what they are giving their permission for**, so that any risks are clearly understood.

Furthermore, whilst we recognise the PSR's concerns, we believe that recent regulatory changes will naturally promote competition and innovation and that there is no clear evidence that requires further regulatory intervention at this time.

The PSR should continue to work closely with UK Finance and the regulatory authorities, not only to avoid potential duplication in oversight, but to ensure better sequencing of initiatives and coordination across the regulatory landscape.

Response to Consultation Questions

1. DO YOU AGREE WITH OUR ASSESSMENT OF;

(a) **The types of data in the payments industry that are relevant to this paper?**

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

(c) **The different ways that payments data can be classified?**

1.1 Broadly, we agree that the types of payment data outlined in the discussion paper as a mix of financial, transactional, behavioural and other types of data, which PSP's and other entities collect in the process of providing payment services to end-users, appears reasonable. However, we believe the PSR definition is too broad in suggesting that payments data includes, but is not limited to, the totality of the information collected by PSP's and other third-party providers in the process of providing core payment services to end-users. We would therefore add a caveat that 'payments data collected in providing core payments services' is limited only to that data which is necessary to securely initiate and complete a payment transaction, i.e. the core payment service which will be provided through the NPA. With this in mind, it is also important to ensure that the PSR works closely with the NPSO as they finalise the summary position of types of data as well as how it's collected and classified.

1.2 A clear and precise definition of what constitutes payments data is important should it be used in any future regulatory text. For example; a Payment Service Provider (PSP) may collect data in the course of providing a core transaction which is superfluous to the secure initiation and completion of the payment. That this data is collected as part of a core payment transaction does not in itself qualify it as payments data.

1.3 Conversely, we suggest that care should be taken with proposals to include any data in a payment message that is not considered necessary for the processing of a payment as it may complicate the legal grounds for processing under General Data Protection Regulation (EU) 2016/679 (GDPR), particularly when that message is passed from one party to another.

1.4 Having reviewed the PSR's assessment of data classification we consider that further clarification may be helpful and avoids misinterpretation.

1.5 The classification of personal data appears to be over simplified as it implies that payment data is personal data only if it serves to identify an individual party involved in the payment transaction. However, any data that can be related or linked to an identifiable individual is potentially personal data and we therefore suggest that the PSR revise their definition.

1.6 For example; the Bacs interbank data flow classifies the date and amount of a transaction as non-personal data. However, in the context of a Bacs message, where this data is combined with other data that identifies an individual, it may be more appropriate for it to be classified as personal data, i.e. to classify the total data contained with a single payment message as personal data rather than seek to break it down into different classifications. Similarly, enhanced data within the proposed new credit message may mean that the combination of a number of data points automatically makes it personally identifiable.

2. 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?

2.1 LBG agrees with the PSR's assessment of the different points in the value chain as described in the discussion paper (sale of raw data, insights from data analysis and the application of insights) together with the view that new technology and increasingly sophisticated data analysis will lead to the development of innovative new services.

3. HAVE WE ACCURATELY DESCRIBED THE DIFFERENT WAYS THAT PAYMENTS FIRMS ARE CURRENTLY USING PAYMENTS DATA? ARE THERE ANY OTHER USES THAT WE HAVE NOT INCLUDED?

3.1 We agree that the Discussion Paper has accurately captured the different ways that payments firms are using payments data both in the collaborative and competitive space as;

(a) Providing personalised products and services

(b) Developing and improving products and services

(c) Cross-selling non-payments based products and services

(d) Preventing and detecting fraud

(e) Prepare and sell statistical reports

(f) Comply with regulations

3.2 The only additional use case that we feel it may be useful to include is the Real Time Information (RTI) service that allows HMRC to receive additional payroll information linked to the payment.

3.3 The use of Artificial Intelligence (AI) and machine learning may lead to greater insights and more accurate decision making but we must ensure that the rules and processes are standardised where possible across the payments landscape to maximise these benefits, both domestically and globally. We support the increased use to data to combat fraud and to improve detection and funds repatriation.

4. DO YOU AGREE THAT THE MISMATCH BETWEEN CONSUMER TRUST IN ESTABLISHED BRANDS AND NEW THIRD-PARTY PROVIDERS COULD LEAD TO HARM IN INNOVATION AND COMPETITION IN THE PROVISION OF DATA BASED OVERLAY SERVICES AND HOW COULD THEY DELIVER BENEFITS? IF NOT, WHY?

4.1 We think it is too early to say whether any potential mismatch in consumer trust may have a negative impact on the development of new data-based overlay services.

4.2 Consumer trust is an important factor in financial services and it is important that consumers have confidence and trust in how their data is being used. Equally important is gaining the trust of Corporates and FI's who are also affected from a data security, reconciliation and operational efficiency perspective. Established brands have built up relationships and developed the trust of their customers. To ensure that this isn't a barrier

to innovation or competition, appropriate accreditation initiatives should be considered that will drive end-user confidence.

4.3 However, trust is hard won and can be easily lost as evidenced in recent high profile incidents and data breaches and applies equally to established brands as for new entrants or third party providers.

4.4 Established PSP's will always be cautious regarding data sharing and sensitive to potential data breaches. There may be increased reputational risk to PSP's arising from a potential breach concerning a customer using a TPP even though they may not directly be party to or liable for the breach.

4.5 The statement that there is a mismatch between consumer trust and new third-party providers is too broad. Different customer demographics display varying levels of acceptance and trust, e.g. millennials are generally more trusting and accepting of new providers and new solutions.

4.6 The discussion paper highlights that the UK payments sector is rapidly evolving and challengers can quickly acquire market share as has been seen by market disrupters such as Apple, Google, and Amazon etc.

4.7 Regulatory initiatives such as PSD2 and Open Banking should open up the market to competition and innovation, and as a result of these initiatives we are seeing new solutions and models come into the market place. These initiatives are still new and require time for solution development. Recent market intelligence suggests that the majority of consumers in the UK have little or no understanding of Open Banking. Clear and simple customer education is key to help deliver consistent messaging across the market to ensure that customers understand how their data is being used and what they are giving their permission for, so that any risks are clearly understood. This will develop confidence in new technology and third party financial service providers.

4.8 As we have stated, firms will build customer trust through the provision of attractive products and good customer experience. Innovation, by its definition, will lead to new products and services, but the market will determine which services are ultimately successful. Education will also be key to help build this trust so that customers have a clear understanding of how data will be used.

4.9 An approved accreditation scheme, such as an Open Banking kite mark (similar to the Direct Debit Guarantee Scheme) may help build consumer confidence and trust, but will need to demonstrate a clear impartial remediation approach and accountability should a third party suffer a data breach.

5. IN THE NEW PAYMENTS ARCHITECTURE (NPA), DO YOU AGREE THAT GLOBAL TRANSACTION DATA HELD IN THE CENTRAL INFRASTRUCTURE COULD HELP PROVIDERS DEVELOP OVERLAY SERVICES? IF SO, WHAT ARE THOSE SERVICES AND HOW COULD THEY DELIVER BENEFITS? IF NOT, WHY?

5.1 We support the assertion that data that passes over the central payments infrastructure could support new overlay services, *in principle*, but challenges around clarification of data ownership and usage that have delayed new services such as Money Mules must be overcome.

5.2 However, we have seen this market developing to an extent as PSP's collaborate with the current supplier to provide data analytics services. Money Mules is a good example of industry collaboration to combat APP fraud and to aid funds repatriation. It is noted that the service provider has had to obtain permission from the PSO's to use its data, notwithstanding that the payments pass over the central infrastructure.

5.3 The PSR could help in working across the regulatory environment to provide clarification and removing any potential barriers. For example; delays in securing data permissions can impact both speed to market and the development of collaborative services. Additionally, concerns over the application of GDPR and the penalties arising from a data breach have led to delays in developing new services, such as Account Name Verification Service.

5.4 Global transaction data held within both the NPA and managed through the new RTGS payment systems could help the development of overlay services which could improve customer confidence, combat financial crime, improve tax collection and reduce tax evasion.

6. WHAT MODELS COULD THE NPSO INTRODUCE TO ALLOW PSP'S TO GET ACCESS TO GLOBAL DATASETS?

6.1 PSP's process a huge and increasing volume of payments data that is being captured by the parties to the transactions (including the central infrastructure providers). Subject to clarification of consent and usage, provision of a central access to data could provide more efficient access for PSP's and at a potentially lower cost

6.2 There is scope for the regulatory authorities to act in concert to open up access to global datasets. Not only domestically, as the PSR should consider the broader international landscape and how different markets have approached these issues, i.e. FATCA regulation.

6.3 The NPSO should consider working through the potential economic models to enable effective monetisation of the usage of global datasets, i.e. the NPSO might act as a broker for transactional data sharing to allow overlay services which utilise global datasets to be developed on a commercial basis.

7. SHOULD ALL REGULATED PSO'S – INCLUDING INTERBANK AND CARD SCHEME OPERATORS – BE REQUIRED TO PROVIDE SOME ACCESS TO GLOBAL TRANSACTION DATA?

7.1 We generally agree that all regulated PSO's (including interbank and card scheme operators) should be required to provide some access to global transaction data where there is a clear customer need or for the purposes of combatting crime.

7.2 It is unclear from the discussion paper whether it advocates a central repository for the provision, storage and management of global datasets. This raises the issue of funding and we note that the paper is silent on the commercial value of data or the cost of maintaining and processing the data; is it right that a third party, not involved in the processing or upkeep of the central payment systems, would be able to access this data for free? We would expect that, at a minimum, there should be an agreed cost recovery model.

7.3 A single repository also brings risk from cyber security threats as well as internal data leaks, i.e. from employees.

7.4 However, we consider that global transaction datasets designed and aimed at improving efficiency and effectiveness of the Payment System Operator (PSO) should be available to all parties.

7.5 We would expect a proportionate approach to security and accreditation, if appropriate, commensurate with the level of risk that the user and data represented.

7.6 The PSR should work with demand side participants to understand the value of global datasets. For example, do global datasets add value or is a more granular level of detail required to be useful? If aggregated too much this may dilute the benefit, however this is dependent on the use case.

7.7 Other datasets i.e. anonymised and lightly aggregated datasets, may offer higher value in the competitive space and consequently financial institutions may provide data on a commercial basis, allowing larger providers the opportunity to recoup their higher costs of payment processing.

7.8 Examples already exist in that UK Finance produces a range of annual payments MI reports that are made free to its members or can be purchased by non-members. Similarly, PSO's collect and provide payment data (volumes and values) to the FCA to support PSR annual fee allocation.

7.9 As we have highlighted, we support the use of datasets to combat fraud, for anti-money laundering purposes or to support any crime prevention activity. We also recognise that there may also be specific use cases, i.e. relating to vulnerable customers, where there may be a clear public or societal need.

7.10 We also support the use of application programming interface (API) to ensure that any overlay services based on data sharing are developed in a secure and standardised manner. This will help incentivise the further innovation of new services and products.

8. IS THERE TENSION BETWEEN THE DEVELOPMENTS 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?

8.1 Tension does exist at Industry level in respect of the development of data analysis tools and GDPR requirements. Some of this is undoubtedly because each PSP is undertaking data impact assessments for new initiatives and notably the risk profile for each PSP is quite different.

8.2 Reaching consensus between the users and data owners has proved difficult and elongated, notwithstanding the significant investment by the industry and the clear benefits that this may bring to customers; for example, the Money Mules and Account Name Verification Service initiatives. The industry needs a consistent message to adhere to data sharing principles, inclusive of law enforcement, to ensure collaboration continues.

8.3 Payments and ancillary payments data are already legitimately shared between parties in end-to-end payments processing. Consent is not required provided that data is used for the purpose of completing the payment securely and effectively.

8.4 As there is often no contract between parties in the payment processing chain the consent collected by one party to use data for an overlay service may not be easily applied to the repurposing of that data once shared via the payment message by another party.

8.5 We suggest that any central consent process could reside with the NPSO or Card schemes as data owners with a legal responsibility to manage their data. Again, an industry accreditation scheme might prove useful.

9. ARE THERE ANY OTHER DATA-RELATED END-USER SOLUTIONS, APART FROM ENHANCED DATA, WHERE THERE COULD BE POTENTIAL BARRIERS TO ORGANISATIONS ADOPTING THEM? IF SO, WHAT ARE THESE BARRIERS?

9.1 New and existing models may prevent full payment information being captured and therefore may not support proposals to develop anti-fraud initiatives based on data analytics. For example, payment aggregation services models, such as PayPal do not provide the underlying merchant data.

9.2 As we have highlighted, Open Banking requirements are new and relatively untested. The PSR should give due regard to a clear dispute resolution process to address and provide clarity and confidence on where responsibilities and liability lies in the event that a payment (e-commerce, or other PISP) journey, that includes TPP's, goes wrong.

9.3 High fixed costs have been raised as a potential barrier to entry; however we do not always believe this to be the case. Fixed costs associated with technology are generally reducing as the industry seeks to take advantage of cloud based services where costs scale to use. Our view is that new entrants are likely to be more nimble in developing new services in a technologically advanced way than incumbent PSP's which are more likely to have to invest proportionately higher costs to migrate existing scaled platforms.

9.4 Conversely, the industry is investing significantly in the NPA and it is anticipated that this will provide a wide range of benefits and new models. Improved connectivity and access to the central infrastructure to a greater number of users could remove perceived potential barriers such as an inability to access data or data truncation.

9.5 The mandatory inclusion of additional data fields could have both a positive and negative impact. Whilst standardisation will improve straight through processing and provide additional information, the additional information may increase the potential cost burden and add more friction to the process for PSP's and Corporates.

10. ARE THERE ANY OTHER PAYMENTS DATA-RELATED ISSUES THAT COULD DIRECTLY OR INDIRECTLY AFFECT OUR OBJECTIVES?

10.1 The PSR has highlighted the potential indirect impact that other regulatory agencies (in particular where they are the lead regulator) have on its regulatory objectives. LBG believes that it is the role of the PSR to ensure it is fully joined up to avoid confusion and any unintended consequences.

10.2 The regulatory burden to PSP's is such that the PSR should focus on issues that directly impact its objectives and role as an economic regulator.

10.3 It is unclear how the PSR considers data that flows in and out of the UK. For instance, payments data may be derived from consumers or merchants outside of the UK (or the European Union). Similarly, it is unclear as to how would the PSR treat a request for access to datasets from an organisation that is domiciled outside of the UK/EU and if it should consider imposing additional controls?

10.4 We have advocated that the PSR allows sufficient time for the initiatives that are currently inflight to bed down. However, we would welcome clarity as to how the PSR will;

(a) Evaluate that these initiatives will deliver the required outcomes,

(b) Ensure it provides the right stewardship for the initiatives to deliver the required outcomes.

(c) Determine what are the appropriate timescales to allow for these initiatives to bed down before taking further action. For example, the low consumer awareness of Open Banking.

10.5 We would welcome further clarification of the PSR's understanding of the end-user needs, not only of consumers which appear well covered, but also SME's, corporates and Financial Institutions (FI's) and how this information will be shared with the NPSO and the NPA programme.

Member of the public

Submission to the Payment Systems Regulator Discussion Paper: "Data in the Payments Industry"

[redacted]

Executive Summary

1. I am contributing to this consultation in a personal capacity but drawing on my expertise in a range of data and consent related activities. In particular, I am co–chair of the Privacy and Consumer Advisory Group (PCAG) to the Government Digital Service and GOV.UK and in this role I am participating in the data sharing review boards set up as part of the Digital Economy Act (2017). I am also a member of the Open Banking Consumer Forum and recently completed a research project on consumer attitudes to sharing their financial data for the Financial Services Consumer Panel (Whitley and Pujadas 2018). I also offer an elective on data governance to MSc students at the London School of Economics and Political Science.
2. A key contribution of my response is to make explicit various assumptions that can be read in the discussion paper as well as introducing alternative perspectives on the assumptions identified.

Specific comments

3. Paragraph 1.3 talks uncritically about "business models based on collecting and processing data". There is a growing academic literature that questions the assumptions (e.g. Zuboff 2015) and the continuing concerns about how companies are making money from personal data (Privacy International 2017; Smith 2018).
4. Paragraph 1.10, I really don't think "valuecreate" is / should be a verb.
5. Paragraph 3.4, I think it is important to emphasise that the increase in available data is not the same as an increase in the amount of data that is being collected. The choice of what data is considered worth collecting and analysing is a business decision. Thus, as the paper notes, whilst there are some data fields that are readily available for "collection" (e.g. from within payment related messages) there are others forms of passive data collection (paragraph 4.12) that some firms would collect and which others would consider as digital exhaust fumes and discard, see also the discussion in ("The economic value of data" n.d.). For example, recent studies attempt to infer emotion through careful analysis of mouse movements on a screen (Hibbern et al. 2017). These choices go beyond the "ancillary data" identified in paragraph 4.6.
6. Paragraph 4.13 makes a very strong assumption that it is possible to anonymise personal data so that it is no longer personal. Again, there is growing evidence of the challenges with this assumption (Barocas and Nissenbaum 2014; Hern 2017; Lubarksy 2017; Narayanan and Felten 2014; Narayanan and Shmatikov 2008; O'Hara et al. 2011; Ohm 2010; Waddell 2017) including specific concerns

about reidentification using financial transactions (Montjoye et al. 2015). There is also excellent guidance about how to consider the risks around reidentification (Elliot et al. 2016). That approach suggests that the claim that a global dataset is unlikely to contain personal information (paragraph 4.18) is one about risk appetite rather than absolute values.

7. Paragraph 5.6 talks about using payments data to address "unmet market demand", implicitly suggesting that consumers would consume more if only the companies that are maximising their profits (for shareholder value) could address this unmet demand. There is also a strong assumption about who "owns" the data that is used to analyse this unmet demand, suggesting a strong asymmetry of power towards the data aggregator (who will probably keep all the surplus value) rather than the consumer.
8. Paragraph 5.9 talks about using "machine learning" to sell high–margin products such as loans and payroll management to current clients. Surely if competition is effective, the existence of "high–margin" products will decline as competitors enter the marketplace.
9. The assumptions underlying machine learning (box B) also need to be unpacked. Current machine learning techniques seek to identify patterns in the data with the assumptions that these patterns are stable over time (i.e. not subject to Goodhart's law (1975)) and that the training set is representative of the population to which the outcomes of the machine learning are intended to apply. If, however, data about certain categories of consumers are excluded from the training set, the resulting inferences will have limited (and possibly negative) consequences for the excluded individuals.
10. For example, consumers with chaotic lifestyles may have data patterns that do not match the "norm" and may find themselves excluded because some of the previous outlier patterns were identified as fraudulent or high risk. Equally, consumers who are similar to Westin's "privacy fundamentalists" and who don't give consent for their data to be shared for analytical purposes may distort the resulting analysis (e.g. Haggerty and Gazso 2005). See also the implications in paragrah 6.25.
11. Paragraph 5.12 is one of a number of paragraphs where the language about the potential benefits of data analysis / machine learning, explicitly shifts to the conditional, e.g. "data analytics *could* detect money laundering or other illegal or suspicious activity" (emphasis added). Unfortunately, the paragraph continues with a definitive statement: "This, in turn, *will* help reduce financial crime" (emphasis added). However, if the antecedent is false we cannot know if the consequent is true or not. See also paragraph 6.55 which mentions a PSP that *plans* to make significant investment and another that is investing in machine learning "in the hope" that it will be able to identify fraud in real time. Again, paragraph 6.57 talks about the use of cloud services that *might* level the competitive playing field.

12. Box A states that Money Dashboard is able to generate revenue of £8.80 per user per annum. If we combine this with the business model presented in paragraph 5.14, it is unclear how much discount the average customer will receive (particularly if Money Dashboard sell their aggregated results to many clients).
13. Section 6 seems to downplay the potential risks associated with sharing the "global transactions dataset" more widely. Whilst there is scope for useful analysis to take place, there is also the possibility that bad actors could undertake their own analysis to beat the system. This is a governance question about who should have access to the global transactions dataset (see also paragraph 6.13).
14. Paragraph 6.5 talks, unnecessarily, about "pooling" the transaction data, suggesting that a new (and vulnerable) data store ("a respository for sharing payment transaction data") will be created that various analytical firms could have access to. API access to 'read' the data is likely to be much more effective and lower risk.
15. I do not understand what is meant by the idea of a "central utility that allows PSPs to share and store non–competitive, encrypted KYC information" (paragraph 6.5). Is this more than (or different to) using assured identities to address KYC requirements?
16. Paragraph 6.14 talks about "lower costs for some users". By implication, there will be higher costs for some other users, such as those described in point 10.
17. Paragraph 6.16 is worded to suggest that if consumers don't agree to do something that they are not obliged to do so, then some form of innovation will be foregone. If we respect the right of individuals to act autonomously then this must be the case. Otherwise, there is a need to rely on presumed consent an approach which caused all sorts of problems for care.data.
18. The concerns about data protection identified in paragraph 6.18 are echoed in the FSCP research we undertook, referred to previously. In particular, we found that even those who had consented to share their personal data did not fully appreciate the consequences of what they had agreed to. For example, participants in the Emma's diary online forum would not have expected (or understood) that their data was going to be shared with the Labour party (Pegg 2018). Similar, Facebook users who signed up for various online quizes *may* have understood that some of their profile data would be shared with the quiz provider, *probably* would not have understood that this data might be used to drive political campaigns and *almost certainly* would not have appreciated that the personal data of their friends would also be shared with the quiz provider if they had not locked down their accounts. Teare et al. (2015) found similar results in the context of tissue donation to biobanks where biobank donors didn't fully appreciate what they had consented to.
19. The notion of trusted brands and organisations needs to be carefully considered from a methodological perspective as for every survey that suggests that high

street banks are most trusted, there is another which shows contradictory results.

20. A possible partial explanation for older people being less willing to use online banking (paragraph 6.23) is because, if things do go wrong, they have more (money) to lose.
21. Another important implication of competition in this space is that some of the companies with whom consumers may have agreed to share their personal data will fail. Greater clarity about what will happen to that personal data is needed (e.g. BBC News 2010).
22. Whilst education is an important activity (paragraph 6.28) it is important to recognise that telling people (or making the information available) does not mean that its implications will be fully appreciated. It is also important to differentiate between "known" uses (and future uses) and "unknown" future uses (e.g. biobanks of tissue samples could not obtain consent for DNA sequencing from donors before the technique existed).
23. It would be great to have informed decisions about data sharing, but our study revealed a range of "less" informed decision making and reliance on various alternative forms for support / redress (Whitley and Pujadas 2018).
24. Consideration of what kinds of questions might be reasonably asked of the global data set (paragraph 6.32) is perhaps something that might be covered by the Data Ethics Framework (GOV.UK 2018a) and the forthcoming Centre for Data Ethics and Innovation (GOV.UK 2018b). It would be interesting to know the appetite for using the analysis of global datasets to identify PSPs that might be more likely to enable money laundering and related activities.
25. When considering the risks around central infrastructure providers, it is helpful to remember the challenges SWIFT faced around processing some data in the US (OUT-LAW 2007). I am not sure if consent is the most appropriate legal basis for processing the data, e.g. to address fraud. The risk of using financial data for surveillance has been known for many years (Armer 1975).
26. I am not entirely convinced of the need to increase competition around central infrastructure providers versus the need to provide an efficient infrastructure (paragraph 6.41).
27. The (governance) question of who can have access to the NPA's central component APIs are probably similar to those that Open Banking is currently considering and there might be some useful symmetries between the two approaches.
28. The addition of enhanced data (Box E) presumably adds new "data risks" that go beyond the traditional approach of managing (physical) infrastructure risks—an alternative reading of the separate processing of remittance data is that it is shared using out–of–band messages. The fact that 30% of companies might use this new functionality over 10 years suggests a relatively unattractive cost benefit analysis (especially in terms of organisational transformation).

29. Discussion of the high fixed costs (paragraph 6.53) highlights the risk of network effects / the "Matthew effect" whereby those companies that can (afford to) build up large data sets will be able to produce "better" services, which increase their revenues and hence allow them to analyse larger data sets, etc.
30. Cloud computing (paragraph 6.57) doesn't necessarily reduce IT costs, even if it does move it from capital to operational budgets.
31. When considering the opportunity to offer tailored recommendations (paragraph 6.60), there is a real risk that the recommender will be able to determine what level of premium (i.e. not necessarily the best for the consumer) the consumer is prepared to pay. By analogy, Amazon's knowledge of which customers bought higher price goods that offered quicker delivery meant that they had a good sense of what they could charge for their Prime service that would enable it to be successful (i.e. infer willingness to pay, paragraph 6.62).
32. There is a risk that those individuals who don't agree to the use of fully automated decisions will be the ones with unusual circumstances (or strong privacy concerns) and will therefore receive a suboptimal service.

Mastercard-Vocalink

DISCUSSION PAPER RESPONSE

Mastercard-Vocalink response to *PSR 'Discussion paper: Data in the payments industry '*

3 SEPTEMBER 2018

Summary

The appropriate use of payments data can detect and prevent fraud, enable consumers to access new services and provide other useful insights with commercial value. We welcome the PSR's engagement in this significant aspect of the payments market.

However, there are issues around access to payments data which require full and detailed assessment before the PSR can consider the appropriateness of any intervention. In particular the PSR needs to consider further:

- the limitations and implications of EU General Data Protection Regulation (GDPR) and related consumer privacy concerns;
- the inherent risks in opening up access to data and the need for a robust regulatory framework to support any such moves, which addresses security issues; and
- the fact that payments data is just one part of a much larger relevant dataset and so opening up access to it without reciprocal access to other (non-payments) data is likely to distort markets and lessen competition.

The comments in this response are divided into 7 sections which outline the most important factors that the PSR should consider. We have adopted this approach (rather than responding to the Discussion Questions directly) because we believe that there a number of significant questions which the Discussion Paper does not address. It is vital that these are considered as part of the PSR's early stage thinking in order to help inform the development of its proposals. We are concerned that in places, the PSR is drawing conclusions (and even proposing remedies) before it has properly understood the wider nature of payments data and some inherent risk factors.

In particular, we are concerned that the PSR appears to be proposing a very specific remedy of requiring regulated Payment System Operators (PSOs) to provide access to global transaction data. We consider that it would be more appropriate, and consistent with its statutory framework, for the PSR first to articulate, assess and consult on possible market failures, and then articulate, assess and consult on possible remedies for any market failure identified.

PSR has not yet demonstrated any clear evidence of market demand for the proposals that it is making (particularly in relation to cards) and so its paper appears to present a theoretical view, rather than something for which there is a genuine, evidence-based need, supported by a commercial case which takes into account costs and risks.

This response is a joint Mastercard-Vocalink response, but for simplicity we predominately refer only to Mastercard. However, we believe that issues related to cards and interbank data are sometimes quite different. Indeed, there are strong arguments that cards data should be outside the remit because, for example:

- cards data is truly global and if the PSR's domestic remit is not clearly defined there is obviously the risk of conflict of laws with other jurisdictions; and
- open banking, the previous work of the Payments Strategy Forum and the New Payments Architecture are driving a lot of the new thinking and market developments for interbank payments data. In contrast, Mastercard does not believe that same range of opportunities necessarily exist for cards payment data, but that providers are already operating in the market without the need for PSR intervention.

1) Privacy, Data Protection and Confidentiality

The existing regulatory framework

Confidentiality and protection of personal data are paramount to developing trusted data practices and unleashing value of data. The EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 are a significant factor in what's been proposed in the Discussion Paper and a thorough analysis on the data protection and confidentiality requirements and how they can be met in practice is key to what is being proposed in the Discussion Paper.

A clear understanding of the roles of the parties as well as associated responsibilities and rights is essential. Issuing and acquiring banks (or in the case of interbank payments, the sending and receiving banks) act as a data controller for the transaction data processed by scheme operators, such as Mastercard, and the scheme operators act as a data processor. What this means is that the scheme operators typically process payments data under the instructions of the banks and would need instructions and permissions from the banks to disclose payments data to a third party. Where a third party determines how the payments data are to be processed (e.g. develop a model), it would act as a data controller.

Banks acting as a data controller would need a legal basis to instruct scheme operators to share the payments data with a third party. Meanwhile, a third party service provider acting as a data controller would also need a legal basis to process payments data for its own purposes. Other than for fraud prevention and monitoring purposes and other purposes stipulated as a public interest (e.g. anti-money laundering purpose), it is most likely that freely given, specific, informed and unambiguous consent would be the viable legal basis.

Consumer rights

In practice, obtaining valid consent is not simple and it requires proper management in order to enable consumers to withdraw consent any time free of charge. Further, consumers have the right to access, correct, update and delete their personal data and the third party service providers will need to put in place a process to respond to such request. Of course, through open banking consumers already have choices to request their data to be ported to a service provider (such as Money Dashboard) to manage their personal finance for example to benefit from payments data analytics and therefore third party service providers already have the means to access the data.

We would also like to note that the joint liability regime under the GDPR and UK Data Protection Act 2018 will elevate the liability level of all those who would be involved in the payments data processing for analytics – the more service providers have access to payments data, the more liability there will be on all the players involved in the payments data processing ecosystem. Increased liability without adequate visibility and control may put the industry players in a difficult position to share the data.

Aggregated and anonymised data has the potential to promote payments data use in a way that benefits consumers while protecting their privacy. Ultimately, insights derived from personal data, not the personal data or raw transaction data in themselves, have the value and may contribute to further innovation. As a result of the GDPR, there are robust anonymisation solutions in the market that allow for using data with significantly reduced risk of re-identification while preserving the value of the data.

In addition to data protection requirements, Mastercard has confidentiality obligations towards its customers and is not in the position to disclose their confidential information (i.e. transaction data) without their permission. We encourage the PSR to take into account confidentiality obligations, including bank secrecy obligations, and consider how to work within these restrictions.

2) Establishing a basis for change

Mastercard strongly supports the PSR's objectives of improving competition in the payments market and is interested in its decision to focus on payments data. We are also aware of the Treasury's recent publication of its own discussion paper "*The economic value of data*", which addresses some of the same issues raised by the PSR. We recognise therefore that the PSR's proposals may be part of a wider Government objective to promote economic growth through the economic exploitation of data.

Evidence of a market failure?

However, we would welcome a clearer and more detailed understanding of which parts of the payments market specifically the PSR believes competition is ineffective and therefore would be improved by its proposals. In Chapter 5, the PSR provides some fairly high level examples of the ways in which it believes that payments data is currently being used by those who have access to it. It describes those examples as producing benefits both to providers and end-users and so it is unclear where (or indeed whether) the PSR believes that any market failure might exist. In addition, some of the examples given relate to the use of data by the PSP concerned, only in order for that PSP to improve its service to that particular customer, which does not appear to have any wider application beyond that bilateral relationship.

Mastercard would therefore like to understand where the PSR sees that there is a market demand for the type of open access which it is proposing. In particular:

- what type of providers would like access to payments data?
- what kind of data do they wish to access?
- what types of services would this data enable them to offer?
- what barriers are currently preventing those providers from obtaining access to that data?

Has the PSR identified that competition for the specific services included in Chapter 5 is being restrained and if so, can it provide evidence of that unmet demand?

There are several references in the Discussion Paper to the need for access to data in order to develop "*fraud and financial crime prevention measures*" and also a generic reference to the use of data by "*data analytics firms, innovators or future overlay services*". If (as it suggests) the PSR is proposing regulation in order to require providers to open access, it is incumbent on the PSR to be much more specific and evidence-based in its justification for such intervention, beyond what appears to be a largely theoretical perspective.

The use of payments data for fraud prevention is a specific use case that has unique challenges which we discuss further below, when considering security and trust implications. In particular, the PSR must be careful that it does not inadvertently create even greater fraud risks by providing access to particular types of data and also that it does not distort the market by further entrenching the position of the incumbents.

More generally, Mastercard's experience of the other markets (where payments data is relevant) in which we operate is that those markets have fairly limited opportunities (judged by the number of potential customers) but that a number of providers are already competing where a market does exist. For example, Mastercard Advisors is

Mastercard's consultancy business providing a wide range of services primarily to banks and merchants. The banks have access to their own payments data, but from time to time Mastercard Advisors may make use of Mastercard payments data when offering services to merchants.

However, this is a very specific market as the services tend only to be relevant to a particular type and size of retailer. Nevertheless, others do already compete in this market because they are able to negotiate directly with the banks in order to obtain access to relevant payments data. As we discuss later in this response, they are able to combine payments data with a wide range of other (often more granular) data, enhancing their value proposition to this retail customers. As this market is already active and working effectively, it is unclear what benefits the PSR's proposals may bring.

Therefore, if the PSR does not yet have substantive evidence, it should conduct market research in order to understand the size of the potential market that exists, which will allow it to develop its proposals on a more informed basis.

Data quality

Whilst considering demand, it is also important to address issues of data quality, which are likely to be a key consideration within this context. For example, it is not possible simply to combine disparate data sets, as many of those datasets have unique data quality issues which third party would either not be able to identify or know how to correct. The risk is that any resulting analyses may well be incorrect.

For example, in the case of cards, transaction volume data would be significantly affected by the issuers who were issuing Mastercard cards at any point in time. So the loss or gain of a large issuer (or the change in mix of issuers) would affect those volumes in a way which might appear to be an increase or decrease in cardholder spend, when in reality that is not in fact the case.

Aggregated data may also disguise other important factors such as the number of days/weekends in a month or seasonal variations. Likewise merchant names in the data change and therefore determining common points of purchase requires an understanding of merchant data issues. Whilst we recognise that PSR's analysis will not yet have reached this level of detail, data quality is an important consideration in any model which it may wish to develop.

Challenges to be addressed

Depending on the model which the PSR might ultimately adopt, there may be huge complexities and risks involved, which we reference elsewhere in this response.

From a legal perspective, privacy and confidentiality issues are the most relevant and we have already outlined the challenges which the GDPR may present. However, there may also be intellectual property questions in relation to the ownership of datasets (which is referenced in the Government's discussion paper) as well as contractual issues between parties with whom the data may be shared. That might also lead to commercial models which need to be agreed because (at the very least) there are likely to be questions of cost recovery from those who might be required to make significant investments in order to be able to provide access to data, for example through data reformatting, data transfer mechanism builds, software rewrites and authentication processes.

For cards, vendors will typically hold the data for the banks, so there will be direct out-of-pocket expenses to the vendor in extracting that data. For interbank schemes, the infrastructure provider will incur direct out-of-pocket expenses to extract the data on behalf of the PSO and/or banks.

Naturally, there will be significant technical issues to be addressed, depending on what form of access is required to what type of data. The PSR will be well aware of the huge amount of work undertaken by the Open Banking Implementation Entity and the respective banks in order to facilitate the access required for those services. In addition, there will certainly be issues of public trust, which go beyond the legal requirements of GDPR that are discussed later in this response.

The need for a cost-benefit analysis

Mastercard is not opposed in principle to any proposals to increase access to payments data, but in view of the uncertain need and potentially significant challenges and costs involved, we strongly believe that the PSR must undertake a rigorous cost benefit analysis to ensure those investments will be justified.

That must begin by developing an evidence base for the demand (and therefore benefits) of what it may be proposing. Without a clear assessment that the costs will be justified, there is a real risk of requiring the industry to undertake a level of investment and technical development work, which might adversely impact and delay other projects which would have delivered more tangible benefits to innovation and end-users in line with the PSR's objectives.

This response has set out some of the risks of mandating access to payments data and in particular a data breach resulting in commercial harm or the loss of privacy. A robust and reliable cost benefit analysis will need to take into account the probability and cost of such risks materialising.

3) The relevance of card data

Mastercard understands that the issues in relation to payments data which have so far been raised with the PSR have been largely within the context of the work of the Payment Strategy Forum. This is perhaps linked, in particular, to proposals for confirmation of payee and request to pay. Whilst obviously important, these are fairly limited examples within the wider context of payments data which the PSR appears to be considering and do not relate to the type of intervention being proposed. Specifically, they do not seem to have any direct connection with the PSR's proposals to open up access to payments data more generally and so would not on their own justify that type of requirement.

The distinct nature of card schemes

However, Mastercard is of course acutely aware of the fast-evolving nature of the interbank market in the UK more generally, led primarily by the introduction of open banking, as well as all of the work of the Payment Strategy Forum and particularly the creation of the New Payments Architecture. This is driving a lot of new thinking and market development in terms of how payments will be delivered in the future and how greater choice and innovation will be delivering benefits to end-users, which might be prompting some discussion in relation to the use of data.

The evolution of card payments, important as they are, is slightly apart from many of these developments. Whilst the cards market will be hugely impacted by the increase in competition from interbank payments, it is not encountering quite the same degree of almost revolutionary change which is just beginning in that sector. As it appears to be this change which is driving thoughts around the use of payments data, Mastercard does not believe that the demand for cards payment data is likely to be quite the same, if indeed the PSR has received any representations at all in relation to cards data.

Indeed, the Discussion Paper makes fairly limited references to the cards market and most of the examples as to how payment data may be used appear to focus on interbank payments data. We have outlined above a general view that the PSR should provide evidence of the nature of the demand which it believes exists, which we believe to be of even greater relevance in the cards market. This is in part because it appears as if the PSR may not have received any direct representations of the need for that data to be provided.

The international scope of card schemes

There is also an important distinction to be made in terms of the global nature of card networks and therefore cards payments data. Mastercard understands that the PSR's focus (and regulatory remit) only extends to UK domestic transactions. This is relatively straightforward from an interbank perspective, as the interbank schemes, other than Swift, are all domestic schemes, which only manage domestic payments between UK bank accounts.

But in the UK, there is no domestic payment card scheme and so all of the schemes operating in the UK are global schemes. In that context, it is not clear what the PSR may mean by a domestic transaction and how it may determine what types of card transactions would be relevant or in scope. The location of the cardholder (most obviously determined by the location of the issuer), the location of the acquirer and the location of the merchant/point of sale are all relevant considerations. Of course, many card transactions (particularly ecommerce transactions) are cross border, but we would naturally assume that both the issuer and the merchant would need to be located in the UK

for the PSR to consider the transaction to be in scope. However, the issues are not straightforward and if the remit is not clearly defined there is obviously the risk of conflict of laws with other jurisdictions.

Card schemes and infrastructure providers

There is a further complexity in that card networks also act as both infrastructure providers/processors and schemes, with the respective functions being separated under Article 7 of the Interchange Fee Regulation. Arguably, the data in relation to those functions is separate, although in reality it largely relates to the same transactions.

On strict interpretation, 'scheme transaction data' would probably be viewed as data related to all Mastercard branded transactions (regardless of the processor). That data is simply reported to Mastercard by its customers, but we cannot verify its accuracy nor completeness. By contrast, 'processed data' relates to the transactions which Mastercard switches and provides a greater degree of granularity, but does not include all 'Mastercard transactions'.
.
The PSR will be aware from its fees work (as well as various other past information requests for transaction data) of the problems caused by the lack of a single Mastercard 'dataset' and the difficulties of dealing with reported versus processed data. If the PSR was to consider any requirement for access to data to be provided, we assume that it would be most likely to relate to processed data (with the necessary issuer consents), but we would welcome any clarification which the PSR is able to provide.

However, the PSR appears to be viewing Mastercard in its role as a card scheme, although the data which forms the basis of our analytics is in fact processed data. Mastercard has access to that data as a consequence of the processing (switching) service which we provide to individual customers. The purpose of Article 7 was of course to further competition in that market and so the data to which we have access is subject to change, as each Mastercard customer decides if they do or do not wish to purchase that service from us. In many other countries, Mastercard processes fewer transactions (and therefore has access to much less data) than we do in the UK.

As previously explained, the resulting data is not owned by Mastercard and so the PSR should not base its proposals on an assumption that we control (or even have access to) a level of data which is outside of our control

4) Interbank Data/The role of a central infrastructure provider

Mastercard, through its subsidiary Vocalink, is the infrastructure service provider to Bacs, Faster Payments, LINK and Cheque schemes. Vocalink does not 'own' the transaction data which passes through its systems, therefore Vocalink cannot give others access to the data without the permission of the banks and/or scheme to which it relates.

Any entity can request permissions from the banks and schemes for data access for any proposed product or solution, subject to the appropriate conditions such as compliance with data security and privacy requirements. The banks and/or schemes can give permission for access to the data as long as they comply with GDPR when doing so. Under contractual obligations, Vocalink has to provide technical access to the data to whomever the banks and/or scheme want. Vocalink has no reason, ability or legal basis to degrade the quality of the data made available to other data analytics service providers.

It is therefore not appropriate or necessary to place a regulatory obligation on infrastructure providers to give access to the data that flows through its systems because:

- the infrastructure provider cannot provide access to data without the permission of the banks and/or schemes; and
- if the banks and/or schemes want others to have access to the data then Vocalink is already contractually obliged to do so.

Vocalink has spent time and money to build its analytics business. To do so it has sought and gained the appropriate permissions to access and use data for specific purposes and it must obtain permission for each proof of concept or service proposition. (As outlined elsewhere in this response, the same situation occurs in the cards market where it is open to any provider to negotiate directly with banks to obtain access to payments data.)

We have knowingly made this significant investment in its analytics business at commercial risk and it is open to others to do the same, if they have not done so already. The PSR should not disincentivise further investment by us (or others) by imposing inappropriate regulation in this area. Such regulation could create uncertainty and stifle investment and innovation, not just in data analytics but potentially in other payment services markets to the detriment of service users. Such action could contradict the PSR's duty to encourage innovation.

5) Public Policy and Consent

A challenging time to open up access to data

The PSR will be well aware that many issues related to data continue to raise significant interest from a media and public policy perspective. High profile data breaches and misuses, as well as the introduction of the GDPR have created a level of public awareness and sensitivity which did not exist just a few years ago. That means that any proposals to open up access to data are likely to be viewed with a greater degree of public caution than might previously have been the case.

The GDPR was, of course, designed in part to address these concerns by giving users more control over their data. But there does seem to be something of an inherent tension between that objective and the PSR's objective significantly to increase access to the data. If its proposals are to be accepted by a potentially sceptical public, the PSR will need to work hard to resolve that conflict, particularly when most official warnings are to take stringent steps to protect personal data.

This is therefore a uniquely challenging time to be proposing a new regulatory environment in which large quantities of personal data will be made available to an infinite number of unidentified entities, for them to use in order to generate commercial profit. Consumers will want to understand why this is being done and what safeguards and controls are being put in place. We address this point in greater detail below when considering what kind of regulatory framework might be needed to govern those who would have access to the data.

Understanding consumer opinion

The PSR's proposals will clearly require consumers' consent, both in the legal sense (as required by GDPR), but also a broader 'moral' consent and support for the objectives which the PSR is pursuing. That consent may not be forthcoming if consumers perceive a new data risk is being created, for which they will receive no correlating benefit. Mastercard believes that it will therefore be vital to gauge consumer reaction at a very early stage to a proposal which has the potential to encounter significant opposition. The PSR should do so by undertaking a detailed level of consumer research, not merely to understand at a macro level views on the opening up of payments data, but also where consumers believe the balance or 'pay off' lies in what they would expect to receive in return for providing consent.

Mastercard has looked at this question in the context of open banking in order to understand how likely consumers are to give access to potential Payment Initiation Service Providers and Account Information Service Providers. We recognise that we are at a very early point in development of open banking and that a lack of awareness is likely to have impacted consumer opinion. However, our own research highlights a likely consumer reluctance to give consent to those providers, even though in that environment consent is only given to a specific entity in order for it to be able to provide a specific service, which has a clearly identifiable benefit to the consumer.

The PSR's challenge will be greater because providing open access to a 'global dataset' to allow providers to use data in an aggregated format will not generally provide any identifiable benefit specific to the individual being asked to give consent. In addition, unlike open banking, the consumer is being asked not merely to give consent to a particular provider (who they may know and trust) but rather to grant access to their personal data to an indefinite number of unidentified third parties.

In this context, there is a particular query in relation to the use of enhanced data and whether its use is in fact in the consumer's interests or it may perhaps simply add friction or irritation to the transaction, whilst at the same time increasing privacy concerns. It might alternatively be better to consider that enhanced data is only suitable for B2B transactions. If there is any obligation to include it within consumer transactions, it may risk driving consumers away from that form of payment.

6) Security and Trust

The PSR identifies consumers' reluctance to share payments data, as one of the three principal policy issues which it is considering, but it will also recognise that the issues of trust and consumer willingness to share data are inextricably linked with that of security in providing access to that data. So if the PSR is thinking about how to encourage consumers to have sufficient trust to give consent, ensuring that there is a robust security framework, including security standards, is a key consideration.

Avoiding security risks

The PSR will be well aware of the security risks inherent in opening access to large quantities of sensitive personal data. Although this is clearly not the PSR's intention, it is important to be aware of any potential unintended consequences. Indeed, it would be an acute irony if, whilst attempting to combat fraud by encouraging the development of more anti-fraud tools, fraud actually increased as a result of greater opportunities for criminals to access critical data. The PSR will need to ensure that it avoids creating larger than necessary repositories of data or single points of access to that data will obviously increase the risks significantly, unless there is an overriding reason why it is required.

However, by far the greatest security risk would be to allow third parties to have access to live transaction data streams. Mastercard believes that such access would only ever even be relevant in a scenario of trying to prevent potentially fraudulent transactions before they have been completed. This is indeed how certain fraud prevention tools in card payments operate, allowing merchants and issuers and their service providers to the transaction to detect and thereby prevent fraud. The nature of card payments means that the authorisation message is the critical point in the transaction flow and if criminals (or potentially terrorists) were able to access that, it could have extremely serious consequences, not just from the perspective of increased fraud threat, but also cyber security and resilience risks more broadly.

These are very real risks, which must be an overarching consideration in any decision that the PSR may make to provide greater ease of access to payments data. Whilst the PSR rightly focuses on its duties to promote competition and innovation, it cannot be at the expense of creating any risk to the security of payments data which would certainly not be in the interests of end-users. Mastercard therefore assumes that the PSR is not considering any kind of access being provided to live transaction data streams, but we would welcome the PSR's confirmation on this critical point.

Co-incidentally the Financial Market Infrastructure Division of the Bank of England recently commenced an IT infrastructure resilience thematic review and a cyber-resilience review of those infrastructures that it supervises.

Participants' role in the transaction process

Mastercard does not believe that this is a sector of the payments market in which the interests of end-users would best be served by the involvement of very large numbers of potential providers in that process.

Those parties who might currently compete and co-operate to perform this role (including the bank, the merchant, the payment processor and the card network or interbank scheme) are able to do so because of their existing core role in the payment transaction, meaning that they have an inherent interest both in the security of the transaction

and the integrity of the data more broadly. Fraud detection and prevention tools are provided as a consequence of that principal role, rather than as the sole purpose of their involvement. If the PSR's objective is to allow others to provide fraud detection and prevention tools in a payment transaction, it must do so to the standards required by, and the approval of, the banks, card network and/or interbank scheme. (The parties giving approval will depend on the specifics of the fraud detection and prevention tool). Otherwise it threatens to undermine the trust between the parties who have a mutual interest in the security of the transaction, particularly if that third party provider is not subject to any regulatory framework.

To access the data, a third party would be required to obtain consent from the individual. The third party would then need to demonstrate to the card network that it has obtained the individual's consent. The authentication data from the individual is likely to be wider than the data required for the primary purpose, and this collection and sharing of wider data increases the risk of loss or misuse.

7) Regulatory Framework

Throughout the Discussion Paper, the PSR makes no comment on the possible regulatory framework which would apply specifically in relation to its proposals to provide open access to payments data, aside from a recognition of the role of the GDPR and need to maintain compliance. Mastercard believes that this is a significant omission and that the establishment of an appropriate regulatory framework should be a key consideration.

Comparisons with Open Banking

One aspect of the open banking model within PSD2 which caused particular comment and concern early in the process was the absence of a need for any contractual relationship between the Third Party Provider and the Account Servicing Payment Service Provider. The concept of an entirely 'open access' API model to which any provider was able to 'plug in' and obtain access created obvious risks and concerns on the part of the ASPSP, but those risks were mitigated to some degree by the establishment of a robust regulatory framework. That framework requires not only direct authorisation and supervision of any TPPs which wish to gain access, but also 'strong customer authentication' to ensure that a rigorous check must be passed each time a TPP wants to access the data (as well, of course, to ensure that the individual consumer in each case has consented to that access being provided.)

It is unclear from the Discussion Paper whether or not the PSR is proposing a similar model, but Mastercard believes that it must seriously consider what type of regulatory framework would be required for the open access model it is proposing. We outlined earlier in this response the public policy issues and concerns which we believe that the PSR's proposals may raise and the related security considerations which are key to addressing them. The regulatory framework is clearly the other element of that response.

The other element of the open banking model which the PSR must consider in this context is how to handle liability issues and specifically where responsibility lies for incorrect data, lost or stolen data or its misuse by recipients. The PSR will be aware that liability has been another significant concern for ASPSPs with respect to open banking and whilst there is now greater clarity than there was, some questions do still remain. Again, the PSR needs to be thinking about these issues at the earliest stages, or else they are likely to cause ongoing concerns to be raised.

Managing public concern

It seems inevitable that the absence of regulatory controls is likely to increase the level of public (and potentially media) interest and concern. The idea of open access to sensitive payments data being permitted without implementing any specific checks and balances or oversight of those able to gain access, may seem alarming. It will almost certainly significantly increase opposition and make consumers far less likely to provide consent where that it required. That may well impact not only these proposals, but also the success of open banking more generally, even though in that case a regulatory framework does exist. We note again that one of the PSR's policy issues concerns the possible reluctance of consumers to provide the necessary consents to data sharing. An effective regulatory framework seems essential to addressing that issue.

A useful comparison can be made in the similar telecoms market where third parties were permitted to request telecoms operators to provide directory information (names and telephone numbers) to providers who wished to establish competing directory inquiry services. For many years this was largely uncontroversial until a new provider announced it would be utilising mobile telephone numbers to allow callers to connect to people who they did not

know. The proposal caused such outrage that it quickly led to a viral campaign encouraging people to opt out of the service, with the result that the provider's business immediately failed and the service was in fact never launched. The PSR will be keen to avoid any similar negative response to its proposals.

8) Distorting the market

We note again the recent publication of the Government's own discussion paper "*The economic value of data*", which addresses some of the same issues raised by the PSR, but from a much wider perspective. By contrast, the PSR is looking at core payments transaction data in isolation, which is understandable in view of its remit and powers. But in reality, the way in which data is used and the providers who use it does not align with the PSR's remit.

Therefore, if the PSR imposes open access obligations only on its regulated entities it risks distorting the market in favour of those who it does not regulate and against those who it does. The result might appear to increase competition in the payments market, but in practice, it will be limiting competition in a wider 'data market'. In simple terms, this challenge arises because of two key factors.

Strengthening dominant players

First, some providers who may have an interest in gaining access to payments data are PSR regulated entities (primarily the interbank and card schemes), but many others are not. The latter category would most obviously include merchants, digital platforms and credit reference agencies (only regulated by the FCA), but is necessarily open-ended. An obligation to provide open access to payment data would require those in the former category to provide data access to those in the latter category, but there would be no reciprocal requirement or arrangement in the other direction. This would inevitably create significant asymmetries in access to data which the PSR will want to avoid, because of the obvious distortions in the market which would naturally follow.

The problem is made more acute by the fact that latter category already occupy positions of significant strength in their respective markets. The largest players in these sectors are all well-known and their access, use and control of data is already a matter of significant public policy and regulatory concern. This is perhaps most well recognised with respect to the digital platforms, but the credit reference agencies have also come under scrutiny with respect to the volumes of data which they hold. There is clearly therefore a risk that opening up one-way access to payments data to these providers will exacerbate existing concerns with respect to these providers. Although those wider issues may not be directly the PSR's concern, even within the payments market, competition is likely to be distorted for reasons now explained.

Combining larger datasets

The second key factor is that for many providers who may have an interest in gaining access to payments data, that payments data is just one element of the much larger dataset which they maintain (or would like to hold). Although the PSR may view payments data in isolation, in reality providers will not treat it as such and will combine it with many other types of, potentially very granular, data which they hold. Indeed, it is the combination of different types of data which often creates the greatest value and competitive advantage to those who are able to do it.

Once again, the risks of asymmetries of information and resulting distortions to competition will be clear to the PSR. Those entities, unregulated by the PSR, will be able to add payments data to their datasets, thereby strengthening their position in the market, without providing any reciprocal access to their data. By contrast, those regulated entities which would be required to provide access to payments data will not be able to combine data in the same way because the data to which they have access will be far more limited. Without the ability to combine and

enhance the value of the data which they have, they will be at a significant competitive disadvantage. Further distortions may be created in the absences of standardization of the payments data.

Card schemes access to data

We outlined earlier some of the unique considerations in the cards market and the fact that technical access to data is only possible where Mastercard processed the transactions. This also creates important considerations from a competitive perspective, because the PSR must bear in mind that this is a core element of the service which Mastercard provides and the ecosystem which we have built.

As Mastercard does not own the data and it is in some way a 'by product' of processing, it might be easy to assume that we have not contributed to its creation and therefore the value which may be generated by it. On that basis, the PSR might conclude that Mastercard has unfair or unjustified preferential access to this third party data and it would be more equitable for that access to be widened, in the interests of competition.

But this would be a significant miscalculation. The data only exists because Mastercard has built the network to process the transactions, which produce the data. That has required a very significant investment over many years. Rather than being simply a by-product of a service, the data is better viewed as the manifestation of that investment. This is a vital consideration for the PSR as it considers the competitive impact of its proposals, because if it did not take account of such investment, it risks distorting the market and denying a fair return to those whose investments have created the market.

The nature of competition

Finally, it's worth considering that the PSR's proposals might also have a chilling effect on the availability and sharing of payments data by those not subject to any regulation, with those who are subject to the regulation. For example, it may make merchants less likely to share data, if it might end up with (potentially unregulated) third parties (most obviously their direct competitors) with whom they have no relationship and over which they have no control. The overall effect will be less payments data available from which any participant is able to benefit.

Even if we are to consider competition within the payments sector more specifically, the issues may be more complicated than the PSR acknowledges. The difficulty arises partly because the PSR appears to be considering a 'market for access to data', rather than a 'market for the services provided using that data'. The reality in some parts of the market may not be as straightforward as the PSR might assume, because again the proposed open access risks creating asymmetries, which could distort competition.

For example, although Mastercard offers anti-fraud products and services to UK banks, it has a small market share. The major players in that market are actually the payment processors, who obviously have access to payments data in relation to all of the payments which they process, whilst Mastercard only has access to data in relation to Mastercard processed transactions. Therefore, if through open access requirements, the processors were able to access data in relation to all Mastercard transactions (in addition to all of the transactions which they already process) it would further strengthen their position in this market, making it extremely difficult for others to compete.

As a consequence, any requirement on Mastercard to provide access to this data is most likely to reduce competition and disincentivise Mastercard's further development and expansion in data use and data analytics. This in turn would inevitably reduce the services which would otherwise be made available

If the PSR is to pursue any proposals to open up access to data, it must of course ensure that it is done on an equal and equitable basis from the perspective of those who are required to provide access. The risks to competition will be significant if there is any possibility that one provider is able to provide access to a different or narrower dataset than its competitor, thereby creating an arbitrage opportunity, particularly where competitors may have an interest in gaining access to each other's data. This is yet another reason, why the PSR should consider the imposition of a stringent regulatory framework to support its proposed model.

[redacted]

Money Advice Service

[redacted]

2nd October 2018

To PSR Payments Data Project Team,

The Money Advice Service (MAS) welcomes the opportunity to respond to the PSR discussion paper on Data in the Payments Industry.

About Us

MAS is a UK-wide service set up by Government to improve people's ability to manage their financial affairs. Our free and impartial money guidance is available online, and by phone or webchat.
Our statutory objectives are set out in the Financial Services Act 2010 and in 2012, we were also given responsibilities under statute to improve the availability, quality and consistency of debt advice across the UK. We are funded by a statutory levy on the financial services industry, raised by the Financial Conduct Authority.

As the statutory body for financial capability, MAS has led work with financial services firms, the third sector, government and regulators to develop the Financial Capability Strategy for the UK. This 10-year strategy aims to improve financial capability, giving people the ability, motivation and opportunity to make the most of their money.

The Financial Guidance and Claims Act 2018[1] makes provision for establishing a new Single Financial Guidance Body, to bring together the functions of MAS, TPAS and Pension Wise.

[1] Financial Services Act 2012 http://www.legislation.gov.uk/ukpga/2012/21/contents/enacted

Our response

MAS fully supports development of the payments ecosystem which works towards meeting consumer needs and ensuring a strong economy. To that end, we have been part of The Payments Strategy Forum[2], and helped in the creation of design principles for the development of payment systems which are reflective of consumers' needs and level of financial capability. We encourage the PSR's work in this area to use and apply these principles. To reduce the likelihood of future detriments being created for consumers, the principles aim to:

- ensure that UK payment services reflect and respond to consumers' needs;
- ensure that UK payment services are developed in an inclusive way that enhances consumers' ability to manage their money day-to-day; and
- invest in financial capability interventions that work, where it remains necessary to develop consumers' capability to engage with payment systems and build trust and confidence in them.

Engaging with consumer capability through the Financial Capability Strategy for the UK

The discussion paper highlights end user reluctance to provide access to their data as a key barrier. We agree this is a potential barrier that could limit or restrict demand for overlay services in a way that could negatively affect competition. Many of the consumers who could potentially benefit the most from these products are those least likely to engage with them, for a variety of reasons including access, digital exclusion and low financial capability.

To address this, it is important that the nuanced nature of this reluctance is understood and responded to by the payments industry. This must include an understanding of the capability and behaviours driving this reluctance and should not be reduced to a lack of awareness from consumers which would restrict demand for new overlay services, negatively affecting competition.

For customers using, and more importantly giving explicit consent, to share their data as they engage with payments is more than just about accessibility, though this is a crucial first step. The confidence, skills and ability to engage with money and financial decisions is integral to financial capability. The 2015 UK Financial Capability Survey[3] shows the importance of financial capability – skills, knowledge, attitudes, motivation and opportunity – on optimising financial behaviour such as managing money well day to day, planning ahead and avoiding financial difficulty.

At present, levels of financial capability in the UK are low and this in turn, impacts consumers' ability and motivation to engage with financial services. Low financial capability results in detriment to consumers, undermines the impact of broader regulatory policy, and inhibits competition in the financial services market,

[2] The Payment Strategy Forums, PSR https://www.psr.org.uk/psr-focus/payments-strategy-forum. In particular:https://consultation.paymentsforum.uk/sites/default/files/documents/Payments%20Strategy%20Forum%20-%20Design%20Principles.pdf

[3] Financial Capability Survey, Money Advice Service, 2015

as well as hindering the achievement of wider consumer and social outcomes. If we are to realise the full potential of the payment systems and choices they offer we need to improve financial capability.

Many UK adults (42%) do not describe themselves as being confident managing their money (giving themselves a score of seven or less out of ten) and around half agree that their financial situation makes them anxious or don't see that they themselves can make a difference to their situation. If people don't believe they can make a change for the better or don't consider the benefits outweigh the perceived risks then it is hard for interventions aimed at getting them to share data or change their financial and payments behaviour to succeed.

There may also be additional factors involved in understanding and responding to consumer reluctance to provide access to their data. This could include,

- the interaction between low digital literacy and financial capability.
- Low engagement driven by strong network effects: consumers don't feel they have a meaningful choice in using online platforms, so disengage or simply do not engage with data and privacy questions
- Individual attitudes and behaviours towards privacy and understanding of the value of personal data contrasting with a lack of trust, clarity and awareness of how providers will use this.

Such behavioural barriers may need a range of different interventions and types of communication to be overcome. They cannot be easily fixed through awareness raising. We believe, therefore it therefore imperative, that the payments industry, as outlined in the Forums' original principles, engages with the Financial Capability Strategy for the UK[4], which can bring together organisations from the financial services sector, government and the third sector to collaborate to improve consumer capability and engagement with their money.

Communication with Consumers

There is an imperative need to ensure that consumers fully understand the implications of sharing their data – both by active and passive consent, particularly where this has the potential to lead to price differentiation for different consumers. In instance where data will flow across different markets, consumers should be made aware that firms, especially those that operate in more than one market, may collect data from one market and use it in another.

Communication of such complexity across markets will require an understanding of how peoples' attitudes, motivations and beliefs interact in their environments. In its evidence review of smarter consumer communications[5], the FCA highlighted good practice for communications that helps people understand, engage and make decisions about their financial matters. This included presenting the most important information within the headings as it is often missed in the body of the text and presenting information

[4] The Financial Capability Strategy for the UK, https://www.fincap.org.uk/

[5] Financial Conduct Authority (2015), 'Smarter consumer communications', DP15/5, 25 June, accessed 3 August 2015. https://www.fca.org.uk/publication/discussion/dp15-05-smarter-consumer-communications.pdf

incrementally to design for cognitive overload. We would strongly encourage firms to take on board the findings from this review when eliciting consent for data.

The Open Banking Implementation Entity (OBIE)[6] has recognised the importance of consistent and effective messaging to consumers on new concepts. To support consumer understanding of the products enabled by the revised Payment Services Directive and Open Banking standards, the OBIE is working with banks, building societies and third-party providers on key consumer messages. Where messages are not competitive in nature, such as in helping consumers understand how to safely share their financial transaction data, collaboration in designing communications can deliver clear benefits to consumers and is also likely to be aligned with the commercial interests of financial services firms.

We support efforts to reduce the complexity of language used to describe and explain data. It is important that the impact of language is tested with consumers to ensure it conveys the desired messages and has the intended impacts. For instance, to support our work on the consumer retirement journey we commissioned ComRes to conduct research into pensions language[7]. This found that it is important that the language used is accessible and not just simple, as terms can sometimes be too unprofessional for a serious topic and that terms and phrases used need to address particular points of concern to avoid consumers distrusting and ultimately disregarding the information provided. As our recent work with OBIE has recognised, there is an intrinsic value to consumers in the use of more consistent language across industry, government and the third sector in building trust and confidence.

At MAS we work to ensure consumers understand and effectively engage with all aspects of financial services. We know that consumers are not a homogenous group and understanding the nuances of decision making are key to effective communication. Using our knowledge of, and networks within the financial capability, we would welcome the opportunity to work with the payment industry to effectively engage with consumers.

With regards,

[redacted]

[6] OBIE https://www.openbanking.org.uk/about-us/

[7] Pension Dashboard Research, A report by ComRes for MAS, May 2017 https://masassets.blob.core.windows.net/cms/files/000/000/868/original/MAS_Consumer_Research_Pensions_Dashboard_Research_v2.pdf

Nationwide Building Society (NBS)

PSR: Data in the Payments Industry Discussion Paper 18/1 response from Nationwide Building Society

September 2018

Executive Summary

We, Nationwide Building Society, appreciate the increasing part that data plays today in our members lives' and in many industry initiatives – including the movement to ISO 20022, development of Enhanced Data, the New Payments Architecture (NPA) and fighting financial crime. We welcome the opportunity to comment on this consultation document and to support the PSR in its consideration of 'Data in the Payments Industry' as this takes shape.

As an organisation owned by and run for the benefit of our members, in developing our responses we have considered both the potential 'member benefit' of innovation opportunities offered and our responsibility to listen and respond to our member needs such as, to be confident in the security of their data and respect of their data privacy rights.

In considering potential actions for data in the payments industry we would encourage further thought on the topic of vulnerable consumers. Vulnerability takes many forms including of relevance to this discussion, financial and digital literacy. We consider there is a case for a consistency of service regarding vulnerability across regulated sectors and would urge a joined-up approach between regulators. We believe all market participants, large and small, challengers and more established participants, should share responsibility in making adequate flexible measures for vulnerable customers.

Nationwide members can engage by branch, telephone, digitally and for vulnerable consumers a Specialist Support Service.

Main comments:

Need for Greater Reflection of Data Protection Legislation in Proposals

We appreciate that as a discussion paper, this is aimed at readers with a wide range of understanding and are aware of the detailed legal response made by UK Finance so do not intend to dwell on legal points here. Going forward, however, it is very important that the PSR take the legal position clearly into account when considering asking the New Payment Systems Operator (NPSO) or card schemes to share global transaction data sets with providers.

Particularly:

- The data subject's rights and the respective responsibilities of data processors and controllers;
- The need for a legal basis on which the data in different use cases would be processed;
- Whether it is transparent and fair to share customers' personal data with unknown providers – who could be 'data analytic firms, innovators or future overlay service providers' quoting paragraph 6.32 - for undefined competition and innovation purposes?

We would agree with UK Finance that if the PSR is considering requiring PSPs to update their terms and conditions and data privacy notices to enable the wide sharing of customer data with other providers for the purposes of competition and innovation, this is unlikely to meet the requirements of GDPR. We would not support the NPSO being required to enable the sharing of global datasets on this basis.

We are supportive of the PSR's proposal to engage with the ICO, and industry to help develop clear understanding of when payments data can and cannot be shared. This will be especially useful in the development of Data Protection Impact Assessments (DPIAs) for each use case as this work develops.

Definition of Clear Use Cases

The paper describes payment data, how it is derived and the drivers which are increasing the production of this. It does not however, clearly specify use cases with which to evaluate – including from a customer perspective or in a legal sense

- why customer personal data should be shared via access to the New Payments Architecture (NPA) for general competition and innovation purposes – particularly over what is possible today through customer consented Open Banking access (e.g. the Money Dashboard case study in Box A). We would encourage the development of such use cases to enable comment.

However, we do believe that access to the global transaction data held within the central infrastructure could be utilised to help prevent financial crime – as per the intent of the NPA where we understand some level of access would be necessary to enable the Transaction Data Analytics (TDA) solution. More information on the detailed solution design, DPIA, registration and accreditation of solution providers etc. would be welcomed to enable full comment.

For other potential 'overlay services', the legal basis for the processing of customer data to share with other providers will need to be understood for each use case. Greater definition of use cases, their objectives, benefits, the data to be shared (including the degree of aggregation and/or anonymisation), the providers etc., will need to be developed for each 'overlay' service to the NPA.

It is possible that overlay service use cases exist that would not necessitate the sharing of global data sets within the central infrastructure. For example, it is not clear this is necessary for Confirmation of Payee.

To ensure the correct level of security and governance for each use case we would expect central assurance – including through regulation, as appropriate - of all providers which have access to the global data sets.

In addition to the legal implications, the security and operational impact of having a number of different parties – as envisaged under the Transaction Data Analytics - accessing the NPA will need to be understood. As will the impact of capturing, storing, retrieving and presenting enhanced data and processing much larger payment messages.

There is a need to define the business case for the industry and Nationwide to invest in developing these capabilities.

We understand however, that the NPA Request for Proposal will need to enable access to global data sets for proven use cases in the future.

End User Education

We believe that campaigns to help customers have trust in new overlay services would best be service specific to enable tailoring of customer messaging for different uses. The method of conducting these campaigns – including participants and funding - would be most effectively decided per initiative.

We would, however, encourage co-ordinated consumer awareness messaging to enable consistent messaging – such as with the Take 5 campaign. There will be a need for relevant participants to agree how to clearly align messages to build consumers' trust to share their data in different use cases with those messages not to share data. We need to ensure we are not sowing confusion in consumers' minds.

However, trust may be only one element of why services are not used. Other reasons could include:

- If the overlay service is not perceived to offer benefit. Although a customer may not consciously think in these terms, Nationwide research would suggest that there needs to be a 'value exchange' between the service received and the data shared. A use case needs to fulfil an identifiable need – with a strong one potentially being enough to get customers to engage – for example, with mortgage brokers today.
- Or the customer is simply not interested – including in being online at all. Given the sums financial institutions, government etc. have spent encouraging end users to move online and the training initiatives available both in the community and through PSPs, it must be asked if education campaigns will encourage end users to engage with technology or overcome the technology barriers cited in paragraph 6.22. And if a customer's first move online would be to share financial data? Expectations may need to be managed here.

Detailed responses to the discussion paper questions follow.

1) Do you agree with our assessment of:
   a) the types of data in the payments industry that are relevant for this paper?

We can understand that the definition of 'the totality of information collected by PSPs and other third-party providers in the process of providing core payment data to end users', and 'ancillary data that is often collected as the payment is being processed' would naturally form part of a discussion paper on data in the payments industry. However, the fact that this definition is not fixed (as indicated by the inclusion of the wording 'not limited to') and the range of providers who could possibly access this data for currently undefined purposes makes commenting on some proposals difficult. More definition is required of use cases including data to be shared, providers involved and the legal basis for processing established.

We would also ask for clarification of which definition of personal data is being used in this discussion. We would suggest that the wording in paragraph 4.15 (taken from GDPR and the Data Protection Act 2018) is the correct one to apply. There are instances in the paper where what is categorised as non-personal data is in fact personal data, as it relates to an identified or identifiable individual (i.e. paragraphs 4.25(b), 4.31(b), 4.38(b), 4.42(b) and 4.48(b)). The application of the distinction between personal and non-personal data therefore needs tightening.

The statement at paragraph 4.16 that *"A further classification of personal data is provided under the GDPR which identifies 'special categories of personal data' as 'sensitive' personal data…"*. Is also inaccurate and unnecessarily confusing. GDPR does not use the term 'sensitive' personal data. Moreover, this term would lead to obvious confusion with the concept of 'sensitive payments data' under PSD2. The use of 'sensitive' in this context should be avoided.

We understand from the recent Bank of England consultation that other types of personal data are likely to be included in the Common Credit Message (including the purpose of the payment). The availability of this data and appropriateness of sharing this would also need to be assessed as part of the next steps.

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

Yes. With the exception that the paper does not:

- Consider Direct Debits, although it discusses Direct Credits.
- Represent the position of agency banks.
- Differentiate between the responsibilities of data controllers and data processors. A clear distinction on this point is necessary as a processor cannot share data just because they have it.

The personal data for FPS does not include any 'payment reference information' / text entered in the free text field provided (4.38).

It could be argued that some of the data discussed in Section 4 includes transactional data rather than the strict data needed to route a payment. Given this, much of this data would not necessarily be present in the NPA clearing and settlement layers global data sets, which is important when considering the later questions on access.

   c) the different ways that payments data can be classified?

Generally, the classifications in the consultation are appropriate other than personal data, as set out above (although, corporate data can also include personal data of its directors etc). We would also add that although not payments data as reflected in the consultation, in the future there could be data which is linked to a payment transaction (i.e. enhanced data) and not collected in the traditional ways discussed in the consultation.

Please also see our response to Question 1.

2) 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?

In the future business models, it is possible that data linked to payments (i.e. enhanced data) could generate value for end users and new players (e.g. data warehouse providers). Although this would need to be understood.

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

Aggregated global data (non-personal) is used by PSPs and PSOs for forecasting – including for operational resilience / capacity purposes. Additionally, aggregated global data sets (non-personal) are used for internal management intelligence and industry reporting and for the verification of payment system operator and the PSR annual fees.

Most PSOs already share aggregated volumes and values.

4) **Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?**

More instances of overlay services use cases will help answer this question going forward. Taking as a parallel though, it is too early in the roll-out of PSD2 and Open Banking to determine who will be the 'winners' of consumer trust. And today no overlay services exist but when Confirmation of Payee is launched, customer trust will be necessary for all PSPs.

Therefore, obtaining customer trust through the secure and regulatory compliant handling of customer data will be a key issue for all brands.

Nationwide Open Banking research shows that for the UK population – data privacy concerns, suspicions about how their data will be used and reassurance on value proposition of a particular use case are key factors in adoption.

Therefore, we concur that many customers are concerned about data privacy and how their payments and ancillary data is used. This is natural as they have been educated for many years to protect their financial data and there are often media stories of unfortunate results stemming from data loss. See our comment below on alignment on consumer messaging.

But trust may be just one element of reluctance to share – customers may not perceive the benefit of enabling access to their data or simply not be interested in the service offered.

We do not agree that if somebody does not want to engage with technology that this is necessarily a complete barrier to innovation and competition. After all, the end-user's ability to engage digitally would not totally restrict them from benefitting from the overlay services. For example, Confirmation of Payee could possibly be utilised in branch.

We do however believe that online engagement offers customer benefits and that in many cases the sharing of customer data will be customer lead and use case driven.

Consumer Campaigns

We are supportive of campaigns to enable customers to make informed decisions about data sharing and consents on a case-by-case basis.

Given the myriad of uses for which this data could be used and regulations and mitigations, as intimated in the consultation we do not think it would be possible to achieve the clarity of messaging to encourage people to share their payments data through a single customer education campaign. Instead, for the overlay services discussed in section 6.14 – 6.29, we believe that balanced communication to understand these services and how to engage with these would best be done as part of the launch/usage messaging for either service.

- Confirmation of Payee – is likely to be an opt-out service – meaning most payees will be automatically registered to achieve a ubiquitous service through as full a participation as possible to address the detriments of accidentally and maliciously misdirected payments. We agree however, there will be a need for end users to understand what is being assured by this service. Therefore, information on the ways in which their data will be used and

other messages to help prevent accidentally misdirected payments and APP scams would best be designed and given at the time based on the final solution.

- Request to Pay - end users are likely to participate in this on a voluntary basis – where raising customer awareness could be important. Participation will be use case driven. The enhanced data in this case could eventually take the form of an invoice or link to a customer utility company account attached to the request and information which may be contained in a response to the request (e.g. a request for payment extension) or an acknowledgement of payment. The solution should in itself be secure enough and satisfy an end user need to encourage use. However, customer communications to understand the service and again how best to engage with it will best be determined when its design is finalised.

We would still encourage opportunities for co-ordinated messaging to be explored – with Open Banking and the UK Finance, Financial Crime messaging – and draw on the expertise of the Money Advice Service as appropriate etc.

Indeed, consumer awareness messaging will need to be properly co-ordinated across the sector to enable consistent messaging – such as with the Take 5 campaign. There will be a need for relevant participants to agree how to clearly align messages to build consumers' trust to share their data with those messages not to share data. We need to ensure we are not sowing confusion in consumers' minds.

Over time, as these overlay services become more mature and what is being assured is clearly defined – i.e. accreditation of vendors, adherence to rules - consideration of a quality kite mark could take place.

5) In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

A definition of the level of aggregation in a 'global transaction data' would be helpful to answer this question.

We believe that access to the global transaction data held within the central infrastructure could be utilised to prevent financial crime – as per the intent of the NPA where we understood some level of access would be necessary for the payments Transaction Data Analytics (TDA) solution.

We also understand that the Bank of England and ONS may wish to see data from payment systems which will be facilitated by the Common Credit Message for statistical purposes.

More generally however, a greater amount of data on a customer could enable the PSPs to tailor or personalise their customer offerings. How overlay services would help in this though would require further clarity as PSPs can already today access (with a customer's permission) their financial records through Open Banking (covering all payment types – including card and cash withdrawals). As commented above additionally, the legal basis for processing this data for this purpose would need to be established. A comparison is made in paragraph 6.42 of PSD2 and Open Banking – in both these cases the customer must agree to the data being shared.

Therefore, a greater definition of use cases is needed to comment on this fully but currently we would not agree access to the global data sets in the NPA is necessary for development of – non-anti-financial crime - competitive overlay services.

For example, we don't believe that access to global data sets on the central infrastructure will necessarily impact on the developing overlay services:

- PSPs will make information about their payees available as part of Confirmation of Payee – separate from the global transaction data in the NPA;
- Request to Pay is a messaging system (in effect a bill) and payees (corporates, consumers etc.) could have the option to add data to the request prior to the initiation of a payment – separate from the data held in the NPA

In some cases, such as the Transaction Data Analytics, a fair funding model would also be necessary to recognise the increasing plurality of the payments market and the costs of capturing, processing and storing this data.

6) **What models could the NPSO introduce to allow PSPs to get access to global datasets?**

We believe that access to the global data sets in the NPA could be facilitated through APIs and leveraging the Open Banking Infrastructure.

We understand that a capacity to share data may need to be built into the RFP for the New Payments Architecture.

A commercial model will need to be developed to recognise the investment and ongoing PSP costs involved in the capture, storage etc of data.

We would expect central assurance – including regulation as appropriate - of all participants which have access to the global data sets to ensure the correct level of governance per use case.

7) **Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?**

As above, a definition of global transaction data and use cases would be useful to answer this question.

Most PSOs already publish some aggregated data today and we would support greater sharing of data to help tackle financial crime (where legally possible and economically effective).

But we would not support wider sharing by all PSOs. Again, we believe that the sharing of data will depend on the actual data being shared and the legal basis for processing amongst other things - which will be use case / overlay service driven. Therefore, access should be on the basis of overlay service / use case not a generic requirement

8) **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?**

More information would be needed on the Transaction Data Analytics solution use case to understand the GDPR position of this solution. However, it is likely that the basis of processing for the transaction data analysis solution would be legitimate interest or legal obligation rather than 'consent'.

We would encourage consideration of the wider application of the SARS regime in this context however.

More generally for the TDA, there will be a need to:

- Understand implementation costs and develop a fair funding and operating commercial model to recognise the costs incurred.
- Develop a governance model considering:
  - Which parties would manage the customer interaction in case of queries and subject rights requests;
  - Which party is responsible for the accuracy of the data;
  - How customer protection and disputes would be handled; and
  - Central assurance – including regulation - of providers with access to global data sets.

9) **Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?**

No.

10) **Are there other payments data-related issues that could, directly or indirectly, affect our objectives?**

We are supportive of the PSR's proposal to engage with the ICO and industry, to help develop clear understanding of when payments data can and cannot be shared. Including, through the development of DPIAs for different use cases

as this work develops. A lack of clarity can delay the development of industry solutions such as Confirmation of Payee – and the PSR's drive to combat Authorised Push Payment scams.

We recognise that Enhanced Data can provide a great deal of innovation opportunities. However, when commenting on the Payment Strategy Forum Enhanced Data solution in the 2017 consultation, we identified a number of operational, compliance and risk issues and think these would be worth raising again here. Including:

- The need to understand the end-to-end enhanced data journey to enable clear specifications of data management responsibilities so that a workable risk and control model, with appropriate standards, can be developed. This would need to consider:
    - How to maintain data quality and data accuracy and responsibility for these.
    - Any cyber-security risks of having embedded data in a payment journey – e.g. a URL. If this extra data included links to external data sources - security standards would be necessary to ensure that the payments couldn't be used to transmit malicious software (e.g. as a Trojan Horse for viruses) to the receiver of the data and potentially other parties. Responsibility for screening would need to be agreed.
    - The risk that data is transmitted which is illegal, breached sanctions legislation etc. A mechanism would be needed to detect where Enhanced Data may indicate AML, terrorist financing or sanction breaches.
    - Any data protection issues regarding the sharing of the data with end users and controlling this. For instance, how would the consumer receive appropriate enhanced data? How would controls be managed on a joint account – both for payments out and payments in? How would GDPR subject rights be dealt with?
    - Issues about IP protection. For instance, who owns the data/intellectual property of any attached enhanced data e.g. contract terms or a warranty. In some cases, this ownership may not be the data subject, controller or processor.
- There will be a need for data storage standards where Enhanced Data is stored separate to the payment which will need to cover:
    - How the data should be shared in compliance with data protection and privacy regulations?
    - How long would the data be stored (both practically and legally)?
    - In what format (e.g. static or 'live')?
    - How would it be managed, accessed, stored, protected etc. etc.?
    - Data and IP ownership.
    - How GDPR, AML, sanctions or anti-terrorist risks are managed.

Two other factors which must be considered in the drive to capture and share data are:

- Cost – to capture, store, retrieve, pass on and as appropriate present additional data in potentially much larger messages. These costs would be on channels, payment and other systems, processes etc. There would also be costs to end users to adopt these; and
- Need to understand operational impact – including scaling, complexity of processing of potentially much larger messages through PSPs and PSO / NPA systems. The extra quantity of material being passed around the networks between participants and the need to store what could be large volumes of information could affect all parties involved in the payment journey. Additionally, the impact of extra data and data access on robustness of performance of financial transaction processing should be factored into the NPA design.

All of the factors above apply to Enhanced Data – without this being shared through wider access to the global datasets in the NPA.

New Payment System Operator (NPSO) (now Pay.UK)

NPSO
New Payment System Operator

[redacted]

07 September 2018

NPSO RESPONSE: PSR DISCUSSION PAPER – DATA IN PAYMENTS

Thank you for giving the New Payment System Operator (NPSO) the opportunity to respond to the PSR Discussion Paper – Data in Payments. We would be happy to meet with PSR to discuss our response in more detail.

The potential policy issues identified in your discussion paper are items we are considering through the scoping of our role as a Market Catalyst and the design of the New Payments Architecture. In both of these activities we will need to satisfy ourselves the final outcome delivers against our Strategic Objectives in a balanced way. This will take time to analyse the various options and we feel it appropriate to be given the time to do this. We believe the outcome of the stakeholder responses to this discussion paper could support our own thinking in these areas and would appreciate working with the PSR to understand this in more detail.

We believe the creation of the NPSO and implementation of a New Payments Architecture are essential steps towards a generational change in UK payments. Our vision for the future is to enable a vibrant UK economy with the NPSO as the leading retail payment authority in the UK, delivering the best in class payment infrastructure and standards for the benefit of people everywhere. We are focused on creating a payments environment that delivers choice to the meet the needs of end users, both now and in the future.

[redacted]

RESPONSE TO QUESTIONS

We have limited responses to those related to potential PSR policy issues due to alignment with the role of the NPSO.

Question 4: Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

Yes, we agree that a mismatch could potentially undermine innovation and competition as it could lead to consumers lacking trusting in new services from TPP's and therefore not using these services – damaging innovation and competition. This is because of the lack of familiarity with new (and potentially unknown) brands.

As the discussion paper highlights there are a potentially a range of actions to address this. As the NPSO begins to consider the scope of our role, in the context of the New Payments Architecture (NPA), it is clear that appropriate actions to engender trust and the extent of the NPSO's intervention will be needed to be determined how they further our strategic objectives. We believe it is important not to predetermine these without undergoing a proper analysis. At a high level we believe the NPSO can help engender trust in the ecosystem for which we are responsible through two key roles.

1: The development, implementation and operation of an appropriate assurance regime. This will enable NPSO, across the ecosystem for which we are responsible, to maintain and protect the quality, security and trust of this ecosystem. We are currently in the process of developing a regime in the context of the NPA and we will continue to engage with the PSR as this work progresses.

2: NPSO acting as a market catalyst. As the discussion paper highlights the Payments Strategy Forum envisaged a Market Catalyst Role for the NPSO. We are in the process of defining this role and are discussing this with the PSR.

The discussion paper highlights campaigns to educate consumers about how their data will be used and suggests these form part of the NPSO's Market Catalyst role. Although education campaigns can be productive in the correct circumstances - see Annex A for a CASS case study - it should be noted these can require a significant amount of resource and budget, therefore should only be undertaken if supported by a robust Business Case.

It is also the view of our End User Advisory Council that product / service design can be more effective than education at addressing issues of trust and we are seeing that view supported by our stakeholder research on the Confirmation of Payee proposition. For example clear messaging built into consumer interfaces will engender greater trust than large scale central education campaigns. We will be in a position to share this research with the PSR shortly.

Question 5: In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

We agree that making global transaction data available could help providers to develop overlay services. It is critical though that access to the data has the appropriate legal and technical controls in place. We set out some of the legal considerations under question 8.

We acknowledge that there are some technical access restrictions for third party access to global transaction data within our systems. As part of the design and procurement phase for the NPA we are exploring options for how the central infrastructure provider for the clearing and settlement layer can facilitate the safe and efficient sharing of global payments data with service providers. As highlighted in you discussion paper this could be through secure open access APIs.

We would ask than rather than place an action on the NPSO at this stage we continue to engage with the PSR as the design of the NPA core clearing and settlement layer develops. Through this engagement we will be able to demonstrate how we are meeting your requirements.

Question 6: What models could the NPSO introduce to allow PSPs to get access to global datasets?

There is value in the ability to analyse payments data to identify, and therefore reduce, fraudulent activity or patterns of activity. NPSO could consider a number of models for PSPs – or any one other designated authority - to have access to “Global Transaction Data”, but clearly this could only happen if such access complied with the GDPR obligations we set out under question 8.

Question 7: Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

In principle the requirements to provide access to global transaction data should be applied equally across all regulated PSOs. This is worth considering in the context of industry-wide fraud and anti-money laundering (AML) prevention measures, where the final payment could be settled in a different payment system from where it originated.

Question 8: 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?

Our initial thoughts on this question are set out below. This can only reflect our very early thinking, and our final view will be tempered by the factual situation that arises.

The effect of GDPR will depend on the definition of "Global Transaction Data" – if this means the aggregate of the data for a specific payments system (the 'totality'), there are no issues provided data's anonymisation or pseudonymisation (See Annex B for definitions) be guaranteed, including by eliminating identification of transaction patterns that may allow PSPs to identify an individual from its unique purchasing habits if an individual customer's personal data (e.g. sort code and account number) is involved, there may indeed be the perception of a tension between the development of industry-wide transaction data analysis tools, and the customer's data protection rights. This may also be perceived as a step towards the programmed end of banking secrecy, which in some countries is protected institutionally. Cross-border payments might have to be excluded from access to "Global Transaction Data" for that reason.

Matters are made even more complicated by the contractual arrangements a customer has with their PSP, although it is almost certain that certain consents will have been given to allow the PSP to use a customer's information for limited banking and security purposes. In addition, PSP's are likely to provide in their Privacy Notices that a customer's information may be used to prevent or detect crime including fraud and financial crime, e.g. financing for terrorism and human trafficking. The PSP would say that this was within their "legitimate interests" (per Article 6. 1 (f) GDPR). However this legal ground may be challenged by consumers who will argue "consent" is the only option regarding access to private and personal transactions by third parties not mandated by a judicial authority on an ad-hoc basis.

In addition to the above, there is the specific provision in Part 3 of the Data Protection Act 2018 which makes provision for the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive. A PSP *per se* is not defined as a ”competent authority” in Schedule 7 Data Protection Act 2018 but may certainly be regarded as acting for ”law enforcement purposes” as the purposes are the prevention, investigation, or detection of criminal offences, etc. (per Section 31 DPA).

The very specific obligations for automated individual decision making (including profiling) set out in Article 22 GDPR, would need to be complied with. This includes consideration of the safeguards in Section 14 Data Protection Act 2018, and any “explicit consent” of the individual customer for such processing.

There is a need to ensure that the DP Principles are followed (Article 5 GDPR) and of course make sure personal data is processed lawfully (Article 6 GDPR).

Finally, the feasibility of pseudonymisation techniques to remove personal identifiers from the individual’s payments data needs to be considered (as set out above).

Question 9: Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

We have not responded to this question.

Question 10: Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

It is important that data protection is properly addressed in the design of a system, its data, processes, procedures and the training of its administrators. The collection of summary data could enable Payment System Operators to understand customer behaviour and trends. This could also potentially be used to support the NPSO’s Market Catalyst role by forecasting future payment needs and requirements that will drive competition and open access

A further key consideration is to define what incentives there are for the payment initiator to provide accurate data. For example, international payments are rejected if the sender and recipient data are not provided.

Regulating data will encourage a shift in behaviour for certain groups of consumers. It may mean that if electronic services are more heavily scrutinised that criminals and tax evaders may return to using cash or other means.

ANNEX A – CASS Case Study for Building Trust

The approach CASS identified was to develop a 'partner brand'. The theory, supported by evidence, suggested the development of a 'trusted' supplier mark that Participants who meet certain accreditation guidelines were allowed to use. Of course this requires policing to ensure only the legitimate organisations are using them (similar to how ATOL protection works). However, for a successful 'partner brand' a centralised awareness campaign, supported by trusted entities using the partner brand, was needed to take place to raise awareness to end-users of the 'brand' and its role. This ensured that when they see the mark, it does build trust. Without any awareness of the partner brand, when end-users see the partner brand, it won't mean anything.

For the successful launch Current Account Switch Service, it was critical that consumers and SMEs had trust in the Service. As required by the Independent Commission on Banking (ICB) the purpose of the implementation of the Current Account Switch Service, was to remove any real or perceived barriers to switching, and therefore contribute to a more effective market. A critical part of the product proposition was that the Service would be backed by a 'Guarantee' which would ensure if anything went wrong with the switch, consumers would be protected. Therefore to define and design the aspects of the Guarantee, the Payments Council launched research in 2012 with independent research agency, the Nursery, to understand the features, and importantly for the question asked here, relating to how trust within the Guarantee is built.

The critical question for the Service was who should be backing the Guarantee. The Nursery research showed that a 'Guarantee' is only as credible as the guarantor. People will buy into an unknown brand if it is guaranteed by a trusted retailor (or vice versa), but in any situation where there is a likelihood of the guarantee needing to be invoked, trusting the organisation offering it essential for it to have any value. However to complicate this there were a few challenges and contradictions:

- Firstly, it is extremely hard for an unknown brand to hold credibility with the public, and organisations at the time such as the Payments Council had little dealings with the public and therefore consumers have not heard of, and had no interest in these inter-bank bodies.
- However, having the Guarantee backed by the banks was not the simple solution either as may consumers stated that financial institutions as a 'concept' are no longer widely trusted. Moreover, there is the common view that people do not trust 'banking' but they do trust 'their bank'.

- However, despite this, many respondents felt that 'logistically' the banks and building societies themselves are the only organisations which are deemed to have the capabilities of making and honouring a Guarantee, particularly where any 'reimbursement' was involved. People did not want to have to 'activate' a Guarantee through a third party.
- Additionally, it was clear the importance of the 'industry' as a whole uniting which supported in building trust.

Due to these various contradictions in people not wanting the Guarantee to be provided entirely by the banks, nor entirely by an independent organisation, the concept of the 'Current Account Switch Service' partner brand was developed. This solution provided an 'independent' brand, supported by a Trustmark Logo, which worked with the Banks and Building Societies to provide the Guarantee, which was ubiquitous across the industry. However, the successful launch of the 'partner brand' relied on a high spend integrated communications campaign which would raise awareness of the Service. There are three prongs to this communications strategy:

- **Paid Media:** A centralised independent marketing campaign which raised awareness of the Service and the Trustmark, explaining the process and benefits of using the Service. This included high reach broadcast channels. The original launch campaign for CASS was a £2.5 million media spend.
- **Owned Media:** The Paid Media strategy is supported by the Banks and Building societies being mandated to use the Trustmark within all of their current account acquisition advertising, websites, branch collateral and on branch windows. This is managed through a set of Brand Guidelines all Participants must agree to adhere to when signing up to be a part of the Service. On average per year, Participants spend 10x more on paid advertising than the central service does, and therefore the exposure of the Trustmark in Participant content, provides a significant halo effect around the central campaign. Neither Paid or Owned Media will work without the other. If there is not already an awareness of the Trustmark built through the Paid campaign ,then when consumer see it on Bank materials, it won't mean anything. And, if consumers only see it in paid media, and not supported by these well-known trusted entities, it won't be as trusted.
- **Earned Media:** Ongoing PR and stakeholder engagement to emphasise the benefits of the service and its impact. This ensures that key audiences are clear of the role of CASS, understand its success and are fully informed about progress – showing momentum and positive steps taken. This includes organisations who are key in the customers switching journeys such as Price Comparison Websites.

ANNEX B – ANONYMISATION AND PSEUDONYMISATION

Anonymisation

GDPR does not give a direct definition of "anonymization". However, GDPR does not apply to anonymous information which is, in essence, non-personal data, and defined as "information which does not relate to an identified or identifiable person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".

The Article 29 WP explained that "to anonymise any data an important factor is that the processing must be irreversible".

Pseudonymisation

GDPR states that pseudonymisation means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". **Pseudonymisation differs from anonymisation in the fact that pseudonymisation can be reversed.** Pseudonymisation is linked to the risk of unauthorised reversal of pseudonymisation.

This is why technical and organisational measures are key to the protection of individual rights of natural persons. Recital 26 adds "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".

Open Rights Group (ORG)

Open Rights Group Response to PSR Discussion Paper: Data in the Payments Industry

Who We Are:

Our mission is to support the development of a healthy, vibrant and fair society, which allows individuals and businesses to live and flourish in the digital age. We do this by working to protect and extend human rights and civil liberties which history tells us are often overlooked or eroded during periods of rapid change.

Our activities include public education and awareness raising, constructive engagement in policy making using our expert research, campaigning and where necessary legal interventions.

We have offices in London and Edinburgh. We have 9 members of staff and we are funded by regular donations from over 3,000 supporters, grants, trusts and corporate supporters. We have ten local activist groups across the UK including Scotland, Wales, England and Northern Ireland.

Our Response:

We welcome the Payments Systems Regulator's consultation.

Our primary concern is that the paper assumes data sharing is inevitable, whilst ignoring the risk to the consumer.

There should be a way for consumers to transact without their data being used for anything other than the purposes of making specific payments.

This is clearly equivocal to using cash as a payment method; and the move to a digital-only model should not entail the compulsory use of data.

With regard to the regulation issue, the ICO is an after the event regulator, and therefore we suggest that the PSR should regulate to ensure that consumers who choose to can opt-out of having their data processed for any purpose other than specific payment transactions (and associated anti-fraud purposes) much like the Telephone Preference Service, but for payment data.

Open Rights Group

[redacted]

Pinsent Masons

Pinsent Masons Consultation Response

PSR – Data in the Payments Industry

As an international law firm we advise on many aspects of the use of data in the context of payment services and systems. Our response below is made on the basis of our understanding of the opportunities and challenges presented to a wide range of clients.

Contact details:

1. Do you agree with our assessment of:

A. the types of data in the payments industry that are relevant for this paper?

We agree that it is important to highlight the value and efficiencies that may be gained through the use of data relating to both core payments processing activities and locations, payment channels, devices and frequencies of use and other forms of ancillary data.

B. the types of data collected by different entities in the industry?

No comment.

C. the different ways that payments data can be classified?

We agree with the four categories set out in 4.13. However, we suggest that more context be provided in order to highlight the importance of data classification.

Data classification processes are key to achieving a number of important objectives for all payment service providers and other market participants. These objectives include mitigating risks relating to the misuse of personal data, cyber, fraud and financial crime. Data classification is also relevant to improving efficiency by reducing duplication and in simplifying data tracking and searching processes. Effective data classification can also be an important means of improving confidentiality, integrity and availability of data.

We recommend that the PSR consider mapping regulatory requirements against different industry approaches taken to data classification. This will assist market participants understand the extent to which their current processes and controls reflect regulatory expectations. For example, payment service providers would benefit from a PSR view on best practice towards confidentiality classification – in which contexts will broad classifications based on 'public, private and restricted' be sufficient to achieve regulatory

compliance aims and when will more granular classification be required? Further analysis and mapping of regulatory requirements against these key data concepts would benefit all market participants.

2. 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 be used to generate benefits for payments system participants? Are there any other points where data could generate value?

We highlight three areas in which payments data can be used to generate value - in:

- addressing credit risk concerns of lenders in the context of the unbanked and underbanked;
- enabling the digital economy through portable identity data; and
- addressing and preventing fraud.

Addressing credit risk

While we agree with the approach that been taken in section 5, we also suggest that the PSR give greater attention to specific use cases for payments data in new or tailored products.

Payments data, when combined with other forms of alternative data, such as utility usage and rental history, has been recognised as potential source for addressing credit risk concerns banks and other lenders have in respect of the unbanked, underbanked and those that have thin credit files. Further market research into the extent to which regulatory frameworks may be adapted to enable the availability of transaction data to address credit risk concerns would benefit both market participants and payment service users.

Enabling digital identities

Over the last few years there have been a number of government, regulatory and private sector-led initiatives have considered the role of payments data in enabling consumers and businesses to engage online. Many of these initiatives have stagnated. Others that have succeeded have been heavily criticised due to concerns about the user journey and frustration experienced in balancing data sharing and cyber, identity theft and other financial crime risks against the benefits of enabling frictionless access to financial services.

There is a clear role for financial services providers to enable trusted use of payments data for the purposes of identifying, verifying and authenticating individuals and businesses. Input from the PSR in helping the sector to gain a more comprehensive understanding of the scope of the regulatory framework in which identity data may be used, including in respect of anti money laundering, data protection and the EU-wide eIDAS regime would be helpful.

Addressing fraud risk and ensuring a balance

We agree with your comments regarding the usefulness of payments data in preventing and detecting fraud. However, we also raise the caution that if appropriate controls are not put in place around open global datasets datasets, there is a risk that risk may increase. This risk remains a key threat to financial stability and user (both system participant and consumer) confidence, particularly following recent attacks on financial institutions that have resulted in data breaches, fraud and disruption. To take an example, a global data set may

reveal which channels (e.g. which system participant or type of payment) is most susceptible to fraud and whilst this has value within a closed group, it presents a risk if made more widely available such that fraudsters could benefit from this intelligence (particularly if the risk is not readily capable of being resolved). This tangible risk must, in our view, be very carefully balanced against less tangible innovation opportunities to avoid the wrong outcomes for users.

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

You highlight that organisations can benefit from using payments data. However, this section would provide greater insight into the opportunities and challenges in respect of the use of payments data if it provided more detail as to the underlying legal structures which govern the use of payments data.

In particular, just because an organisation holds significant levels of data, it does not mean that it is able to use that data to commercial ends. We would typically see infrastructure providers, and payment system operators, being highly limited in how they are able to use the data that they hold or are the guardian of – they would be under contractual restrictions (under system participation agreements) and wider legal duties (including under data protection legislation and wider criminal law, and civil/public law duties). Control over how data is used is often reserved to a material extent to the system participants (although this varies between payment systems).

4. Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the new provision of data based overlay services? If so, how can this be addresses? Which parties should be involved?

We agree with the broad notion that a loss of consumer trust can harm innovation. However, we challenge whether the discussion should be framed to focus primarily on 'trust in established brands versus trust in new brands'. More consideration could be given to key underlying causes including the extent to which customer redress, dispute resolution and access to compensation funds are understood. Customer trust will only be enhanced if they are given greater clarity as to the extent to which they are taking a financial risk in using a third party provider, together with transparency regarding how their personal data is being processed and kept secure. Without greater clarity and transparency many customers will assume that the risk they are taking may be greater than it is. We recommend engagement with the ICO to consider this more fully how to achieve transparency, as well as encouraging the publication of data protection impact assessments (in abridged form to avoid disclosing any confidential information). It is also worth noting that the levels of trust will be constantly evolving as uses of the end user data and the technology being used to analyse that data will be constantly developing – the trust will be at risk where there is a delta between what consumers have been told is happening to their data v. what has actually been enabled through innovation. While both the established brands and third party providers will need to ensure that the transparency assessment keeps pace with innovation, this should not in and of itself harm innovation and competition.

5. In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

We again highlight the risks that could arise as a result of creating and holding global transaction data sets within a central infrastructure. More attention should be given to the extent to which centralisation of this resource is necessary in order to enable real-time access or whether alternative storage mechanisms could be used.

7. Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

Our view is that this needs careful cost benefit analysis - with the risk (e.g. around fraud) forming part of this analysis. Whilst technology has advanced, and the costs of storage and processing have reduced and will continue to reduce, this is a significant technology and business / communication project that is complex and costly - it should not be underestimated. Equally, the opportunity for those other than the incumbent infrastructure providers to deliver upon such a project should not be overstated.

8. 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?

We suggest that the PSR make efforts to clarify the role of consent in this context. In our experience, there is a great amount of misunderstanding in respect of the role of consent in the use of data by financial institutions and payment service providers. Consent is one of a number of legal grounds which can form the basis for data processing activities. Other bases on which data may be processed include circumstances where it is necessary for compliance with a legal obligation and where the purpose of the processing falls within the legitimate interests of the organisation so long as that legitimate interest is not overridden by concerns that it interferes with privacy or other fundamental rights. We recommend that the PSR ensure that guidance provided by Information Commissioner regarding consent is applied specifically to different contexts in which payments data is envisaged as being used. However, to the extent that the data is being shared or processed for the prevention or detection of fraud, provided that such processing and/ or data sharing is necessary and proportionate for that purpose, we do not agree that there is a tension as such. To the extent that any tension does exist, the technical requirements could be developed to take account of the GDPR principle of privacy by design to limit excessive data analysis being carried out that may then fall foul of the data protection requirements because it exceeds what is necessary for the prevention or detection of fraud.

However, in the many circumstances in which consent is relevant in the payments data context, lessons should be taken in respect of the work undertaken by the Open Banking Implementation Entity.

10. Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

We highlight three important challenges:

- the level of fraud, and the capabilities deployed by different participants is a service differentiator – there are likely to be tensions around the scope and capability of centralised fraud systems if any are developed, and centralised fraud prevention also has its own risks (e.g. if a gap is found it may be more readily exploited if it has been set centrally);

- thorough consideration must be given to any competition law implications in connection with the use of global transaction datasets – market share and market segmentation data can be revealed from global transaction datasets, and this is a risk that system operators and participants strive to avoid becoming an issue; and

- analysis of the costs of undertaking an industry wide project of this nature must not be underestimated and, if it is to proceed, it should only be with proper planning having been undertaken before a delivery date is set .

Santander UK

Confidential **3 September 2018**

PSR Discussion Paper: Data in the Payments Industry

Response from Santander UK, plc

Overview

1. Santander UK (hereafter Santander) welcomes the opportunity to input into the Payment System Regulator's (PSR) Discussion Paper on data in the payments industry. The use of data is a critical debate for our customers and firms, and we look forward to working with the PSR as its policy approach to this rapidly evolving space takes shape.

2. Santander has reviewed the PSR's Discussion Paper and attended the industry event to discuss the evolving policy and regulatory approach. This paper sets out our detailed answers to the questions in the Discussion Paper. We would also note the following key points:

    - Of paramount importance to data in the payments industry is ensuring that firms and authorities work together to enhance customer awareness and understanding of how their data is used, or can be used, and always ensuring that there is a consistent approach centring on consumer consent and legitimate interest. This will promote trust and understanding. This aligns with our Group's positioning on the use and access of data – Santander Group differentiates between raw data (that which customers provide) and elaborated data (that which is inferred or derived). We consider that, with regard to elaborated data, consumers should have the right to decide whether or not to share, and on what terms.
    - When personal data is involved (i.e. information from which an individual can be identified directly from the information in question, or indirectly identified from that information in combination with other information), the proposals must be compliant with GDPR/data protection legislation. This includes making sure that individuals are aware of how their personal data will be used, that they are able to exercise their rights as and when required, that there is a lawful basis for the processing and that when/if the lawful basis is consent, that this consent is freely given, auditable and can be withdrawn at any time. We suggest that the PSR engages with the Information Commissioner's Office (ICO) on these discussions.
    - We believe the PSR can take an active role in facilitating Data Workshops on multiple issues covered in the discussion paper, including a forum for the usage of global datasets. We cover this further in our responses to the paper's questions below.
    - Consistent and clear regulation is key. We ask that the regulators and relevant authorities continue to carefully coordinate so that firms have legal and regulatory certainty over the applicability of regulation, and that it is without conflict or contradiction. It is equally important the regulation does not stifle the ability for controlled and well understood innovation and opportunities to be progressed to support a customer-centric future.
    - The activity post this Discussion Paper phase needs to ensure that there is a fair and balanced position created in the Data space – Open Banking, for example, drove a demand for banks to provide data to any relevant authorised entity. This leaves a one-sided picture where the value to customers can be greater enhanced by all parties having access to more rounded information. We consider that any initiative to

open further banks' elaborated data should be symmetrical for other non-bank players, and cross-cutting across all sectors.

- We would also stress that the volume of regulatory demands on the banking sector, in particular stemming from a vast number of payments projects to be implemented, is currently vast and stretches into 2024. The PSR should therefore comprehensively prioritise, cost and coordinate its priorities on any potential actions arising from this discussion paper with HM Treasury, the Bank of England/PRA and the FCA, as well as the Competition and Markets Authority (CMA) with their Open Banking objectives regarding further industry change, as otherwise this could further increase operational risk in the payments sector.

3. Please note that we do not consent to the publication of this response, either in whole or in part, without prior discussion. We would be happy to discuss our comments with the PSR, and can be contacted at santanderregulatoryliaison@santander.co.uk to arrange or with any further queries.

Answers to Consultation Questions

Question 1: Do you agree with our assessment of: (a) the types of data in the payments industry that are relevant for this paper? (b) the types of data collected by different entities in the industry? (c) the different ways that payments data can be classified?

4. A) Santander agrees the core payment services data has been captured within the paper.

5. B) The data outlined within the paper correctly reflects the core elements of the industry payment messages. Santander suggests a delineation, with regard to actively provided data, into that which the consumer is aware they have provided and that which the consumer is not aware they have provided. Santander considers that this builds a clearer picture regarding consent models, counterparty information and sheds light on the reasoning underpinning inferred decisions. Santander considers that there will be an increase in the number of customers who wish to be made aware of the actively or passively provided data to Payment Service Providers (PSPs)/Third Party Providers (TPPs), which ultimately shapes decision-making processes and outcomes. This delineation would also support customer awareness and outcomes.

6. C) The paper captures the various ways in which payments data can be classified.

Question 2: 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 points where data could generate value?

7. Santander agrees the paper highlights the main points of the value chain. Value can be driven primarily by ascertaining the purpose of the transaction, and the way in which the transaction was executed. These two elements can both drive value and insights into what triggered the transaction for the consumer and their resulting behaviours or traits. Generally, data analysis of the payment transaction gives an insight into the purpose of the transaction, based on details including merchant, transaction reference, amount, or Recency Frequency Monetary (RFM) of transaction. Santander emphasises the importance of ancillary information – channel information gives insight into how transactions are completed, and this can generate significant value beyond what the transactional message provides.

8. Santander considers the sale of raw data to be an interesting point: fundamentally, selling raw data requires an incentive. The paper does not specify who is selling the data - whether it is the consumer or PSPs - so these two scenarios must be discussed. As mentioned in responses to question 5 and 6, for PSPs/Payment System Operators (PSOs) to share datasets they must be incentivized. In order to incentivize these parties, collaboration must be achieved and maintained in a bidirectional manner. For example, PSOs selling their data to PSPs/TPPs must be informed as to, first who owns the data (for example we do not believe they own any personal data), and therefore where value sits, and how their data is being used within data products, and Santander considers it logical that the PSR facilitates these discussions (discussed further below). The PSR must look to facilitate Data Workshops between different TPPs/PSPs using PSOs' data. These workshops can focus on the following topic areas and should give clear, insightful ideas into how these problems can be overcome:
    - definition of the problem posed by PSO;
    - dataset description and dictionary being released by PSO;
    - objective of data products within each PSPs/TPPs; and
    - disclosure to agree ethical review of data products (if required).

9. Customer willingness to sell their raw data is variable, and is dependent on a number of factors – generally, it is recognised that customer appetite to sell their raw data is limited. Highlighting immediate benefits to the customer is likely to aid their understanding and decision making process – for example, cases studies could be used to outline the benefits in a readily comprehensible manner. Once the data is sold, the focus shifts to the PSPs/TPPs and the way(s) in which they will use it to drive future value for the customer. Santander considers that the PSR could look to hold confidential data product discussions to review what PSPs/TPPs are currently using their shared data access for and, if they are not providing sufficient value to customers, the PSP or TPP in question is then at risk of losing access to the shared datasets (this discussion model could also be applied to global datasets). Santander considers that security of customers' data is critical, with customers only willing to share or sell their data if they have confidence within the system they are sharing. It is therefore critical that PSPs and TPPs are subject to the same level of regulation with robust controls in place to secure customer data.

Question 3: Have we accurately described the different ways that payments firms are currently using payments data? Are there other uses that we have not included?

10. Santander considers, at a highly simplified level, that the PSR has summarised well the different ways in which payment firms are utilising payments data. Ultimately, it is impossible to map out all elements being utilised across the industry, but Santander would expect the PSR to retain a certain level of awareness of all offensive and defensive data products across the sector. Santander recognises the increasing use of Machine Learning (ML)/Artificial Intelligence (AI)/Data Science within the payments industry is ever expanding, and it is essential that the PSR, as the main regulator in this space, keeps pace with these new and exciting technologies to oversee and manage the regulatory framework.

11. Another use, not mentioned in the paper, is the integration with external data sources and how they can be integrated with payment information to drive insights. Anything like

customer demographic features, Extended Industry Sort Code Directory (EISCD), channels information, freak events (e.g. weather), sporting events etc. can drive further insights into why customers have triggered transactions and ultimately aid in the understanding of these customers. Santander appreciates the PSR cannot monitor and approve all external data sources that TPPs/PSPs use within their payment data products, but should instead encourage a community that actively integrates with external sources to help increase their understanding of payment behaviour.

Question 4: Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data-based overlay services? If so, how can this be addressed? Which parties should be involved?

12. Santander considers the central issues to be data protection and consumer understanding surrounding the usage of their data, within a competitive data environment. Recent events such as Cambridge Analytica, highlight the risks and sentiments regarding alleged data misuse. The approach to data usage by all firms must therefore be transparent and promote active consent in order to build consumer trust.

13. Santander fully supports the development of data-based overlay services, whether directly or indirectly utilising Santander data.

14. To address the issue, Santander considers that a data community needs to be established around each dataset or global dataset that is utilised within the PSR discretion. This discretion centres on the purpose of the global dataset or data product being developed by the TTP or PSP. For example, defensive data products (DDPs) that are being developed for the purpose of financial crime identification or fraud prevention will have direct benefits to customers, and should be progressed with fewer governance reviews. Offensive data products (ODPs) are products that drive revenue or customer growth for PSPs and TPPs; these should fall closer within PSR discretion. These ODPs do not have immediate benefits to consumers, can lead to incorrect consumer contact/classification and can drive aggressive marketing practices. Santander emphasises that the PSR should pay close attention to the governance framework around these ODPs and how they will impact consumers – i.e. is the ODP accurate; does it provide value to the consumer, drive competition, and enable ethical innovation.

15. Santander suggests that the PSR should consider splitting ODPs and DDPs into separate work streams, each with different governance and reporting frameworks. At its highest level, the PSR must challenge PSPs/TPPs in these key areas:
    - How will this data product benefit the wider society?
    - How will this data product directly affect consumers?
    - What is the purpose of this Data Product? Are there any other viable alternatives?
    - How can we trust the output of the Data Product? Can you evidence the results?

16. The level of discretion applied by the PSR should be determined on the nature of the product: DDP or ODP. These discussions and/or reviews must take place in a confidential manner to ensure the intellectual property of these data products is not compromised. Multiple TPPs/PSPs may decide to collaborate and work on data products together, which means the PSR may also have to facilitate discussions across entities to reveal the inner workings of their

data products. Ultimately, the PSR needs to apply an increased framework to ODPs due to the potential impact of these products and will need to encourage/incentivize the development of DDPs along the way.

17. There is potential for certain TPPs/PSPs to develop a monopoly regarding algorithms/data products based on certain global datasets. It will be the PSR's responsibility to intervene should there be indication that these monopolies are forming. One solution may be that groups of TPPs or PSPs beginning to develop a monopoly within a specific global dataset must host an insight workshop allowing other PSPs or TPPs to understand how they are using the data and why their data product is working so well. This would not remove the monopoly, but should encourage others to innovate data products that will challenge the monopoly.

18. Santander has raised concerns in the past about the uptake of digital payment technologies by certain customer segments, and how this may lead to overlay services creating divides between demographic groups. Analysis of customer demographics reveals who is more or less likely to share their data; this is directly correlated to the size of the digital footprint of the consumer, for example the millennial group living within London will have a much greater digital footprint than an older male group living within the North West of England. These divides will become apparent within certain overlay services, especially those that deploy Machine Learning/AI which learns from the data it is given. Bias is an issue within Machine Learning/AI: if adoption rates are high amongst certain demographic groups this can lead to biased data products, which could potentially give rise to discrimination, as noted in the PSR Chairman's speech of 11 July 2018, which included real-world examples of this. Santander considers that Machine Learning/AI has the potential to add great value to customers, but care must be taken so as not to disenfranchise certain consumer groups, and to ensure that Machine Learning/AI is deployed to improve customer outcomes and inclusivity.

19. We suggest the PSR and PSPs/TPPs play a role in educating consumers about the uses of data, emergent technology and the benefits this brings. One way to do this would be to provide relatable examples of how overlay services can provide value to the consumer, for example: *Joe Bloggs shared his mortgage data with his PSPs and other mortgage companies. Through certain predictive models other TPPs/PSPs automatically approved cheaper rate mortgages for Joe and instead of reaching out to Joe directly, they fed the information back to his current mortgage provider. If Joe's current mortgage provider was unable to adjust the rates to match or better the cheapest option, then those cheaper mortgage providers would be allowed to approach Joe.*

20. Santander strongly believes the importance in the value of transparency to customers is paramount: customers must be made aware of what their data will be used for. This should take the form of a readily comprehensible agreement between banks and customers, outlining the data that is to be shared and the possible customer benefits. Customer understanding is critical and will ultimately determine whether or not the customer enters into a contract for services of this nature. Early entrants in the digital payments technology space should be assessed by the PSR on their capability to handle consumer information (much of this is taking place within Open Banking and PSD2 space) – negative experiences with overlay services could further erode consumer trust and would have reputational and other ramifications for market participants (with a knock-on effect for competition).

Question 5: In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

21. Santander agrees that PSOs/Central Infrastructure Providers should allow access to limited global datasets: this will be paramount in developing and releasing overlay services as it provides a complete end-to-end view of customer transactions. More than half of customers today have more than one bank account, across multiple banks, which can give limited views of our customers. Access to global datasets would afford Santander and other PSPs the opportunity to explore full customer data profiles, allowing for more accurate predictions and, as a result, products offered that best meet the needs of customers. This has obvious benefits for both customers and PSP/TPPs, allowing customers to gain access to personalised products and services, whilst allowing PSP/TPPs the framework to build secure and defensive data products that will ultimately keep customers' payments safe. However, Santander raises a concern that the way in which customers' data is shared across different organisations should be carefully considered. As such we would welcome further clarification as to how any data-sharing model fits with domestic and European legislation such as GDPR and the Data Protection Act.

22. As referenced in paragraph 14, we suggest the services offered as a result of access to global datasets can be categorised as defensive and offensive data services. Turning to defensive data services: allowing PSP/TPPs access to global datasets allows for cross-account fraud security measures, identifying payees from other accounts, cross-entity card blocks following lost/stolen notification etc. The possibilities within this space are numerous, as access facilitates reactive cross-account defensive data products that can allow a customer or PSP/TPP to manage security checks/controls across all accounts quickly.

23. Turning to offensive data services: Santander considers that access to global datasets will provide significant insight into cross-account behaviour of customers and the way in which they may treat these accounts differently. Offensive products focus on improving the competitive position/profitability of PSPs and their customers via intelligent targeting and improved customer scoring/profiling: it centres on analysing cross-account information to better understand the services and products offered to customers.

24. Both of these data service strategies align with our wider Santander Group position regarding raw and elaborated data. Actual data (raw and elaborated) can be intertwined with the strategy of the data service. Santander Group differentiates between raw data (that which customers provide) and elaborated data (that which is inferred or derived). We consider that, with regard to elaborated data, customers should have the right to decide whether or not to share, and on what terms. For example, a defensive data strategy or product that is used to improve the protection of customers against fraud should be provided through raw data across the industry. On the other hand, an offensive data strategy that considers the selling of Product X to Segment Y based upon certain features would be constructed from elaborated data. In this case, only those customers that have agreed to share elaborated data could be approached with new products and services. Reversing this, only those PSPs/TPPs who have provided the elaborated data could benefit from the offensive data product they have constructed.

25. Santander highlight concerns here regarding the way in which customers' data may be shared and how this fits with domestic and European data protection legislation. Greater clarity on key questions is welcomed: for example, is true aggregation and anonymisation sufficient to share these global datasets? We believe that sharing of information should come with the proviso that global datasets are handled securely and with the approval of data subjects. Santander recognises that agreeing secure and standardised environments for the sharing of data will take time and funding. Data leakage from global datasets will hurt the reputation of those working within them; therefore, the onus will be on PSPs/TPPs to prove their ability to securely work within these areas. Responsibility will be placed on the PSPs/TPPs to gain consent from their customers, which can then be shared across platforms with safeguards in place to ensure customers do not get contacted by other organisations.

Question 6: What models could the NPSO introduce to allow PSPs to get access to global datasets?

26. Global datasets will only work well when there is a clearly defined problem to be resolved: the New Payment System Operator (NPSO) should set out the problems to be solved and release specific global datasets to allow PSPs/TPPs to resolve the issues. It is extremely difficult to produce insights from large datasets where the problem is poorly defined or unscaled.

27. Competition should be central to any model: PSPs/TPPs must prove their ability to securely handle global datasets and demonstrably produce value for consumers, whether through offensive or defensive services. Similar to sites such as Kaggle (where global datasets have been shared securely since 2010), PSPs/TPPs could compete for access to PSR-controlled global datasets. The top firms could be selected to run and produce data products, which can then be put forward to ethical committees to determine their impact on the customer.

28. One example, to illustrate the point on the NPSO setting out problems to be resolved:
Produce a series of data products that can help identify customers with vulnerabilities; analyse the key trigger events that lead a customer to a poor financial decision or transaction that can lead to negative outcomes.

29. After issuing this problem statement, the NPSO could liaise with PSOs of global datasets to pull together a sample of untraceable transactional history of customers (both vulnerable and non-vulnerable) to release to PSPs/TPPs. This then commences the innovation and competition between different PSPs/TPPs to produce the best data products that solve the problem defined by the NPSO/PSR. Within the data science space, data products can be quantified and ranked. This ability would allow the PSR/NPSO to review and assess the data products produced by different TPPs/PSPs and select those data products they believe provide the best service to consumers. These data products can then be stripped in a confidential and technical manner, reviewed by ethical committees, and ultimately approved by the PSR/NPSO to bring about the desired outcomes. The action in this example, could be that the top five data products are approved by PSR/NPSO to be used on live global datasets. Those PSPs/TPPs that feature in the programme are then able to test their data products against live data and are incentivized with potential new customer streams or product/service offering to new customers.

30. Santander considers that if the NPSO/PSR can continuously define new problems and gain PSO support to provide sample global datasets, then this could be a significant opportunity to develop innovation and competition within the payments data space.

Question 7: Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

31. All regulated PSOs should provide access to truly aggregated and anonymised global datasets. Santander acknowledges that access to full global datasets held by PSOs would be technically unfeasible, carry a severe cost, and would necessitate significant regulation. However, Santander considers PSOs could be incentivized to provide reduced datasets in a forum maintained and regulated by the PSR.

32. Santander actively invites the PSR to host a discussion regarding possible models for incentivising the release of global datasets – any model must work for both PSPs/TPPs and PSOs. The sharing of this data can be incentivized through joint venture data journeys for both PSOs and consumers of the shared datasets. Ultimately, the PSOs will want to understand clearly what value they will gain if they share these global datasets, and this can be demonstrated through joint collaboration of both PSOs and potential data value generators within PSPs/TPPs.

33. Santander emphasises the need for the PSR to take an active role in facilitating and regulating the data community that is produced from global datasets - this includes the following:
    - initial release and demonstration of global datasets by PSOs;
    - facilitation of use-case workshops across the data community on specific global datasets;
    - definitions of problems collated from the PSOs on live problems with datasets;
    - regulation of fair usage within the global datasets; and
    - technical availability of these Datasets.

Question 8: Is there a 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 the issue?

34. There is a tension between the two: on one hand the payments industry needs to develop cross-bank data analysis tools to help us better protect our customers and also offer them bespoke offers; whilst on the other hand, consumers and regulators are becoming increasingly focused on (and question) the industry's usage of consumers' data. Santander proposes a dual-layer consent model that is dependent on the strategy of the data product and any resulting actions leading from that data product. Santander has no concerns over industry-wide data analysis tools providing there is a sufficient control model surrounding these tools.

35. The technical requirements centre on the quantity and movement of data. Santander believes providing industry wide datasets will require significant processing power, both by the central operator and Santander. A further problem is the timeliness of this data: few organisations can establish true real-time technologies, and this will lead to limitations on certain solutions. Initially, however, there is significant benefit for Santander to utilise these historical industry-wide datasets and, over time, we would look to move to a real-time solution to aid the progression of our data products.

Question 9: Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are the barriers?

36. There is value in capturing further ancillary data within the transactional standardised method; however, the potential barrier is how this enhanced data will be captured and processed in a timely and accurate manner. Santander considers that significant value can be driven from the channel information held about a payment. Edge device adoption is increasing month on month, but fundamentally the success of these enhanced data elements will be determined by greater customer awareness of the benefits and the resulting adoption rates.

37. Speed and ease of execution is fundamental to the success of contactless and edge device payments; if the objective is to increase the amount of data-related end-user solutions at the point of transaction, these solutions must not slow down or increase the complexity of the transaction. Potential barriers surround the time taken to process the transaction if there is an increase in data products or data processing required at point of transaction. The sheer amount of data being captured may be a technical barrier if systems are unable to cope with the volume. Moreover, steep data processing requirements could also act as potential barriers to new PSPs/TPPs – if there is significant cost attached to processing certain end-user solutions this could prevent small but innovative firms entering the market.

Question 10: Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

38. A range of enhanced data elements could be added to transactional messages, but care should be taken to ensure that inferred data products that arise from this are not prejudicial. Edge devices must be reviewed in terms of what enhanced data can be captured at the point of sale. Channels drive the data streams for payments: these corridors host the most valuable data and contain the strongest features to determine payment behaviour. Some inferred conclusions may assist the customer – for example, data may flag that the customer was erratic when entering faster payment details by the way they entered the figures into their phone screen, or may flag that that the customer has entered their chip and pin three times slower than normal – prompting an investigation.

39. Given the increasing usage of edge devices and non-customer initiated transactions, Santander would welcome discussion surrounding policies that support this usage of devices outside of core payment channels. It would be helpful to agree standards for information sharing and other information that is permitted to be gathered from the edge device transaction (e.g. behaviour of customer/tone of voice, etc.)

Confidential **3 September 2018**

40. Given the expansive use of data science, Santander would also welcome discussion as to how models can be constructed to easily remove/anonymise/reduce customers' data, and how to prevent this from generating bias.

41. Santander would welcome clarification as to how organisations should approach customer requests for 'right to explanation' without exposing key features that drive the competitive advantage of those models.

42. PSD2 has had significant impacts on how systemically important financial institutions (SIFIs)/PSPs/TPPs handle customer data. Santander would welcome discussion on the ways in which social media organisations, which fall outside of the scope of financial services regulation, share and process data. In order to generate the best consumer outcomes, we consider that a level playing field should apply in respect of consistent standards and regulation.

[ENDS]

Transpact

Dear PSR,

I would like to make one submission in response to the PSR Discussion Paper: Data in the Payments Industry.

Although it is not dealt with specifically in the discussion paper, it is very much a part of the necessary data discussion.

PAYM has been successfully conducting Confirmation of Payee (CoP) for the last five year for many millions of payments every year.
As part of PAYM's CoP, PAYM shows the payer the account name of the payee before the payer authorises the payment, to ensure that the payer can determine that the payee is the intended recipient.
This has prevented much fraud and unnecessary payment misdirection, and is a critical feature of CoP.

CoP is about to be introduced for all Faster Payment System (FPS) payments.

But due to data concerns, the CoP of FPS is semi-impractical, as it does not show the name of the payee's bank account to the payer, as PAYM's CoP does.
Instead, the CoP of FPS that is about to be introduced will attempt itself to match and decide whether the name of the payee is that represented by the name that the payer has entered.
This is a catastrophe waiting to happen. Many payments will work seamlessly without issue, but many other payments will be flagged as dangerous or erroneous when they are safe – due to the payee's bank account name not matching exactly or well enough with the name that the payer entered.
This will cause huge frustration to payment users, and lead to late and missed payments, and a national outcry.

This needs to be corrected before it is too late.
To prevent this catastrophe, CoP of FPS needs to work the same way as the successfully proven CoP of PAYM w, with the name of the payee's bank account shown to the payer, and allowing the payer to make a fully informed decision themselves (at their own risk). Anything else (with the payee bank account name not shown to the payer) will lead the PSR to be castigated as a national furore about missed and delayed payments occurs on the introduction of CoP for FPS.

Please let me know if you would like any clarification or information.

Best Regards,

[redacted]

[redacted]

UK Finance

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.

Visa

Visa

Response to DP18/1 Data in the Payments Industry

1. Executive summary

We live in an increasingly digital world in which the ways data is created, stored and used are growing exponentially. Like many aspects of digital policy, the parameters around what constitutes reasonable and ethical treatment of data are still evolving.

However, one established principle is that a relationship of trust and confidence between all participants is vital for the success of the digital economy, and the benefits it offers for society. Visa is committed to working with Government and other stakeholders to maintain trust and confidence in relation to data across all sectors.

In our own sector, the PSR's discussion paper is timely, as payments data increasingly presents new opportunities, challenges and questions. Consumer trust and confidence in the payment system is paramount to a healthy economy, digital or otherwise.

1.1. The primary use of payments data is to safely and securely process a payment

The primary reason Visa uses payments data is to ensure that payments are safely and securely processed. Our ongoing engagement with consumers strongly indicates that they share this priority.

We utilise the data collected as part of the payments process to protect users of our payment system, and therefore the wider economy, from a wide range of risks. For example, we use data to support an authorisation decision, to detect fraud, to support regulatory compliance activities such as AML and to prevent the financing of terrorism.

Our anti-fraud detection systems, which apply the latest in machine learning and artificial intelligence, have helped keep Visa's global fraud rates near historic lows, less than one tenth of one percent of volumes transacted on Visa cards are lost to fraud.

We also invest heavily in data security measures, since a data breach anywhere in the payments system would substantially increase these risks. One recent innovation is the **Visa Token Service**, which provides the ability to protect sensitive data by replacing sensitive information with a unique digital identifier (a "token"), while also delivering a huge improvement in the convenience of digital payments.

[redacted]

We would support initiatives to increase information sharing between participants in the market for risk management purposes, which we see as a separate issue from the use of data for commercial activities.

1.2. Secondary applications of payments data deliver significant benefits, but need to be considered carefully, responsibly and ethically

We appreciate that examining wider, secondary applications of payments data offers further opportunities for participants in the payment system, ultimately benefitting consumers. The treatment and use of data is a fundamental part of the innovations delivered by today's competitive and dynamic card payments market, for example, **Visa Commerce Solutions** includes a capability for issuers and merchants to use payments data to design offers and rewards tailored to consumers' preferences, and then automatically apply these to eligible purchases once the consumer has actively chosen to participate.

Visa embraces openness, collaboration, and engagement with other organisations to deliver innovation as a competitive necessity. We are currently considering potential opportunities for collaboration on data driven solutions across the payments ecosystem, including ideas to benefit consumers and public organisations, as well as to help financially or digitally excluded groups.

To avoid compromising consumer trust and confidence, **all of these applications of data need to use a considered, responsible and ethical approach, taking into account consumer attitudes**. Our engagement with consumers suggests that they are cautious about sharing their payments data, so this needs to be handled sensitively. The Visa brand is built on customer trust, so maintaining this is a commercial imperative, as well as being the right thing to do.

Data protection regulation provides the legal parameters of what we can and cannot do with data that we hold, particularly since we often only process data in line with instructions from relevant 'data controllers' (our clients). Above and beyond this, however, we take the evolving issue of data ethics extremely seriously, and we examine these matters on an ongoing basis through a company-wide council, taking into account specific issues in the jurisdictions in which Visa operates including the UK. We employ stringent privacy policies that protect all parties involved – consumer, merchant, issuer and acquirer. Visa does not share transaction data with third parties unless a consumer opts-in to a loyalty and rewards program offered by a partner.

1.3. The PSR's objectives are already being delivered by the dynamic and competitive cards market

With regards to the PSR's stated objectives for data in the payment sector, namely promoting competition, innovation and the interests of everyone that uses payments systems, we believe there is strong evidence that these are already being delivered.

Should the PSR wish to implement regulation in this area, we would hope to see certain criteria established, including evidence of detriment to consumers and a thorough assessment of cost and benefit of regulatory intervention versus market driven solutions. Additionally, any new policies relating to the collection and sharing of data, should carefully consider the consumer

perspective, and include a clear model of consumer permissions, controls and safeguards to avoid damaging the trust that consumers place in the payment ecosystem as a whole. We would support any PSR initiatives to help raise consumer awareness and understanding around these issues.

Contents

2. Introduction

We welcome the opportunity to provide our views on the PSR's discussion paper, data in the payments industry. We are pleased that the PSR is considering data and taking views from stakeholders on the role it might play.

Our view is that future policies relating to data should start by better understanding the people and businesses who use the payment system. We elaborate on this in section 3.

The remainder of our response follows the structure of the PSR's discussion paper, with each section containing our comments on the paper's chapters.

A response to the PSR's specific discussion questions is included as an appendix.

3. The consumer perspective

Future policies relating to data should start by better understanding the people and businesses who rely on the payments industry every single day.

With advances in data analytics, the scope for using payments data in commercial practices is increasing, but consumers may not be aware of this. With regard to the way data is used, trust is particularly important given that consumer's understanding of the way companies use data can be limited. For example, 2018 research by the think tank Doteveryone, whose consumer research[1] into Digital Understanding found, for example, that 62% of respondents didn't realise their social networks can affect the news they see, and 45% are unaware information they enter on websites and social media can help target ads.

Our ongoing engagement with consumers indicates that consumers are generally cautious about sharing their payments data, even if this is in return for services such as tailored offers or discounts. Our findings are consistent with research in other areas. For example, Ofgem's recent consumer research[2] found that while almost half of consumers are happy in general to share data with organisations with whom they have a relationship, financial records were perceived as more sensitive.

Consumer trust in this system is paramount, given the importance of payment systems to financial stability, and the economy as a whole. Confidence in payment systems, and in Visa has been hard won, and would be easily lost, for example if Visa was required to use data for a purpose that consumers were not comfortable with, or in the event of a data breach.

This highlights the need for companies with access to individual's data to use it in a responsible manner and to avoid breaching consumer trust. Recent news stories around the use of data,

[1] People, Power and Technology: The 2018 Digital Understanding Report http://understanding.doteveryone.org.uk/

[2] Consumer views on sharing half-hourly settlement data: https://www.ofgem.gov.uk/publications-and-updates/consumer-views-sharing-half-hourly-settlement-data

concerns about privacy, and data breaches highlight the potential risks around the way companies secure and use data.

We believe that when consumers see the Visa logo they know they can be confident that this is payment they can trust[3]. Visa is committed to upholding consumers' trust, including through the ethical and responsible use of data by any parties connected to the Visa payment system. We describe Visa's approach to using data and partnering in a safe and secure way in sections 4.3 and 4.4 below, and explain our approach to data ethics in section 6.3.

Any future moves to encourage new uses for payments data should consider the concerns that this consumer research highlights. In particular, any moves to share data with a wider range of organisations should be under tightly controlled circumstances.

4. Data in the changing payments landscape

4.1. The card and digital payments landscape

We agree with the PSR's view that the UK payments industry is evolving quickly. We are committed to supporting the evolution of payments within the digital economy and ensuring our business makes it possible for everyone to participate fully.

This evolution provides benefits for consumers, businesses and the economy as a whole. In 2016, Visa commissioned Roubini ThoughtLab (an economic consulting and research firm) to assess the benefits that developments in digital payments can bring. The research[4] analysed 100 cities across the world, and estimated that reaching an 'achievable level' of digital payments could result in total direct net benefits of up to US$470 billion per year, accruing to consumers, businesses and governments.

Benefits of increased digital payments include time savings, reduced fees for cash access (e.g. cheque cashing charges), interest earnt from holding funds in an electronic account rather than cash, reductions in crime and fewer transactions in the 'black economy'.

Digital payments are not limited to card transactions, which are increasingly giving way to frictionless, fully digital experiences across new connected devices and customer journeys. Consumers want to buy products and services with their computers, tablets, phones, cars and even wearables, and they expect to pay for coffee with a tap or transfer funds to friends with a click.

As an example, contactless card payments, first introduced in 2007, offer a quick and convenient alternative to cash for low-value transactions, while including all the security and consumer

[3]In 2015, the Reader's Digest listed Visa as the most trusted credit card, based on a number of factors, including quality, value, and reliability. Forbes has listed Visa in the top 30 most reputable companies. And Visa is consistently ranked as one of the top brands in the world.

[4] Cashless cities: realising the benefits of digital payments: https://usa.visa.com/visa-everywhere/global-impact/cashless-cities.html

protections embedded in card payment methods. The value of transactions via contactless cards in the UK has increased from £620m to over £4.3 billion (representing an increase of almost 600%) in the two years between July 2015 and June 2017.[5]

This progress is underpinned by a more innovative, dynamic and competitive global payments market than has ever existed. In 2016, the value of electronic payments surpassed the value of cash payments worldwide for the first time,[6] marking the fact that payments have entered a period of transformative evolution.

4.2. Visa's role in the changing landscape

Visa was founded on the principle of responsible and secure innovation. We believe that businesses that facilitate digital transformation have a shared responsibility to work together, and to play their part in ensuring the economy of the future is built on stable foundations. This means an ambitious level of investment in innovation; world-leading security to combat the ever-greater cyber threat; a responsible approach to data; and a high degree of collaboration and partnerships across the whole ecosystem.

In terms of partnerships and collaboration, our 'four party' business model inherently fosters co-operation and shared responsibility. There is naturally a high degree of collaboration with issuers and acquirers, with whom we hold direct, commercial relationships (these parties in turn hold their own separate relationships with consumers and merchants). However, Visa is increasingly looking outward across the whole fintech and digital ecosystem. Two examples are Visa Direct and our Token Service:

Visa Direct

We recently launched Visa Direct, a fast and secure payments platform that allows financial institutions, developers and partners to utilise Visa's global network to offer real-time, person-to-person payments and business disbursements services. Visa Direct addresses a growing market of businesses and consumers who expect to be able to move money between themselves at the same speed as their emails and mobile apps, within seconds.[7]

This is a significant evolution of Visa's offerings, in a world of sharing apps, marketplace apps, and the gig economy – all of which are 'mobile first', powered by apps capable of moving information and services at real-time speed across the world. Ireland is set to be the first majority-enabled Visa Direct market in Europe, which means over 80 per cent of cards will be enabled for the service.

---

5 Source: Statista Dossier on Contactless payment in the United Kingdom (page 12)

6 https://blog.euromonitor.com/2016/09/consumer-card-transactions-overtake-cash-payments-first-time-2016.html

7 Visa Direct offers real-time push payment capabilities that utilise Visa's global payment system. Through their participating financial institutions, businesses and consumers can use the Visa network to send money to over one billion eligible Visa card accounts.

Visa's Token Service

With demand expected to increase for devices embedded with payment capabilities, Visa has invested to build a global network of 'Visa Ready' partners to offer digital payment token services to ensure that a wide range of appliances can become more secure places for commerce.

Visa's Token Service is a security technology that can help clients build and maintain digital payment experiences while protecting sensitive information from fraud. It replaces sensitive payment card account information, such as the 16-digit card number, expiration date and security code, with a unique digital identifier (a "token") to process payments without exposing actual Primary Account Number (PAN) details.

We are also looking further ahead. In particular, we are currently researching how technologies like quantum computing and artificial intelligence will impact how consumers purchase and engage with products and services. Visa pioneered the use of sophisticated machine learning systems to reduce fraud on our network, and today, we are applying AI and machine learning across several areas of our business, from authorisation, authentication and risk management, to cyber security, operational systems efficiency and fraud management. In 2015, Visa launched Visa Research to apply AI, machine learning and deep learning to areas such as security and the future of commerce.

4.3. The role of data in the changing landscape

We agree with the PSR's view that data is one of the driving factors for the rapid evolution in the UK payments sector. Many of the examples and success stories described in the section above were supported by data. For example, the data collected as part of a contactless payment enables built-in protection from unauthorised use, giving consumers confidence to embrace the new way to pay.

The responsible innovation and data analytics we describe in this section are benefits we can deliver for our clients and ultimately consumers, but it is not the principal product we offer, and the chief reason we collect data is to enable a safe and secure payment and protect against risks. Other uses of data are secondary to this core business.

This said, we understand the value of data and analytics and want to cultivate ideas, relationships & opportunities, accelerate breakthroughs using data and improve analytics capabilities.

Visa offers optional products and solutions that use aggregated and anonymised purchase data to help fight fraud and share insights with merchant, acquirer and issuer clients. These products also help to enhance the consumer experience, improve merchant and issuer client programs, and strengthen commerce. We employ stringent privacy policies that protect all parties involved – consumer, merchant, issuer and acquirer. We do not share transaction data with third parties unless a consumer opts-in to a loyalty and rewards program offered by a partner.

One example is Visa Commerce Solutions, which includes a capability for issuers and merchants to use payments data to design offers and rewards tailored to consumers' preferences. These can then be automatically applied to eligible purchases once the consumer has actively chosen to participate.

We are also exploring further applications of data through our new Data Science Lab:

Visa Data Science Lab in Europe

In July 2018, Visa launched our new Data Science Lab. The Data Science Lab is a European pilot that uses responsible data analytics to inform our strategy, as well as that of our clients, in order to improve and grow the payments eco-system.

It includes a purpose built area presenting data-driven insights and commercial opportunities in an interactive and engaging way that democratises data and improves decision-making.

We plan to build on two 'pillars' for use of data from the lab:

1. **Internal:** Be the centre of expertise in the organisation driving operational efficiency in the way data and insights are presented so that they can be consumed more easily and translated into action more rapidly. Additionally, the lab will lead and nurture the skills and capability of the wider data community

2. **Client:** Use data to deepen partnerships with clients, further build brand trust, enhance decision making that will improve their payments and strategies and grow their portfolios

The data analytics provided by the lab will be carefully considered in light of data protection and ethical issues (see section 5.4 and 6.3 respectively).

We are already collaborating on joint activities with a wide range of external organisations such as Imperial College London, IBM and Microsoft to share perspectives, develop new proof-of concepts, and build data skills programmes. For example, we are exploring ways to put momentum behind a new UK Apprenticeship standard for Data Analysts that uses Apprentice Levy funds. Additionally, we are cooperating with the education sector to help better structure analytics and data science post-graduate programmes to fit business needs for innovation.

We think these examples demonstrate that the card payments industry is already delivering significant progress and innovation with respect to data.

In the UK, a combination of a generally well-constructed regulatory environment, policy stability, and the right infrastructure conditions has resulted in continual investment and expansion of the market, as well as innovation. ***Any future policy developments should be made collaboratively with industry and build on this progress, rather than replicating or replacing it.***

Interventions should avoid attempts to 'pick winners' or choose specific innovations, which could inadvertently distort the market, stifle innovation or threaten the UK economy's leading position in digital payments.

We understand that there are several government sponsored data groups being set up to look at data. We are keen to collaborate with these initiatives wherever possible.

4.4. Link to Open Banking

The discussion document references Open Banking, and we agree that Europe's PSD2 initiative will open up new opportunities, although it is still at an early stage.

However, the card payments market is not comparable to the retail banking market. In order to stay competitive in this rapidly evolving environment, companies in the payments sector are already forging close partnerships with fintechs, and opening APIs to third parties, providing opportunities for new and creative service offerings.

Visa Developer Platform

In 2016, we launched the Visa Developer Platform (VDP), transforming our proprietary technology network, VisaNet, into the world's largest open commerce platform. VDP provides simplified access to many of Visa's most in-demand products and services through an open network of Visa APIs, allowing anyone to transform great ideas into new digital commerce experiences.

VDP offers 90+ APIs, enabling access to some of Visa's most popular capabilities, providing developers with a safe testing environment for the development of new digital payments and commerce solutions.

While Visa's open API platform has been effective in enabling third-party developers to access Visa's technologies, opening access to third parties is not without risk, especially with respect to security, privacy and data protection considerations. **Accordingly, we do not believe that additional regulation is necessary to *introduce an Open Banking type initiative for the payments market.***

5. The collection and classification of payments data

5.1. Comments on the discussion paper

In terms of comments on the PSR's characterisation of data in card payments:

- There is a greater range of possible information flows and a greater level of complexity involved in card payments than the description in the discussion paper. It is impractical to include all of the possible flows of information for payments in a simplified set of diagrams. However, the fact that there is (appropriately) variation in the information flow

for different card payments should be acknowledged, and a 'one-size-fits-all' intervention across all forms of payment should be avoided.

- Cards are fundamentally different from interbank payments, including an already rich data set. This should be emphasised in any description of information flows in the industry.
- Data is a competitive driver for card payments and alternative payment methods. The flexibility in payment messages and the data collected in them underpins this.
- Data protection and data security requirements cannot be compromised and should be emphasised in any description of data in the payments industry.
- Changes to the data architecture in the cards payments ecosystem are potentially disruptive, with high associated costs. They should only be made following a thorough cost-benefit analysis.

The rest of this section expands on these points. More specific comments on the PSR's description of information flows for card payments are contained in the appendix.

5.2. Cards are fundamentally different from interbank payments

An explanation of the flow of information in different payment system ecosystems should emphasise the fundamental difference between each system, including the **payment messages**, which contain the data collected as part of a transaction. The PSR should bear in mind the qualitative difference between card payments and interbank payments:

Fundamental differences between interbank payment and card payment ecosystems

	Ecosystem	Processing Method	Messaging Construct	Funding Model	Authentication
Card	End to end between merchant and consumer through acquirer-Issuer links with global acceptance.	Real-time authorisation with daily net settlement and either deferred or batch clearing or real-time transactions clearing.	Request/response payment messaging with issuer decisioning logic. Card payment message construct includes authorisation, clearing and settlement.	Funds pulled from available 'open to buy' amounts.	Strong card / cardholder authentication (e.g. PIN, CVV) built into payments messages with EMV and PCI compliance requirements.
Interbank	Between two financial institutions for the purposes of domestic clearing and settlement.	Real-time clearing with either real-time gross settlement or multiple intra-day settlements.	Unidirectional push* payment message without any issuer decisioning logic. Push* payment message includes clearing and settlement.	Funds pushed* from "good funds" account balance.	Limited user authentication handled outside of payments message supported via proprietary solutions.

*Faster Payments and CHAPS

Within card payments a rich data set already exists, which allows a multi-layered analysis and results in accurate decision-making based upon fact. Utilising this data set allows us to offer additional value-added products but also provide key fraud and risk capabilities such as risk-based authentication.

While interbank payments tend to occur between financial institutions, cards payments frequently involve a much higher number of parties and intermediaries within the Merchant to Acquirer, Acquirer to Issuer and Issuer to cardholder domains. Consequently, there are many additional and more flexible end-points. Additionally, local, regional or global legal and regulatory demands mean that payment messages require continual maintenance. This necessitates frequent, rapid messaging standards maintenance cycles for the card industry.

Any future policy decisions should start from the premise that the data involved with card payments is significantly different from the data collected during interbank payments.

5.3. Data as a competitive driver

The card payments industry is not a monopoly. Multiple card schemes compete with one another and innovate to secure clients. Consumers also have a range of other payment methods to turn to if we don't offer a competitive service. In addition to Scheme-to-Scheme competition, there is added competition between Processors (which in Europe are required to be separated from Schemes under the Interchange Fees Regulation), and competition with alternative payment methods such as PayPal, offerings from technology companies such as Amazon, Apple and Google, and retailer solutions such as Tesco Pay+.

One of the ways we compete is through our payment message, and the way we use the data gathered. The type of data collected may differ depending on the type of payment transaction. For example, in our core transaction processing business that supports a typical consumer purchase of a good or service, we only collect card account number, expiration date, security codes, and transaction data such as merchant type, amount and date. When offering optional, related services we may collect additional information, such as a Visa Checkout[8] user's name, shipping address, username, and password (but only as needed to provide the service offered). New products and services could require different data to be collected.

The additional value adding services provided by cards necessitates some flexibility in the data collected during payments. Future regulation of the data collected during card payments risks reducing competition and the innovation it drives. We have provided similar feedback to the Bank of England's recent consultation on the ISO 20022 standard for payments[9].

5.4. Data protection

Visa, like all other organisations in the payment sector, must work within the legislative framework that applies to the processing of personal data. This includes the General Data Protection Regulation and, in the UK, the Data Protection Act 2018 ('Data Protection Legislation').

---

[8] Visa Checkout allows users to pay online merchants using an account that stores their payment details, rather than filling in forms to enter this information.

[9] ISO 20022 Consultation Paper: A Global Standard to Modernise UK Payments https://www.bankofengland.co.uk/news/2018/june/iso-20022-consultation-paper-a-global-standard-to-modernise-uk-payments

In the context of transaction processing, Visa generally processes personal data as a 'Data Processor' acting on behalf of its clients, who are the 'Data Controllers'. When acting as a Data Processor, Visa cannot determine the purpose(s) for which personal data can be processed; only the Data Controller can do this.

This is particularly relevant in relation to the PSR's concept of 'global transaction data', which we discuss further below in section 7.4.

GDPR introduced new standards relating to consent, which consumers are just beginning to appreciate and grow accustomed to. Consent for use of consumer data is difficult to demonstrate, particularly since the way companies use data isn't static.

This is even more complex if it involves sharing with third parties, since data could be accessed, or copied, or transferred further and reused. Once shared, it is increasingly difficult for any entity to ensure data protection or retain control of who has access to data.

As a result, any future policies involving sharing data, or collecting more data than is required for the payment product or service being delivered needs a clear model of consent, and effective safeguards and protections.

5.5. Data security

Championing security is one of Visa's core strategic goals. There is a growing cyber threat to companies such as Visa and the payments ecosystem at large, and Visa has devoted substantial resources to effectively address that threat. For instance, in the last year (as of early 2018), the Visa Cyber Defence team has managed over 6,500 security incidents ranging from malware, Distributed Denial of Service (DDoS) attacks, and insider threats. A data breach anywhere in payment systems could lead to fraudulent use of the data obtained, either in payments services or in other markets where payments systems are used to transact.

Accordingly, cyber security is integral to Visa's business and receives significant levels of investment (including over 500 security professionals with specialties ranging from Cryptography to Forensic and Security Engineering) and management attention.

Visa actively promotes the protection of payments data in the wider ecosystem through significant investment in leading, developing and continuously evolving content within industry organisations such as the Payment Card Industry Security Standards Council. Examples include the PCI DSS (Payment Card Industry Data Security Standard), EMV technical standards and the introduction of EMV payment tokenisation.

Visa employs extensive data security measures to protect all personal data in our care, including measures that are above and beyond the Payment Card Industry Data Security Standard discussed above. We use data devaluation techniques such as encryption to further protect information on our network. Through Visa's Data Protection Program, we are close to encrypting 100 percent of our data repositories. We extend data security and encryption requirements to third-party hosted or provided solutions and monitor compliance with those requirements through our Supplier Risk Management program.

A further demonstration of our commitment to data security is the Cyber Fusion Centre we are launching in Europe, co-locating the Visa's top cyber talent and creating a world-class security centre, centralising command and control for rapid threat detection and incident response.

Future policies that may widen access to consumer data should consider the cyber security requirements placed on organisations with access to this data, and the cyber risks this could introduce. The more points of potential attack are added, the more difficult it becomes to detect potential points of breach. The strength of data security against cyber threats is only as strong as the weakest point in the transactional chain.

If going ahead with any policies to increase access to data, pre-vetting or authorisation would be required before granting access. A clear process would need to be set out for this, and should avoid placing unfair financial or resource burdens onto selected companies.

However, given the fast-changing nature of cyber threats and the ingenuity of hackers, it is vital that cyber defences evolve just as quickly to keep ahead of potential risks. Regulation to set security practices or technologies that companies should adopt can create an additional compliance burden that may not be necessary or beneficial, as regulation moves more slowly than technological advances, and may be obsolete by the time it is enacted.

5.6. Disruption from changes to data architecture

It is important that the information carried in a payment message is limited to that which is necessary for the purposes of risk management, settlement and the delivery of consumer and merchant needs so as not to introduce unnecessary risk or complexity into the system. Visa's system scales to support 68,000 transactions per second at peak capacity. This scale means that careful consideration is required before adding additional information so as to maintain the high standards of efficiency and security our clients, merchants and consumers expect.

Visa operates on the basis of two global business releases for issuers and acquirers per year. Each release is carefully managed in terms of level of change systems and processes for Issuers, Acquirers and for Visa. Business releases are applied to the global platform and therefore impact all clients. The nature of the releases change – some are functional changes, others are systemic to the whole card ecosystem and are applied simultaneously by all participants (MasterCard et al).

In order to implement changes to the data we collect, change would be required within the core of Visa's systems, across all UK issuers and all global acquirers. The level of change and risk introduced to the business releases would be such that it could take many years for changes to be effective in the live system.

Therefore, any move that alters the data architecture of the card payments industry should be subject to a thorough cost benefit analysis, identifying the concrete benefits they will deliver for consumers compared to the level of disruption caused.

6. How is payments data used?

6.1. Comments on the discussion paper

The primary purpose of the data collected as part of payment transactions is to ensure safe and secure payment processing, including the mitigation of fraud risks.

Any additional benefits arising from payments data must be secondary to these requirements, which cannot be compromised.

In this section, we expand on this point, as well as providing additional information on the way Visa uses data for fraud risk management, and the potential difficulties for vulnerable consumers that developments in data may pose.

6.2. Tying data back to its purpose

Any discussion of data in the payments industry should recognise that the collection and commercialisation of data is secondary to the use of data to perform essential functions associated with the service we provide, such as:

- Authentication of a legitimate payment
- Compliance with Anti-Money Laundering (AML) regulations
- Facilitation of subsequent service access (e.g., password reset or form fill capabilities)
- Delivery of the core feature of the product such as alerts on potentially fraudulent account applications
- Delivering a good consumer experience (e.g., reducing the time it takes to safely and securely make a payment)

When offering payment services, we collect only the information reasonably necessary to operate the service. For example, in our core transaction processing business that supports a typical consumer purchase of a good or service, we collect card account number, expiration date, security codes, and transaction data such as merchant type, amount and date.

Beyond our core processing business when offering optional, related payment services such as Visa Checkout, commercial card programs, issuer processing, and risk products, Visa may collect additional personal information such as names, usernames and passwords, government ID, and identity verification data as needed to operate the service. Consistent with our practice for transaction processing, we collect only what is reasonably necessary to operate the service securely, effectively, and in compliance with local laws.

While we do use data analytics to provide new services for clients, consumers and merchants (see 4.3 above), this is a secondary activity. ***Any future policies should recognise this and under no circumstances risk compromising or impeding the primary function of safely and securely processing a payment.***

6.3. Ethical use of data

As the range of potential uses for data increases, and a greater level of insight into consumer behaviour is possible, the ethical questions surrounding its use also grows. Visa believes that companies with access to data have a responsibility to use it in the right manner.

As discussed in section 6.2 above, Visa is looking to do more with data to provide new services that clients, consumers and merchants value. However, we want to go about this in a thoughtful and consistent way, to avoid compromising the trust that our consumers and clients place in us.

One of the ways we achieve this is through considering new data uses from an ethical perspective, including our Data Use Council.

Visa's Data Use Council

Visa have constituted a global Data Use Council (VDUC) to help define and implement the company's strategic vision and principles for data use. The VDUC reviews and advises on strategic data use decisions and is responsible for ensuring that such decisions are subject to a robust cross-functional review. The VDUC's remit includes all business units, functions, geographies, and affiliates.

The VDUC considers whether a particular use of data is in line with applicable laws, regulation and contracts, but also looks at strategic, brand and ethical perspectives.

Ethical questions around data are not static, and Visa is developing new internal arrangements to provide a consistent set of principles and expectations around what is and isn't appropriate.

Any future policy decisions should consider the ethical questions surrounding data use, and we would be happy to engage with the PSR and wider stakeholders in the future to share perspectives.

6.4. Fraud

Fraud is an issue that Visa also takes very seriously. Our anti-fraud detection systems, which apply the latest in machine learning and artificial intelligence, have helped keep Visa's global fraud rates near historic lows, less than one tenth of one percent of volumes transacted on Visa cards are lost to fraud.

Our fraud prevention and detection measures include:

- Visa Transaction Controls, which enable cardholders to suspend misplaced cards and block or create alerts for different types of transactions, which can help prevent or detect fraud.
- Visa Advanced Authorisation allows us to assess the fraud risk for every Visa-processed transaction as it is taking place. If a transaction appears to be at an elevated risk of fraud, Visa issuers can stop the transaction before it is complete, protecting the cardholder from fraud.

- Visa's Payment Systems Intelligence team, which identifies, disrupts and minimises criminal activities targeting Visa clients, merchants and the overall payments system, leveraging Visa's global view of crime, which puts the company in a unique position to combat sophisticated breaches and disrupt fraud schemes

Technology advances have already reduced the risk of fraud. For example, the introduction of EMV[10] in Europe has resulted in a significant reduction in the exploitation of easily compromised magnetic stripe data. More recently, the tokenisation of Primary Account Numbers sent in payment messages is further reducing incidents of data compromise and the subsequent use of that data to undertake transactions.

One current example is the roll out of 3D-Secure 2.0 protocol for e-commerce, credit and debit card transactions, which will enable a real-time, secure, information-sharing pipeline that merchants can use to send an unprecedented number of transaction attributes that the issuer can use to authenticate transactions and individuals more accurately without asking for a static password or slowing down commerce. This will provide fraud protection for both merchants and cardholders (rather than just cardholders).

Looking ahead, we are seeing an increase in 'social engineering', where scammers attempt to persuade the individuals to make a genuine transaction on behalf of, or to the benefit of, the criminal. One well-known example of social engineering is "phishing", whereby fraudsters seek to obtain personal information by posing as a legitimate organisation. One estimate finds that share of financial phishing (i.e. attacks against banks, payment systems and e-shops) has increased, for the first time, to over half of all global phishing detections.[11] To date, Visa has taken down over 2,000 Visa-targeted phishing websites globally.

There may be an opportunity for future policy developments to share data or information to enhance fraud detection capabilities of all participants in the industry. However, these need to be delivered in a way that does not impede market-based initiatives to improve fraud prevention and mitigation, and should avoid adding friction to the payments process. They must also include safeguards against risks such as reverse engineering based on shared information.

6.5. Vulnerability

We agree with the PSR that vulnerable consumers may be disadvantaged in the future if they are unable to engage with new payments solutions. However, our view is that there are additional risks for vulnerable consumers, which need to be addressed.

Vulnerable consumers may be more susceptible to the sort of harms that can arise from the misuse of their data - for example frauds and scams. Or payments data could be used to exploit vulnerable consumers by targeting particular services at them, by engaging in exploitative

[10] EMV is the global standard for chip-based Debit and Credit Card transactions

[11] https://usa.kaspersky.com/about/press-releases/2018_financial-phishing-accounts-for-more-than-half-of-all-phishing-attacks

pricing practices or even excluding vulnerable individuals or groups from certain markets entirely.

We support the UK Government's strong stance on a digital transformation in which no-one is excluded, and we are committed to tackling the causes of exclusion - financial, digital or otherwise.

Globally, our reach makes Visa's network and services a powerful platform to drive financial inclusion (and associated educations). We recognise our role and responsibility in working with governments and other stakeholders to try to ensure no one is left behind by the transition toward greater use of secure digital payments.

7. Potential PSR policy issues

7.1. Overall

Based on the information in the sections above, we have a number of comments on the potential PSR policy issues contained in the discussion document. The discussion paper includes three objectives that the PSR want to address:

- promote the interests of those that use or are likely to use payment systems
- promote competition in payment systems
- promote innovation in payment systems

Visa's supports these objectives and believes that they are already being delivered in the card payment market. With the rapid pace of technological change, growing consumer demand for new and innovative services, and increasing propensity for companies to enhance product offerings - either through third-party partnerships or in-house development - ***Visa does not see compelling reasons for regulator intervention in the card payments market along the lines of enhancing or standardising the data collected during a payment, or introducing new sharing methods for commercialisation of data.***

However, we believe that the regulator could play an important role in two areas. The PSR identifies that there is an opportunity for it to help increase understanding of new technology and become more willing to adopt it. We support initiatives like this, in addition to those already been delivered by other organisations.

Secondly, there may be opportunities for the PSR to facilitate sharing information to increase the capability of participants in the payment system to protect against fraud. We see this as a separate issue from sharing data for commercial applications.

7.2. End-user ability to adopt new digital payments technology

The discussion paper includes ideas for the PSR to increase consumer and merchant understanding of new technology and be more willing to adopt it, e.g. education campaigns. As we described in section 3, consumer trust and consent are vital requirements for any new products and services relating to data.

Consumer understanding of digital technology can be low, so campaigns to increase this could both increase the uptake of new products and services, and reduce the risk of breaches of consumer trust if they do not fully appreciate what they are signing up for.

We support the idea of initiatives like this, and would welcome the opportunity to collaborate with other parties to deliver this.

7.3. Data standardisation and enhancement

The discussion paper includes suggested measures from the Payment Systems Forum relating to standardisation of data. These include common messaging standards, and changes to quality of data. The discussion paper also includes a description of the adoption of 'Enhanced Data' within the NPA, and the work the Bank of England is currently considering on the ISO20022 standard for payment messages[12].

We fully appreciate the importance of rich payment data and the wide economic benefits it can bring by equipping payment service providers and governments alike with valuable information to make better informed decisions. As described in section 5, a rich card payments data set already exists due to the nature of card transaction variables.

As we have stated in our response to the Bank's consultation on ISO 20022, Visa supports the increasing richness and applicability of data in card payments. ***However, we do not believe that further standardisation of data, or additional requirements around data collection would be appropriate in the card payments market.*** Not only does this risk adding friction to the payments process, it could impede competition in the sector given that we compete partly on the basis of our data and payment messages.

The future vision for the data collected as part of payments should enable sufficient commonality while ensuring differentiation to support innovation and competition. We feel that existing industry initiatives already strike this balance.

7.4. Data sharing and global datasets

The discussion paper includes proposals for data sharing, including payment system operators providing access to global transaction datasets. We see two very separate aspects to data sharing. One relates to improving the fraud, AML and financial crime detection and monitoring:

Specifically, from a fraud protection and prevention viewpoint, harnessing global fraud data would be very valuable in terms of enhancing fraud prevention and detection capabilities. We would support developments in this area. This might include initiatives to enhance:

- Detection of bad players or actors and data to deal with them (e.g. 'grey lists' such as Visa Merchant Alert Service)

[12] ISO 20022 Consultation Paper: A Global Standard to Modernise UK Payments https://www.bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme/consultation-on-a-new-messaging-standard-for-uk-payments-iso20022

- Identification and validation of individuals whilst minimising transaction authentication friction
- Devaluation of data (i.e. making it less valuable even if it is fraudulently obtained)
- Profiling to identify illegality in the system (e.g. merchants selling illegal or brand damaging goods or services)
- Other profiling or sharing to support regulation or mange risks

We would support any initiatives to increase companies' capabilities in this space, bearing in mind limitations such as data security.

The second aspect to data sharing relates to increasing access to third parties. As described in section 4, there are already opportunities for third parties to access Visa's capabilities in a controlled and managed way, for example through the Visa Developer Platform, and we are already collaborating with other parties to pursue new ideas relating to data.

We do not agree with the PSR's statement in the discussion paper that third parties may find it hard to obtain datasets, at least in relation to Visa's data, nor do we believe that any action from the PSR is needed to reduce restrictions around access to global datasets.

Additionally, the payments data that Visa holds is collected as part of a competitive market, where clients, merchants and consumers have access to other card schemes or alternative payment methods. Therefore, the data we hold does not represent a 'global' dataset.

Additional sharing of data for any application would also introduce risks around data security and data protection, as described in section 5.

Data protection concerns are particularly relevant in relation to the PSR's concept of 'global transaction data', that is, the aggregation of transaction data for a specific payment system. Although the global transaction datasets are aggregated, the PSR notes that they may, in some instances, contain personal data. If this is the case, the global data sets are caught within scope of the Data Protection Legislation, the impact of which includes the following, when Visa is acting as a Data Processor:

- Where appropriate, the Data Controllers (the Issuers) must instruct Visa to undertake this data processing activity: in those circumstances, there must be clear instructions to Visa to aggregate the transaction data for a specified purpose (Article 28, GDPR).
- This specified purpose must be determined by the Data Controller (and not Visa, or a third party).
- The Data Controller must identify the 'lawful basis' upon which the data processing is undertaken. If consent is relied upon as the 'lawful basis', there must be a clear mechanism for the individual to withdraw consent (Articles 6, 7, GDPR).
- In order to meet the GDPR's transparency requirements, the Data Controller must provide information to cardholders about the aggregation of transaction data. This information must be provided in a transparent, concise and intelligible way (Article 12, GDPR).

- The global transaction datasets must be able to technically and functionally deliver on data subject rights (such as the right of access, deletion or correction), where applicable (Articles 15 – 22, GDPR).

We would expect that new regulation or clarification from the ICO may be required to allow sharing of these global datasets. Issues around liability and the controller of the dataset would also need to be addressed.

For these reasons, we do not believe there is a case for the PSR to make such global datasets available to third parties and any future policies should be carefully considered in terms of the demonstrable problem or market failure they will solve, and must in all cases avoid changes that could compromise data security and protection.

Should the PSR wish to implement regulation in this area, we would hope to see certain criteria established, including evidence of detriment to consumers and a thorough assessment of cost and benefit of regulatory intervention versus market driven solutions.

8. Appendix: responses to consultation questions

1. Do you agree with our assessment of:

a. the types of data in the payments industry that are relevant for this paper?

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

c. the different ways that payments data can be classified?

The flow of information in a card payment transaction is more complex and variable than the simplified description given in the discussion paper:

- Interchange Fees Regulation requires the separation of Scheme and Processing elements of card-based payment system operators. In places the discussion paper treats these interchangeably. In general, the range of language used in the document such as 'card system', 'payment system operators' and 'scheme' could be misleading. We suggest that 'Scheme' and 'Processing' be used to avoid this ambiguity.
- Figure 5 in the discussion paper shows a simplified card payment. However, it should also acknowledge that there are alternative routes a card payment could take. For example, the diagram represents a dual-message transaction. While this is the approach taken for the majority of card payments in the UK, Visa is moving toward single-messages (i.e. combined authorisation and clearing) in some cases.
- There is also some ambiguity in the PSR's description of 'card holder' and 'card'. In some cases, (e.g. for an online transaction) a cardholder enters their data themselves or it may be stored by the merchant from a previous transaction. For others, the data is embedded in the card itself (e.g. in a POS terminal).
- Figure 5 shows value added services such as fraud scoring occurring in the 'card system' box (i.e. Processing). This can also occur at other points in the process, for example Issuers can perform their own fraud-prevention measures, and value-adding services can also be offered to merchants and acquirers.
- The global nature of card payments means that although the institutions listed in the PSR's diagram are correct, the actual complexity involved could be higher with international institutions involved, and several sets of national or regional laws.
- Figure 4 showing LINK cash withdrawals should also acknowledge that there are other possible variants for an ATM transaction (e.g. using a credit card and following a process more similar to a card payment).

More minor comments are:

- Section 4.45 of the discussion paper references 'If the cardholder authenticates the card and the transaction goes ahead, an authorisation message is routed…', which is not strictly correct. The authorisation process first checks that sufficient funds are available, followed by other checks such as fraud checks. It would be more accurate to state that the cardholder authenticates themselves not the card.

- Section 4.48.a states that 'card security standards limit the use and distribution of this data'. For completeness, card security standards also determine rules for storage of data.
- Figure 5 has labelled the clearing and settlement message between merchants and acquirers incorrectly.
- Figure 5 includes an arrow as part of clearing and settlement messages between the cardholder and merchant labelled 'goods taken/shipped'. This is not part of clearing and settlement or the information flow of a card payment, so could be removed.
- The different parts of section 4 use different language for different participants in the payments processes. For added clarity consistent terms should be used.

2. 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?

See question 3 below.

3. 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 primary purposes of the data collected as part of payment transactions are the safe and secure processing of a payment, and the mitigation of risks such as fraud. Any additional benefits arising from payments data must be secondary to these requirements, which cannot be compromised.

While use of data for fraud prevention and detection is acknowledged in the discussion paper, the primary purpose of the data payment companies collect should be emphasised more.

For more detail, see section 6 of our response.

4. Do you agree that the mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition in the provision of data based overlay services? If so, how can this be addressed? Which parties should be involved?

Consumer trust in the payment system is paramount, and should not be compromised (see section 3 of our response for details).

However, for card payments, there are already routes for third-party providers to have access to systems to provide overlay services. Examples include Visa Developer Services, which provides an open network of Visa APIs, allowing anyone to transform great ideas into new digital commerce experiences (see section 4.4 of our response for details).

Our view is that the safe, managed access provided for third-party providers of overlay services is working, and we do not see a case for regulatory intervention.

5. In the New Payments Architecture (NPA), do you agree that global transaction data held in the central infrastructure could help providers develop overlay services? If so, what are those services and how could they deliver benefits? If not, why?

See question 7 below.

6. What models could the NPSO introduce to allow PSPs to get access to global datasets?

See question 7 below.

7. Should all regulated PSOs – including interbank and card scheme operators – be required to provide some access to global transaction data?

As described in section 4 of our response, there are already opportunities for third parties to access Visa's systems and data in a controlled and managed way, for example through the Visa Developer Platform and we are already collaborating with other parties to pursue new ideas relating to data. Therefore, we believe that any action from the PSR is needed to reduce restrictions around access to global datasets.

Additional sharing of data for any application would also introduce risks around data security and data protection (described in section 5 of our response).

Therefore, we are not in favour of new requirements for PSOs to provide access to global datasets.

8. 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? (related to developing new industry-wide fraud and anti-money laundering (AML) prevention measures)

While we support initiatives to use data to support fraud prevention and detection, or anti-money laundering, there is a tension between sharing industry-wide data and data protection requirements (amongst other tensions such as data security). In Visa's case, we generally process data on behalf of our clients, and are not the 'data controller' in GDPR terms.

A clear permission model would be required for any move to increase data sharing, potentially with clarification from the Information Commissioner's Office. Issues around liability for the shared data would also need to be overcome.

Furthermore, we do not see issues like data protection and data security as issues that can be balanced or traded-off for other benefits. These are minimum requirements, which must not be compromised (for more detail, see sections 5.4 and 7.4 of our response).

9. Are there any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them? If so, what are these barriers?

The competitive and dynamic card payments market continues to deliver new products and services that benefit consumers. Many of the examples and success stories described in the section above were supported by data. For example, the data collected as part of a contactless payment enables built protection from unauthorised use, giving consumers confidence to embrace the new way to pay (for more information and examples, see section 4 of our response).

Given the data-related innovations that continue to be delivered in the card payments sector, we do not see barriers to adoption, we do not see a case for any regulatory action in this area.

10. Are there other payments data-related issues that could, directly or indirectly, affect our objectives?

Two other issues the PSR should consider if moving forward with any proposals relating to data sharing are:

- Arrangements to handle quality or completeness issues with data provided (e.g. due to technical issues).
- Recovery of the operational costs relating to providing, collating and managing global datasets, which should not place an unfair burden on some companies and not others (noting that any costs will ultimately be passed on to consumers).