PSR Payment Systems Regulator

Response paper

Data in the payments industry

Response to our discussion paper

September 2019

RP19/1

In this document we set out the feedback we received to our discussion paper DP18/1, *Data in the payments industry* (June 2018), and our responses.

If you have any questions, you can email us at **PSRPaymentsDataProject@psr.org.uk** or write to us at:

Payments Data Project
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

You can download this paper from our website: psr.org.uk/psr-publications/policy-statements/rp19-1-response-to-discussion-paper-data-in-payments-industry

Contents

1 Executive summary

1.1 This paper sets out the feedback we received to our June 2018 discussion paper DP18/1, *Data in the payments industry*, and our responses. In the discussion paper, we asked stakeholders for their views on:

- data in the payments industry
- payments data usage
- end-users' willingness to share data
- access to scheme-wide datasets[1]
- realising the benefits of enhanced data

1.2 We received 20 responses. Most respondents recognised the potential benefits of increased payments data use. However, they also raised several issues, such as the need for more clarity on legal definitions of data and processing of data, and the lack of well-defined use cases to justify opening access to scheme-wide data.

1.3 We have concluded that the move to the New Payments Architecture (NPA) provides an opportunity to look at the feasibility of opening access to the data processed over the NPA's central clearing and settlement layer (in the rest of this document we refer to this as NPA scheme-wide data), and building a data-sharing capability into the NPA. One possible first step could be to develop and publish synthetic NPA scheme-wide data.

1.4 Synthetic data is data artificially generated by a computer. It can be created by applying a machine learning model to real data to generate an artificial dataset that has similar characteristics to the real data.

1.5 Giving firms access to synthetic NPA scheme-wide data would allow them to explore potential uses for scheme-wide data without putting real transaction data at risk. If they develop use cases with the synthetic data, this may justify looking at opening access to real NPA scheme-wide data.

1.6 We will therefore work with Pay.UK to look at the feasibility of opening access to NPA scheme-wide data once it is in operation, including the possibility of first developing and publishing synthetic NPA scheme-wide data for industry use.

1.7 We will also continue to monitor developments in the payments data space to make sure it is working well for everyone.

1 In DP18/1 we referred to scheme-wide data as 'global data'.

2 Background and responses to our discussion paper

In June 2018 we published our discussion paper DP18/1, *Data in the payments industry*, which explored the opportunities and potential risks of increased data use in the payments industry. We received 20 responses. Stakeholders broadly agreed that increased payments data use has the potential to add value. However, they also raised important issues such as a lack of clarity over legal definitions of data and processing of data, and a lack of clearly defined use cases for scheme-wide data.[2] In this chapter, we provide an overview of the stakeholder feedback to our discussion paper, and our responses.

2.1 Data is an important part of the UK payments industry. It is collected, analysed and used at various points during a transaction, and plays a vital role in making sure the payment reaches its intended destination. Data is also at the core of customer security and system innovations.

2.2 The payments sector is evolving quickly, and data will play a key role in this evolution.[3] Payments data is being generated on a larger scale and at a lower cost than ever before. This is being driven by increases in computing power, affordable storage, and software that can analyse large datasets.

2.3 Consumers and businesses are also changing the ways they pay for goods and services, increasingly relying on non-cash payment methods. As the volume of electronic payments has increased, so has the volume of data.

2.4 Alongside these changes, there have been various regulatory changes and policy initiatives designed to give third parties access to payments data (with customers' consent)[4], while simultaneously strengthening the legal framework around use of data that identifies individual people.[5]

Our discussion paper

2.5 In June 2018 we published our discussion paper DP18/1, *Data in the payments industry*. The paper explored the opportunities and potential risks of increased data use in the payments industry and the potential role that regulators could play to ensure these opportunities benefit end-users.

2 Scheme-wide data is data on all the transactions in a particular payment system. In DP18/1 we referred to scheme-wide data as 'global data'.
3 For example, the move to a Common Credit Message using the ISO 20022 standard for UK interbank payments.
4 These include the Open Banking Standards and the second European Payment Services Directive. Other competition and regulatory bodies, such as the Financial Conduct Authority and the Competition and Markets Authority are responsible for implementing and overseeing these initiatives.
5 The General Data Protection Regulation (GDPR).

2.6 In the paper, we asked stakeholders for their views on the following:

- **Data in the payments industry:** The types of payments data and the different ways data can be classified.
- **Payments data usage:** Where payments data could be used to generate benefits, and the different ways that firms use data.
- **End-users' willingness to share data:** Potential reluctance of end-users to share their data with providers of overlay services[6], which may limit innovation.
- **Access to scheme-wide datasets:** Potentially opening access to scheme-wide data to allow firms to develop overlay services, such as new ways to detect and combat fraud and financial crime.
- **Realising the benefits of enhanced data[7]:** Potential barriers to adopting enhanced data, such as investment costs.

2.7 We also held an industry workshop on these issues in July 2018. We had 40 participants from a wide range of organisations, including payment service providers (PSPs), payment system operators, trade organisations, technology providers, and other regulators.

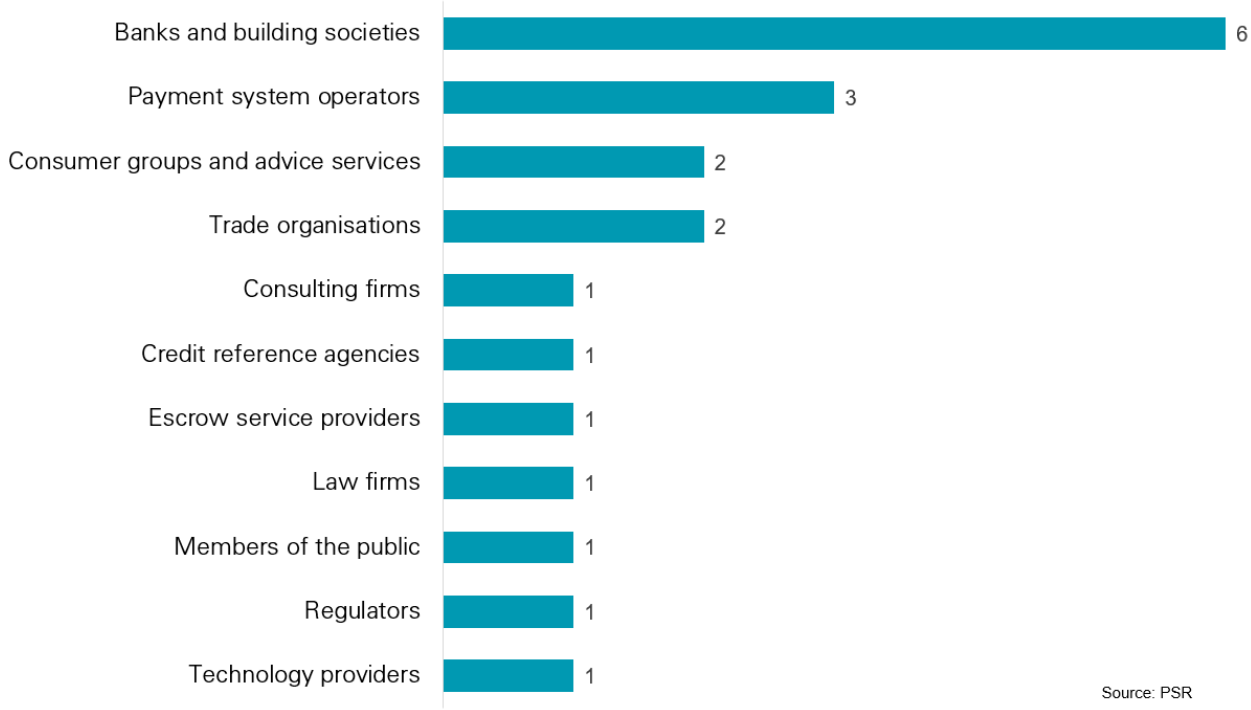
6 Payments-related services such as transaction data analytics and Confirmation of Payee.

7 Enhanced data is the technical capability to add, associate, retrieve and access increased amounts of information to payment instructions, in a structured and standard form. Enhanced data will be made possible in the NPA by the ISO 20022 messaging standard.

Responses to our discussion paper

2.8 We received 20 responses. The largest number were from banks and building societies (see Figure 1).

Figure 1: Breakdown of respondents by organisation type



Source: PSR

Views on data in the payments industry

2.9 We asked stakeholders whether they agree with our assessment of data types and the different ways that payments data can be classified.

Most respondents wanted clearer data definitions

2.10 Respondents said we need to differentiate between data collected as part of core payment services (the information necessary to securely initiate and complete a payment transaction) and other types of data. To this end, they suggested that we work closely with Pay.UK in defining types of data and how they are collected and classified.

2.11 Some respondents said the discussion paper did not cover Direct Debits and data collected by indirect PSPs. Others said we did not account for sponsoring banks submitting data into payment systems on behalf of agency banks.[8]

8 A PSP has indirect access to a payment system if it has a contractual arrangement with an indirect access provider to provide payment services to its customers using that payment system. An agency bank is an indirect PSP that has its own sort code, which is provided by its indirect access provider.

2.12 A few respondents said card payments data is fundamentally different to interbank payments data. They said card payments data is a rich dataset that should be included in any description of data flows in the industry.

2.13 Respondents said they wanted clarity on what counts as personal and non-personal data. They said any data related or linked to an identifiable person should be considered personal data, not just data that serves to identify an individual party to a payment transaction.

2.14 Respondents said we assume it is possible to anonymise personal data so that it is not personal even though it may be possible to re-identify such data.

2.15 Most respondents highlighted the need for us to work with the Information Commissioner's Office (ICO) to gain clarity on 'special categories of personal data'.[9]

Our response

2.16 As outlined in the discussion paper, we define payments data as including:

- all the information collected by PSPs and other third-party providers in the process of providing core payment services
- the ancillary information collected as the payment is being processed[10]

Although our definition of payments data encompasses both, it distinguishes between data collected as part of core payment services (as described in paragraph 2.10) and ancillary data.

2.17 Data on Direct Debits, indirect/agency PSP transactions, and card payments data should be considered in any general discussion on and description of data types and flows.

2.18 We will discuss data types and classification with Pay.UK in our work with it on potentially opening access to NPA scheme-wide data (discussed in paragraphs 2.53 to 2.57). Pay.UK is the body responsible for delivering the NPA.[11]

2.19 The ICO is the competent authority for General Data Protection Regulation (GDPR) issues. In its guide to the GDPR, the ICO states that personal data is data that relates to an identified or identifiable living individual. This is data that can be used alone or in combination with other data to identify specific individuals.[12]

2.20 Personal data does not only include specific identifiers such as a person's name or bank account number. It can also include any identifier that could be used in combination with other data attributes to reveal someone's identity (for example, an HTML cookie).

9 Under the GDPR, special categories of personal data include racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership. It also includes genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.

10 Ancillary data is the information captured that is not always necessary to process a payment. For example, the location where the payment was made, or information on the device through which the payment was made.

11 The NPA is the conceptual model for the future development of the UK's retail payment infrastructure. Pay.UK will deliver it in stages, with the core clearing and settlement layer forecast for implementation after 2021.

12 ICO, *Guide to the General Data Protection Regulation* (May 2019): ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

2.21 The GDPR does not define non-personal data. Firms must assess whether data relates to an identifiable individual, in which case it would be personal data and subject to the GDPR. If it does not, the data would not fall within the scope of the GDPR. In deciding if data relates to an individual, firms may need to consider the content of the data, the purpose of processing it, and the impact that processing it will have on the individual.[13]

2.22 Truly anonymised data cannot be used to re-identify an individual. Anonymising data involves stripping personal data of sufficient elements that mean the individual can no longer be identified and cannot at any point be re-identified.[14]

2.23 The ICO also provides GDPR guidance on special category data and the legal basis for processing it.[15]

Views on payments data usage

2.24 We asked stakeholders whether they agree with our assessment of where data could be used to generate benefits.

Respondents said using or exploring the potential of payments data requires a lot of resources and care

2.25 Most respondents said although payments data could be used to generate benefits for end-users along the value chain[16], not all firms have the resources to do this.

2.26 Some respondents said there is sometimes an incorrect assumption about who owns the data that is used to analyse possible unmet market demands. They said care should be taken to inform all applicable parties as to where data ownership lies and what consequences that ownership may have.

Our response

2.27 In DP18/1 we detailed a range of benefits that could stem from payments data use, such as developing personalised products and services, detecting fraud, and compiling statistics.

2.28 We recognise that firms may need to use significant resources to derive these benefits and to develop other potential uses for payments data. Firms need to determine the appropriate investments in data capabilities (for example, using cost benefit analyses).

2.29 Exploring further uses for data requires care to account for, and minimise, any associated risks and to inform parties of their obligations. Innovation can only happen safely if data is properly secured.

13 As above.
14 ICO, *Guide to the General Data Protection Regulation* (May 2019): ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/
15 ICO, *Guide to the General Data Protection Regulation* (May 2019): ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
16 See Figure 6 in DP18/1: psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf

Respondents said we need to consider the roles of data controllers and data processors

2.30 We asked stakeholders whether we accurately described the different ways that firms use data.

2.31 Many respondents said government and public bodies use payments data for policy development and statistical purposes. For example, HM Revenue and Customs uses payments data for tax payments, while the Office for National Statistics uses payments data to assess the size and health of the UK economy.

2.32 Respondents said we need to consider the different roles of data controllers and data processors because holding data does not mean an organisation is able to use it for commercial purposes. They said payment system operators and infrastructure providers are highly limited in how they can use the data they hold, due to contractual restrictions (under system participation agreements) and wider legal duties.

Our response

2.33 The GDPR specifies different legal obligations for two types of entities: data controllers and data processors.

2.34 A data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[17]

2.35 Data controllers are responsible for specifying the purpose of processing personal data under the GDPR. The purpose the controller sets applies to any data processor operating on the controller's behalf. For example, if a data controller sets contract performance as a basis for processing a set of data, the data processor cannot use the data for any other purpose.

2.36 In the context of UK payment systems, financial institutions (for example, PSPs) are usually the data controllers.

2.37 A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[18] Data processors can only operate within the limits set by the data controller and can only act on the controller's documented instructions. Data processors must also obtain the controller's consent before appointing any sub-processors.

2.38 In the context of UK payment systems, data processors include payment system operators (for example, Pay.UK) and infrastructure providers (for example, Vocalink).

17 GDPR Article 4 (7).
18 GDPR Article 4 (8).

Views on end-user willingness to share data

2.39 We asked stakeholders whether they agree that a mismatch between consumer trust in established brands and new third-party providers could lead to harm in innovation and competition.

Respondents said robust and transparent data security practices are key to building consumer trust

2.40 Respondents said trust levels vary across demographics and evolve as new entrants gain profile and support from a growing customer base. They also said this will only slow – not stop – innovation and competition in the payments industry.

2.41 Some respondents said consumers are generally reluctant to share data with anyone. Education and a shift in perspective are needed to create a situation where people are willing to share their data. They said any provider with access to consumer data should be accredited and the accredition list made public.

2.42 Respondents said third-party providers need to clearly communicate safeguarding practices and adhere to agreed standards to build trust. They also said it was important for consumers to see that the same regulation for data-based services applies to both established players and new entrants.

2.43 Respondents said a robust security framework, including common security standards, is key to encouraging consumers to give consent to use their data. In addition, consumers need to understand how their data is being used and who has access to it.

2.44 Some respondents said Pay.UK could play a role by developing and operating an assurance regime, as well as acting as a market catalyst for sharing payments data. They also suggested that the industry and regulators could play a role by developing and adopting a single, common, and trustworthy approach for sharing payments data.

Our response

2.45 Implementing an accreditation scheme for all firms that have access to consumer data would be impractical because every firm has consumer data in some form. Responsibility rests with firms to make sure they have appropriate data use policies in place that meet both legal requirements and consumer expectations, and to communicate those policies to their customers.

2.46 Robust and transparent data safeguards are critical for building people's trust and, where necessary, obtaining consent to use their data. Firms need to clearly communicate their data security arrangements to their customers.

2.47 Work is underway on common messaging standards, including security standards. Pay.UK is developing a core standard messaging suite using the ISO 20022 global standard which will facilitate the payments proposition of the NPA and replace existing payments standards in the Faster Payments Scheme and Bacs, and build on the enhanced data requirements from the Payments Strategy Forum. The NPA will also require common security standards.

2.48 In addition, the Bank of England and Pay.UK have jointly developed the Common Credit Message – an ISO 20022 message that will be used for both CHAPS and the NPA core standard messaging suite.

Views on access to scheme-wide datasets

2.49 We asked stakeholders whether they agree that scheme-wide transaction data held in the central infrastructure could help third-party providers develop overlay services.

2.50 Several respondents said the term 'global datasets', which we used in DP18/1, is ambiguous and confusing. We have now adopted the term 'scheme-wide' datasets to better describe such data.

Most respondents said use cases for scheme-wide datasets remain unclear

2.51 Respondents said although data could potentially be used to deliver customer benefits through innovative new products and services, there are no concrete use cases for scheme-wide datasets yet. One respondent said there is a need for market research to understand the size of the potential market for overlay services.

2.52 Several respondents said potential overlay services may include the following:

- **Transaction monitoring:** Fraud and anti-money laundering alerts; onboarding and Know Your Customer processes; additional payer and payee data to facilitate a per-payment risk score.
- **Operational services:** Use of AI and machine learning services to increase straight-through processing rates and support for reconciliation services, including data matching and enrichment.
- **Commercial uses:** Cross-selling; identifying demand for services to inform investment opportunities.

Our response

2.53 Scheme-wide data has the potential to promote innovation and deliver customer benefits, but the use cases need to be made clearer. Industry would be best placed to develop potential use cases. However, firms need access to relevant data to work through the available information, experiment, and develop business propositions.

2.54 The move to the NPA provides an opportunity to look at the feasibility of opening access to the data processed over the NPA's core clearing and settlement layer (i.e. NPA scheme-wide data) and building in a data-sharing capability because the system is currently being developed and procured. One possible first step that could provide firms with useful data while mitigating data protection and security concerns could involve developing and publishing synthetic NPA scheme-wide data.

2.55 Synthetic data is data artificially generated by a computer. It can be created by applying a machine learning model to real data to generate an artificial dataset that has similar characteristics to the real data.

2.56 Giving firms access to synthetic NPA scheme-wide data would allow them to explore potential uses for scheme-wide data without putting real transaction data at risk. If they develop use cases with the synthetic data, this may justify looking at opening access to real NPA scheme-wide data.

2.57 Given the lack of well-defined use cases, we do not consider it appropriate for us to require regulated payment system operators to open access to scheme-wide data at this point. However, we will work with Pay.UK to look at the feasibility of opening access to NPA scheme-wide data, including the possibility of first developing and publishing synthetic NPA scheme-wide data for industry use.

Respondents suggested several different models for PSPs to access scheme-wide datasets

2.58 We asked stakeholders what models Pay.UK could introduce to allow PSPs to get access to scheme-wide datasets.

2.59 One respondent said Pay.UK could develop scheme-wide datasets on a commercial basis.

2.60 Another respondent suggested the following access models:

- Pay.UK generating data extracts where it then acts as a broker for transactional data sharing.
- Access to data stores through application programming interfaces.
- Access to a common 'sandpit' environment hosted and managed by Pay.UK.

2.61 Since access management would be a common challenge across all models, the respondent suggested that access could be offered at tiered levels (for example, Pay.UK could allow greater levels of access for anti-money laundering and fraud detection, as opposed to more commercial purposes).

2.62 One respondent said we should consider different standards for different types of data. For example, information provided in real time and data containing personal information could have higher standards than anonymised, scheme-wide, or time-lagged data.

2.63 Some respondents suggested leveraging the Open Banking infrastructure to manage end-user consent.

Our response

2.64 As discussed in paragraphs 2.53 to 2.57, we do not consider it appropriate for us to require regulated payment system operators to open access to scheme-wide data at this point. However, we will work with Pay.UK to look at the feasibility of opening access to NPA scheme-wide data in the future, including the possibility of first developing and publishing synthetic NPA scheme-wide data for firms to explore potential use cases.

2.65 If it is practical to implement, one possibility could be to make the synthetic data public, with no access restrictions. This would mean a wide range of firms could freely explore the data and potentially develop use cases.

2.66 However, there may be compelling reasons to limit access to the synthetic data. If that is the case, access models such as those suggested by respondents would be considered.

Respondents said payment system operators should only provide limited access to scheme-wide data

2.67 We asked stakeholders if all the regulated payment system operators should be required to provide some level of access to scheme-wide transaction data.

2.68 Most of the respondents said access should not be for marketing or commercial purposes, but to help firms develop services that benefit end-users and increase the integrity of payment services – particularly by preventing fraud and money laundering.

2.69 Some respondents said it would not be appropriate to place obligations on infrastructure providers to give access to the data that flows through their systems because they cannot provide access without the data owner's permission.

2.70 One respondent suggested that a flexible approach that allows businesses to choose how to allow access to scheme-wide data (more secure and expensive as opposed to less expensive approaches) should be pursued.

2.71 Some respondents pointed out that a cost benefit analysis would be necessary before requiring payment system operators to grant access to the data they hold because creating such infrastructure is costly.

Our response

2.72 If it is practical to open access to scheme-wide data – real or synthetic – it would only be for the NPA. The NPA is currently being developed and procured, so there is an opportunity to build in data-sharing capabilities.

2.73 There are already ways for third parties to access card data (for example, the Visa Developer Platform and Mastercard Developers). We don't consider there is currently a case for us to intervene with respect to access to card scheme-wide data.

2.74 As part of looking at opening access to NPA scheme-wide data, legal limits, such as the GDPR, and potential limits to data use would be explored. For example, access might only be provided for use cases that have been identified using synthetic data, or only for certain types of data.

Respondents said there is tension between potential innovation and data protection requirements

2.75 We asked stakeholders if there is tension between developing industry-wide transaction data analysis tools and data protection requirements.

2.76 Respondents said there is tension between the potential innovations stemming from payments datasets and the need to adhere to data protection and other legal requirements, especially the GDPR.

2.77 Some respondents said complete anonymisation of data might resolve the conflict between the GDPR and broader access to scheme-wide datasets.

Our response

2.78 If data is prepared in a certain way, it may be possible to use it within the regulations on data protection and other legal requirements.

2.79 For example, one possible way is by anonymising the data. This involves stripping personal data of sufficient elements that mean the individual can no longer be identified and cannot at any point be re-identified. The GDPR does not apply to anonymised data.

2.80 Synthetic data, if prepared appropriately, should also fall outside the GDPR because the data would not represent or be linked to identifiable individuals. It is created by generating artificial data values.

Views on realising the benefits of enhanced data

2.81 We asked stakeholders if there are any other data-related end-user solutions, apart from enhanced data, where there could be potential barriers to organisations adopting them.

Respondents said the significant investment required and legal limitations on data use pose barriers to adoption

2.82 Most respondents said the ability to capture and utilise enhanced data requires substantial investment. One respondent said we should consider the complications of enhanced data. For example, the optimal interoperability and ubiquity of the Confirmation of Payee service[19] will require consistency of naming convention, or the ability to link related data that may have considerable differences in presentation.

2.83 One respondent said the mandatory inclusion of additional data fields could have both a positive and a negative impact. They said while standardisation will improve straight-through processing and provide additional information, the additional information may increase the potential cost and add more friction to the process for PSPs and corporates.

2.84 Some respondents said migrating to ISO 20022 will take time and substantial investment. It will therefore likely be some time before the benefits are realised.

Our response

2.85 ISO 20022 is a global standard for financial messaging. This standard allows participants, operators, and systems in different markets to communicate in a consistent message format.[20]

19 Confirmation of Payee is a service that checks whether the name of the account that a payer is sending money to matches the name they have entered.

20 wearepay.uk/what-we-do/standards/iso-20022/

2.86 Pay.UK and the Bank of England are leading the implementation of the ISO 20022 standard within their infrastructures. The standard will be used for both the NPA and the Bank of England's renewed real-time gross settlement (RTGS) system, including for CHAPS payments.[21]

2.87 As part of the change, it will be important to strike a balance between richer data made possible by using this global standard and potentially adding more cost or friction to payment processes.

Other payments data-related issues

2.88 We asked stakeholders if there are other payments data-related issues that could affect our objectives.

Respondents said cybersecurity and data breaches were key issues

2.89 One respondent said in addition to understanding the regulatory position on access to scheme-wide data, there is a need for greater understanding of the operational and information security implications of allowing more parties to access scheme-wide datasets in the central infrastructure.

2.90 Some respondents said the increased load and speed of data in payment systems will have system resilience implications. One respondent suggested that we should do further analysis to map the business case, cost, operational and resilience implications of access to scheme-wide data, as well as the implications of processing significantly larger data messages. This business case should include how enhanced data is captured, retrieved and presented.

2.91 Some respondents said our view of how data flows in and out of the UK was unclear, particularly in relation to card scheme transactions (which tend to be global in nature). They said we need to clearly determine the types of card transactions that would be relevant to the scope.

2.92 Respondents said there is a need to identify how data is managed, by whom, and how it is stored, owned and controlled.

2.93 They also said cybersecurity and data breaches affect not only the financial system, but also consumer behaviour and attitudes towards the market.

Our response

2.94 Providing access to synthetic data should not have system resilience implications because it would not contain real payments data. As part of assessing its practicality, its potential impact on industry and payment systems would be considered.

2.95 We are only concerned with data relating to UK payment systems because they fall within our remit.

21 bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme

2.96 We don't consider there is currently a case for us to intervene with respect to access to card scheme-wide data. There are already ways for third parties to access card data (for example, the Visa Developer Platform and Mastercard Developers).

2.97 Any data breach that leads to compromised consumer data could have negative impacts on consumer confidence and trust. These effects could go beyond the scheme-wide data and could have a negative impact on consumer confidence in other areas. One advantage of the synthetic data approach is that it will allow firms to explore scheme-wide data and potentially develop use cases without the risk of compromising real data.

2.98 Generally, cybersecurity approaches need to be risk-based, with common security standards and requirements as opposed to different standards for different types of firms (for example, financial institutions versus financial technology firms).

2.99 While regulators play an important role in setting standards and ensuring oversight, industry stakeholders have a direct relationship with consumers and therefore play a key role in securing consumer trust. This includes communicating how data is managed, stored and controlled.

Next steps

2.100 We have gathered a lot of useful information from the responses to our discussion paper and our subsequent discussions with stakeholders.

2.101 We have concluded that it is not appropriate for us to require regulated payment system operators to open access to scheme-wide data at this point because of the lack of well-defined use cases.

2.102 However, the move to the NPA provides an opportunity to look at the feasibility of opening access to its scheme-wide central clearing and settlement data and building in a data-sharing capability because it is currently being developed and procured.

2.103 Access to NPA scheme-wide data may help firms develop new or improved products and services such as anti-fraud and anti-money laundering tools and improved reconciliation services.

2.104 One possible first step that could provide firms with useful data while mitigating data protection and security concerns could involve developing and publishing synthetic NPA scheme-wide data.

2.105 We will therefore work with Pay.UK to look at the feasibility of opening access to NPA scheme-wide data, including the possibility of first developing and publishing synthetic NPA scheme-wide data for industry use.

2.106 We will also continue to monitor developments in the payments data space to make sure it is working well for everyone. If we identify issues that affect our objectives, we will consider whether we need to take further action.

Annex
Questions from the discussion paper

In DP18/1, we proposed a list of questions related to data in the payments industry. The questions are set out in this annex.

The collection and classification of payments data

Question 1: Do you agree with our assessment of:

- the types of data in the payments industry that are relevant for this paper?
- the types of data collected by different entities in the industry?
- the different ways that payments data can be classified?

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?

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?

Access to scheme-wide/global datasets

Question 5: In the New Payments Architecture (NPA), do you agree that scheme-wide/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 New Payment System Operator introduce to allow PSPs to get access to scheme-wide/global datasets?

Question 7: Should all regulated payment system operators – including interbank and card scheme operators – be required to provide some access to scheme-wide/global transaction data?

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

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?

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, where are these barriers?

Other payments data-related issues

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

PUB REF: RP19/1

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: psr.org.uk