PSR Payment Systems Regulator

DP18/1

Discussion paper: Data in the payments industry

June 2018

We welcome views and evidence which will help to inform our assessment of the key questions outlined in this discussion paper.

If you would like to provide comments, please email these to us by 5pm on 3 September 2018 at PSRPaymentsDataProject@psr.org.uk. Alternatively, please write to us at:

PSR Payments Data Project Team
25 The North Colonnade
Canary Wharf
London E14 5HS

We will consider your comments on this report when preparing our response to this consultation.

Contents

1 Executive Summary

With this discussion paper, we want to start a conversation on how data is used in payment systems, so we can make sure it works for everyone.

The UK's payments sector is rapidly evolving and data is becoming increasingly important. The way payments data is collected, used and shared presents opportunities for payment service providers (PSPs) and end users – the people and organisations that use payment systems. For instance, it could create new business models and improve access for new entrants into the sector, stimulating competition and innovation. It could also enhance the detection of financial crime and strengthen protections for end users. However, some of these opportunities – particularly those that could benefit end-users – might not happen through market forces alone.

We want to understand what role we might play to make sure new uses of data work well for the people and businesses that use payment systems. This could be through removing barriers to setting up new services, or through mitigating risks associated with them.

We have identified three key areas which could directly affect our objectives:

- Some people may be reluctant to share the data attached to their payments.
- Potential providers of new services may have limited access to data about transactions across a whole payment system.
- There are potential barriers that could stop consumers and businesses getting the benefits from additional 'enhanced' data attached to transactions.

We have also identified a number of issues that could potentially affect our objectives indirectly. These are either due to market competition and technological change, or are issues where other regulatory agencies have the lead role.

We want to gather industry and stakeholder views on our findings to make sure we can take the right actions. In particular, we want to hear how changes in data use could have an impact on our objectives, and where we could consider developing policies or taking action to unlock benefits for end users, or reduce risks where appropriate.

Data in the payments industry

1.1 Data is an increasingly important part of the UK payment industry.[1] Data is collected, analysed and used at various points during a payment 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.

1 See paragraph 4.3 for a discussion of what we consider payments data to constitute.

1.2 The UK payments sector is fast evolving, and we expect that data will have a key role in this evolution. Changes in the sector are being driven by a variety of market, technological, end-user and regulatory factors that have data at their core.

1.3 Technological change is leading to payments data being collected, processed, shared and used in digital form at lower cost and on a larger scale than ever before. The ability to access increasing amounts of data offers potential market opportunities such as business models based on collecting and processing data. This is all driven by increases in computing power, affordable storage, and software that can analyse large data sets to gain new insights.

1.4 End-users – the people and organisations that use payment systems – are also changing the ways they pay for goods and services, with an increasing reliance on non-cash methods. These all generate payments data. And as the volume of electronic payments has increased, so has the volume of data.

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

1.6 Other new initiatives have sought to change and enhance the amount of information sent within a payments message.[2]

Our analysis into payments data

1.7 In our early scoping work on payments data, we noted that the increased collection, analysis and sharing of payments data could drive innovation, resulting in more payment products and services being available to end-users. It could also influence how companies gain competitive advantage, which could ultimately affect market structure and the nature of competition in the sector. This could mean end users get a reduced range or quality of services. The increased commercial use of payments data could also have implications for end users in terms of privacy, data protection and product choice.

1.8 Against this background, we want to inform our own thinking about the potential impact of data on the issues relevant to our objectives. Within the context of our statutory remit, we want to understand the opportunities and potential risks of the changing treatment of data in the payments industry. We also want to see if there are areas where we should consider developing policies or taking action, and have put forth initial suggestions for discussion.

2 In June 2018, the Bank of England published a consultation paper setting out proposals for the design and implementation of a messaging standard to be used in CHAPS. This also proposed a common adoption of the messaging standard across the retail systems, Bacs and Faster Payments, to be implemented in the New Payments Architecture (NPA).

Our findings

Data collection, analysis and use in the payments industry

1.9 We consider 'payments data' to be a mix of financial, transactional, behavioural and other types of data, which PSPs and other entities collect in the process of providing payment services to end users. We found a number of ways in which payments data can be classified – for example, by the identifiability of individual people, or how individual transaction data is aggregated to form global transaction datasets.

1.10 We examined how payments data is currently collected and processed in a typical transaction involving interbank payment systems, card payment system and ATM transaction. We found a number of points in the transaction chain where data could be used to valuecreate commercial products or improve services. This could be done by, for example:

- selling the raw data itself to other entities
- analysing the data and generating insights
- applying insights from the data

1.11 However, there are legal obligations associated with data collection and use. UK data protection legislation imposes obligations on parties that collect, process and use data that identifies living individuals (directly or indirectly).[3] Those who can be identified by the data (data subjects) have rights under this legislation and, from 25 May 2018, have increased levels of control over how their personal data may be used. Those who collect payments data also have obligations under other laws, including anti-money laundering (AML), counter-terrorism and anti-fraud laws.

1.12 We found that, where permissible under their data protection obligations, or required under other laws, payments firms use the payments data that they collect to (amongst other uses):

- provide services and personalise products
- develop and improve products and services
- cross-sell products and services
- prevent and detect fraud
- derive commercial value, for example through selling statistical reports
- comply with regulations

3 In particular, the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Potential PSR policy issues

1.13 We have identified three potential areas where data use could directly affect our objectives, and where we may have a role in helping to remove barriers that could prevent the realisation of data-related opportunities, and therefore end-user benefits from arising. These areas include:

a. **Some people may be reluctant to share the data attached to their payments with third-party companies providing other payments-related services ('overlay services'):** End-users may be reluctant to share their data with providers of overlay services if they have concerns that their data may not be treated appropriately. This may limit the potential benefits that end-users may derive through newer and more innovative payment services.

b. **Potential providers of new services may have limited access to data about transactions across a whole payment system ('global' datasets), including those needed to develop new industry AML and anti-fraud measures:** Global datasets combine all the transactions in a payment system, and the analysis of global datasets can potentially be valuable in so far as it provides insights about the totality of transactions processed through the system. In particular, access to certain global transaction data can potentially allow for the development of new ways to detect and combat fraud and financial crime, new methods for avoiding scams, and new approaches to AML compliance (which could potentially lower costs, increase access to payment systems and enhance competition and innovation).

c. **There are potential barriers that could stop consumers and businesses getting the benefits from additional 'enhanced' data attached to transactions:** Some of the services that the Payment Strategy Forum anticipated in its strategy for payments[4], particularly enhanced data, will make it possible for new forms of data about the end-users to flow through the payment systems. Our engagement with stakeholders, and evidence from the Forum's consultation, indicated that certain factors could affect the adoption of these services.[5]

1.14 We have also identified a few other payments data related issues that could potentially affect our objectives in a more indirect way. To the extent to which these issues interact with our objectives, we propose (where appropriate) to work with other regulators to jointly take action. Issues identified include:

- the impact of high fixed costs on the collection, analysis and use of data
- the potential for enhanced price differentiation

4 Payments Strategy Forum, *A Payments Strategy for the 21st Century*, (November 2017) Paragraph 5.47 https://implementation.paymentsforum.uk/strategy

5 See also paragraph 6.48.

2 Introduction

The purpose of this discussion paper

2.1 We have statutory objectives to promote competition and innovation, and to ensure that payment systems are operated and developed in the interests of service-users. Since our inception, we have focused on creating market and regulatory arrangements to foster innovation and competition in the payments industry. This includes our work on improving access to payment systems and promoting competition in central payments infrastructure. We also created the Payments Strategy Forum to identify user needs and encourage collaborative innovation.

2.2 Data is seen as an area of emerging interest in the payments industry: specifically, how it is collected, used and shared within the payments industry. Better and new uses of payments data could transform the payments landscape over the next few years.

2.3 In 2017, we began scoping our work on data, and identified that the increased collection, analysis and sharing of payments data could:

- drive innovation, leading to more payment products and services being made available to end-users
- influence how PSPs gain competitive advantage, which could affect the structure of the market and the nature of competition in the sector
- affect end-users, with implications for privacy, data protection and product choice

2.4 We noted three particular points about privacy and data protection:

a. Data protection laws only apply to personal data (data which could be used (directly or indirectly) to identify a living person) – so will not be relevant to all the data flows we discuss in this paper.

b. Data protection laws do not apply to data about legal persons such as corporate entities, including most retailers and merchants (although confidentiality obligations may apply to their organisational data).[6]

c. Data protection is the responsibility of the Information Commissioner's Office (ICO) and not within our own remit. Organisations within the payments sector must work within the legislative framework that applies to the processing and use of personal data. As of 25 May 2018, this includes the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

6 Data protection laws only apply to personal data (data which relates to a living individual who can be identified). Information Commissioners Office, Key definitions of the Data Protection Act, what type of information is protected by the Data Protection Act: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

2.5 More broadly, a number of recent regulatory and policy developments have affected the way the payments sector collects and uses data. These include the Open Banking Standards Initiative (introduced following the CMA's retail banking market investigation), and the second European Payment Services Directive (PSD2). Other competition and regulatory bodies, such as the Financial Conduct Authority (FCA) and the Competition and Markets Authority (CMA), are responsible for implementing these initiatives and policies.[7, 8]

2.6 We want to start a conversation with our stakeholders about the impact data could have on our objectives. We want to:

- understand the opportunities and risks associated with the increasing collection and use of data
- find out if there are areas where we should consider developing policies or taking other action

2.7 Our work focused on data collection, analysis and use by payment system operators (PSOs), central infrastructure providers and payment service providers (PSPs). This falls directly within our statutory remit. However, there are other important interactions between different participants in the payments industry, and an unduly narrow scope could miss important insights. For example, third parties are expected to have greater involvement in data collection and analysis, which could involve using data from PSOs or central infrastructure providers.

2.8 Therefore, we are considering payments data within a broad frame to take account of how a range of participants collect, share and use payments data.

What we have done

2.9 In developing this paper, we built on our initial scoping work by carrying out additional research and analysis to understand the emerging trends and debates with respect to payments data. This included desk research into data completed by academics, regulators (both UK and international) and sectoral organisations (including consumer organisations).

2.10 To better understand how the issues are perceived by the industry, we spoke with different stakeholders in the payments industry about their data collection, use and sharing practices. We also discussed their concerns about upcoming data-related changes in the payments sector.[9] In total, we had 14 meetings involving PSPs, PSOs, consumer organisations and industry organisations.

7 The PSR has a role with respect to certain access elements under PSD2. Refer to PSR guidance: www.psr.org.uk/sites/default/files/media/PDF/PSR-PSD2-Approach-and-PPG-September-2017.pdf

8 See also chapter 6 and annex 2.

9 We did not make use of our information-gathering powers under section 81 of FSBRA.

2.11 A number of bodies are responsible and have oversight for different aspects of the collection, protection and use of data in the UK payments sector. We met with the CMA, ICO and FCA to understand their perspectives. We also met the UK Regulators Network (UKRN) and the UK Competition Network (UKCN) to learn about data collection and analysis issues in other regulated sectors, and how these issues compare with those in the payments sector.

Work by other organisations on data in the payment sector

2.12 Payments data issues are becoming more and more important in policy discussions in the UK, the EU and internationally. Regulators, industry groups and other stakeholders have also examined the subject. Annex 1 contains an overview of work done by the CMA and UK Finance in the UK and work that organisations such as the EU and the OECD have done globally. We have used insights from these sources in this paper.

Structure of this discussion paper

2.13 This paper presents our initial findings and gives stakeholders an opportunity to contribute to and inform our future work. In particular:

- **Chapter 3** explains market, technology and end-user changes that are leading to increased data collection, analysis and use in the payments industry. We also look at regulatory requirements.
- **Chapter 4** defines payments data and describes how it is gathered and classified. This includes who collects what data and what happens to it.
- **Chapter 5** sets out our understanding of how PSPs use payments data.
- **Chapter 6** gives our view on payments data issues that could affect our aims to enhance competition and innovation or otherwise benefit service users. This includes removing barriers to data-related opportunities (and therefore end-user benefits), and limiting the risks associated with data.
- **Annex 1** provides an overview of the work done by other bodies in relation to data.
- **Annex 2** provides an overview of data-related regulatory and policy developments.

Next steps

2.14 We welcome your views and evidence. This will help us assess the questions outlined in this discussion paper.

2.15 Please send your views to PSRPaymentsDataProject@psr.org.uk by 5pm on 3 September 2018.

3 Data in the changing payments landscape

The UK payments sector is evolving fast, and data is key in this development. Changes include technological advances, shifts in end-user behaviour and opportunities created by digital payment methods. There have also been important regulatory and policy changes. All of this will have a significant impact on the way data is collected, processed and shared. This will lead to opportunities for new business models that rely on improved access for entrants. It will also provide scope for more effective protection for the people and businesses that use payment systems such as better financial crime detection.

Introduction

3.1 The rapid evolution of the UK payments sector is being driven, in part, by factors with data at their core. This means it is particularly important to understand the role of data in payments. In this section, we look at four general areas:

- **Technological changes:** This includes the process of capturing, storing and using increasing amounts of digital information.
- **End-user changes:** How consumers and businesses are changing how they pay for goods and services.
- Market opportunities: How technological changes and increasing amounts of data can deliver commercial, customer and other benefits.
- **Regulatory and policy changes:** This includes the Payment Strategy Forum initiatives, the Open Banking Standards Initiative, PSD2 and the introduction of the General Data Protection Regulation (GDPR).[10]

Technological changes

3.2 Digital technologies have been an economic driving force since the emergence of computers and information and communication technologies (ICT) in the 1970s. The growth in the volume of digital information has been phenomenal and continues at an exponential rate. Research suggests that 2.5 quintillion bytes of data is now created every day. It is also claimed that some 90% of the data in the world today has been created in the past two years alone.[11]

10 As part of the RTGS renewal programme, the Bank of England will also consult on a new ISO 20022 standard in June 2018: www.bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme

11 IBM, *Bringing Big Data to the enterprise*, 2012

3.3 Digitisation (capturing, storing and using increasing amounts of digital information) has transformed entire sectors of the economy – including the payments industry.

3.4 The most obvious impact of digitisation in the payments sector is the increase in the type and amount of data that PSPs, PSOs and third parties collect. Organisations such as regulators, central banks and government departments are following the same trend. As more people and businesses shift from cash to digital payment methods, the rapid digitisation of the payments sector is expected to continue. And as the costs of collecting, storing and analysing data decrease over time, data could be collected and analysed on an ever-larger scale.

Changes in end-users' behaviour

3.5 People are changing how they pay for goods and services thanks to developments in ICT, the internet, increasing computing power and mobile devices.

3.6 These changes can be seen in:

- **The declining use of cash and cheques:** In 2006, cash was used for 62% of all UK retail payments. By 2016, this had fallen to 40%. By 2026, this figure is expected to decline further to 21%.[12] By 2026, debit cards (plastic and tokenised) are predicted to overtake cash as the payment method most used by consumers.[13]
- **The rise of internet banking:** The use of the internet for banking activity by UK adults has risen by 33 percentage points since 207, to 63% in 2017.[14] Moreover, over 77% of adults used internet banking to make payments for the purchase of goods and services in 2017. This represents an increase of 24 percentage points since 208.[15]
- **The rise of mobile banking:** Mobile banking in the UK is expected to reach 32.6 million users in 2020, up from 17.8 million 2014. The total value being moved through mobile apps is projected to reach £3.4 billion a week in 2020, up from £1.7 billion a week in 2014. Analysis has suggested that technological developments allowing for this increase in mobile banking can help reduce barriers to entry for new providers.[16]

12 Payments by value. Payments UK, Extract from UK Cash and Cash Machines Summary 2017, Page 2

13 Payments UK, Extract from UK Payments Market Summary 2017, Page 2

14 Office for National Statistics, *Statistical bulletin: Internet access – households and individuals: 2017*

15 Office for National Statistics, *Statistical bulletin: Internet access – households and individuals: 2017*

16 Centre for Economics and Business Research, *Future trends in UK banking, analysis and projections, (2014), page 4, 6, 10, 11*

- **The growing use of mobile payment applications:** In 2016, more than half (53%) of online payments were made using tablets and smartphones, up from 26% in 2013.[17] Some analysts suggest that by 2020, the proportion of all retail transactions made through mobile payment methods (for example, digital wallets) will reach 22%, up from virtually nothing at the start of the decade.[18] Younger people in particular are expected to lead the way in making purchases and payments on their mobile devices.[19]
- **Rapid growth of real-time payments systems:** Between 2015 and 2016, faster payments transactions increased to 1.3 billion payments. Projections by UK Finance suggest that by 2026, one-off payments processed as faster payments will grow by 77% (to 2.3 billion payments).[20] This is in sharp contrast with a 67% decrease in the use of cheques over the same period (from 471 million to 156 million payments).[21]

3.7 These changes in end-user behaviour have two important implications for data. First, non-cash payments tend to create a 'digital payments trail'. Second, more payment systems participants can use access to end-user information to generate value.

Market opportunities created by data

3.8 Organisations across many sectors, including financial services and payments, are interested in how they can use digital technologies and data to create revenue and improve business processes. This is generally known as digitalisation.

3.9 In the UK payments sector, existing providers as well as newcomers (such as fintechs) are developing business ideas that rely on payments data as a critical input. For example, Google Pay collects data (e.g. transaction and account data) from users to facilitate the provision of advertising. In turn, advertising helps to keep the service free for users.[22] Similarly, PSPs such as Money Dashboard use payments data to provide insights on their customers' spending habits (Box A below). One card scheme operator told us that data is a key asset for them and is central to the scheme's business model.

17 The UK Cards Association, *The UK Card Payments 2017*, page 6

18 Centre for Economics and Business Research, *Future trends in UK banking, analysis and projections*, (2014), page 13, 14

19 The UK Cards Association, *The UK Card Payments 2017*, page 11

20 Payments UK, Extract from UK Payments Markets Summary 2017, Page 5

21 Payments UK, Extract from UK Payments Markets Summary 2017, Page 6

22 Google Pay privacy policy: https://payments.google.com/payments/apis-secure/get_legal_document?ldo=0&ldt=googlepaytos&ldl=und; Google general privacy policy: https://privacy.google.com/intl/en-GB/how-ads-work.html

Box A: Money Dashboard: an example of the emergence of data-based business models[23]

Money Dashboard is a personal financial management application serving over 100,000 consumers. Money Dashboard offers an account aggregation service that enables users to see all their account data from different financial institutions. It provides functionality for budgeting and forecasting, allowing consumers to make decisions about how to spend their money.

Money Dashboard's business model is based on users' data and their potential market value. The Money Dashboard application is free for users whereas the data revenues equate to £8.80 per user per annum.[24] Money Dashboard's privacy policy sets out the various ways in which users' data is processed to provide services. For example, the company generates revenue by selling aggregated market research from anonymised account and transaction data.[25, 26]

Regulatory and policy developments

3.10 A number of regulatory and policy developments affect how data is collected, processed and used in the payments sector. These include:

- our work with the Payments Strategy Forum
- the Open Banking Standards Initiative, introduced following the CMA's retail banking market investigation
- the second European Payment Services Directive (PSD2)
- the GDPR and the Data Protection Act 2018

23 www.moneydashboard.com/privacy

24 www.iii.co.uk/gb-business/professional-services/money-dashboard

25 GFK Partners with Money Dashboard, Research Live, 8 August 2017: www.research-live.com/article/news/gfk-partners-with-money-dashboard/id/5026122

26 www.moneydashboard.com/privacy

3.11 Annex 2 of this paper has more detail on these developments, and we set out some of the opportunities they create in section 6. Although each development varies in terms of scope and objectives, all relate to either access to data or data protection and have three main goals:

a. Give customers greater control over how their data is processed and shared (for example, data protection provisions in the GDPR and PSD2).

b. Level the playing field in the payments sector by removing obstacles to data-sharing where customers have agreed to it, and create and adopt common standards for payment messaging (for example, access to customer account data in PSD2, the CMA's Open Banking remedy, and the Forum's recommendations).

c. Allow innovative new payment methods for service users. These could range from payment messages providing more in-depth or combined information to the pooling of payments data to identify fraud and reduce financial crime (Open Banking, PSD2 and the Forum's enhanced data proposals).

4 The collection and classification of payments data

We define payments data as the totality of the information collected by PSPs and other entities in the process of providing payment services to end-users. This includes data that is provided as part of providing core payment services to end-users and the 'ancillary data' often collected as the payment is being processed.

Payments data can be obtained in different ways, including data that is actively provided by the end-user and data that is passively obtained. There are various ways in which payments data can be classified, including classification based on: the identifiability of the data subject (whether the data is personal or non-personal); and whether the data relates to information about a specific individual transaction or comprises the aggregation of transaction data for a specific payment system into a global transaction dataset.

We examine how payments data is currently collected and processed in a typical transaction involving Bacs, Faster Payments, CHAPS, a card payment system or an ATM transaction.

Introduction

4.1 In this section, we provide a definition of payments data, outline the different ways in which payments data can be classified, and consider the types of payments data collected and used by PSPs, PSOs and ATM and Card Schemes in a typical transaction.

What is payments data?

4.2 In providing payment services to customers, PSPs and other entities (such as third-party providers or AISPs) can capture and hold a range of information about their retail and corporate customers.

4.3 For the purposes of this discussion paper, the PSR considers payments data to include (but not limited to):

a. The totality of the information collected by PSPs and other third-party providers in the process of providing core payment services to end-users.[27]

b. 'Ancillary data' that is often collected as the payment is being processed.

27 This includes third party providers or AISPs. It also includes the card schemes in the context of card payments.

Payments data collected in providing core payments services

4.4 Payments data can be collected through the use of core payment services such as:

- Debit and credit transfers[28]
- Card payments
- Mobile payments
- Digital wallet payments[29]
- Cheques
- ATM transactions

4.5 Among the types of information that can be collected through end-user use of these payment services include:

- personal or identity details of the payers such as their names, telephone numbers and email addresses
- sort codes and account numbers for the payers and the payees
- reference information for the payment
- date and time of the payment
- Primary Authorisation Numbers (PAN) for card transactions[30]

Ancillary data

4.6 However, in providing payment services, PSPs and other payment entities can also capture additional information that is not always necessary to process the payment. Such 'ancillary data' can correspond to a single transaction or the aggregation of many transactions, and includes:

- the location where the payment was made
- information regarding the channel through which the payment was made
- specific information regarding the devices through which the payment was made (for example, mobile device identification numbers, IP addresses and cookies for online payments)
- usage data such as the frequency with which consumers log on to their online/ mobile banking or payments accounts

28 Through various channels (e.g. mobile, internet, phone) and using interbank payment systems such as Faster Payments, Bacs and CHAPS.

29 Both staged and pass through wallets.

30 The cardholder number, usually a sixteen digit sequence, embossed on a card and encoded on the card's magnetic stripe and held within the chip. The UK Cards Association, Glossary: www.theukcardsassociation.org.uk/glossary/?search=P

How is payments data obtained?

4.7 At the broadest level, there are two ways in which payments data can be obtained from end-users. This includes payments data that is:

- actively provided by end-users – for example, as part of initial relationship building processes with PSPs
- passively obtained by PSPs and other payment entities

4.8 Whether data is actively or passively obtained has implications for end-user awareness of the extent to which their data is being collected and processed, including, critically, their consent for the PSP or other payments entity to do so.

Actively provided data

4.9 Data provided voluntarily by the end-user typically includes information initially collected when end users register for services provided by payment firms. This includes, for example, the name, date of birth or address of the user. This also includes information end-users provide as they use payment services, such as payee sort codes, account numbers and card PAN data.

4.10 This type of data collection is facilitated primarily by customers agreeing to a PSP's terms and conditions (T&Cs) when they open an account with a PSPs. PSPs are required under data protection law to set out the types of personal data that will be collected and processed by PSPs in providing consumers with payment services.[31]

4.11 Various changes to PSPs T&Cs may be required as result of the introduction of the GDPR.[32] The GDPR places a greater emphasis on an end-user's ability to obtain information about them.[33] It also requires consent to be given in the form of an affirmative opt-in, which is separate from other terms and conditions.[34]

Passively obtained data

4.12 Passively obtained data is gathered primarily through observing an end-user's payments-related behaviour or conduct. Most of the ancillary data in payments is collected in this way – although often users would have provided the consent for the data to be collected.

31 The Data Protection Act 2018 requires that in collecting such data, the data controller has to make certain information available to data subjects relating to: (a) who the data controller is; (b) the purpose/s for which the information will be processed; and (c) any further information which is necessary in the specific circumstances to enable the processing to be fair. GDPR adds to the above by requiring that the information presented to the data subject must be transparent, concise, easy to understand and free to access.

32 Specifically, T&C's may need to become more specific, as well as making the various 'tickbox' agreements more frequent and granular within documentation to better compartmentalise customer consent.

33 The GDPR gives individuals the power to obtain a copy of some of the personal data held about them from data controllers in a 'structured, commonly used and machine-readable format'.

34 Information Commissioner's Office, Overview of the General Data Protection Regulation (GDPR), October 2017.

Table 1: Passive methods of gathering data

Observation methods	Make up a large proportion of how firms gather the ancillary data of an end-user and can sometimes be effectively impossible for consumers to avoid. Many PSPs 'track' internet banking users on their journey from page to page and sometimes even within the page. This observation technique has been extended to other payment platforms such as mobile applications.
Inference techniques	Draw on data to 'guess' previously unattainable information about an end-user, such as age or gender, to varying degrees of accuracy. For example, grocery retailers that also offer motor insurance can use purchasing data from loyalty schemes to infer information about the characteristics of a customer's household and appropriately tailor the insurance policies they market to that customer.[35]

How is payments data classified?

4.13 Payments data can be classified in various ways, including according to:

a. The identifiability of the data subject, that is, whether the data is personal or non-personal

b. The degree of structure of the data, that is, whether data is structured, semi-structured or unstructured[36]

c. The accessibility of the data, that is, whether data is open, shared or closed to third-parties[37]

d. The degree of aggregation of the data, for example, whether the data shows an individual transaction, grouped transactions or all transactions combined together ('global data')

4.14 For the purposes of this discussion paper, the two important classificatory distinctions are between:

a. The identifiability of the data subject (and the distinction between personal and non-personal data), and

b. The degree of aggregation of the data (and the distinction between individual and global transaction data).

35 CMA, *The commercial use of consumer data*, June 2015 and Information Commissioner's Office, *Big data, artificial intelligence, machine learning and data protection*, September 2017, page 13

36 Payments Market Practice Group, *Structured ordering and beneficiary customer data in payments*, September 2017

37 For instance, as set out by the Open Data Institute. The Open Data Institute, *Closed, shared, open data: what's in a name?*, (November 2017)

Identifiability of the data subject

4.15 Data can be described as either 'personal' or 'non-personal', depending on whether it can be used to identify specific individuals:

- 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.[38]
- Non-personal data is data that is usually collected and processed in a way that identification of specific individuals is not possible.[39]

4.16 A further classification of personal data is provided under the GDPR which identifies 'special categories of personal data' as 'sensitive' personal data (for example, characteristic biometric data used to authenticate payments). PSD2 provides a specific definition of 'sensitive payments data' as 'data, including personalised security credentials which can be used to carry out fraud'. It is worth noting that data characterised by PSD2 as 'sensitive payments data' is captured within what we have referred to as payments data.[40]

Global transaction data

4.17 Individual transaction data involves information about a specific transaction that utilises a specific payment system. In contrast, the term we refer to as 'global transaction data' comprises the aggregation of the transaction data for a specific payment system. Accordingly, depending on how the data is combined and aggregated it is possible to develop different global transaction datasets for a specific payment system. For example, one global transaction dataset might provide information on all the transactions utilising the FPS system over a specific period, or for particular types of PSPs.

4.18 Depending on the type of data included in a global transaction dataset, and the degree of aggregation applied, it may be the case that a global transaction dataset could comprise some personal and non-personal information. For example, a global transaction dataset may simply comprise data on the volume of all transactions utilising a payment system over a specific period. Given the level of aggregation, this global transaction dataset is unlikely to contain personal information. Alternatively, another transaction dataset may be aggregated such that it comprises data on specific users of a payment system. For example, it may comprise the account numbers of all the users of the payment system originating form a specific PSP or type of PSP, or it may aggregate data about payments generated from a specific location.

38 Data Protection Act 2018 section 3(2), ICO Key definitions: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

39 ICO Key definitions: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

40 That is, there is no data that can be used to carry out fraud that could not be required in the processing of a payment.

4.19 In some circumstances, such global transaction datasets could potentially contain data that could be classified as personal (for example, where it contains account numbers or the names of the payer or payee, or where it is sufficiently disaggregated such that an individual could potentially be identified). As discussed in chapter 6, where data protection laws apply, those who have access to such global transaction data will need to ensure that they have received the appropriate consent of the end-user (or can rely on another lawful basis).

Data flows for typical payment systems transactions

4.20 This section sets out our understanding of how payments data is currently collected and processed in a typical transaction involving an interbank payment system, a card payment system or an ATM transaction.[41]

Interbank payment system transactions

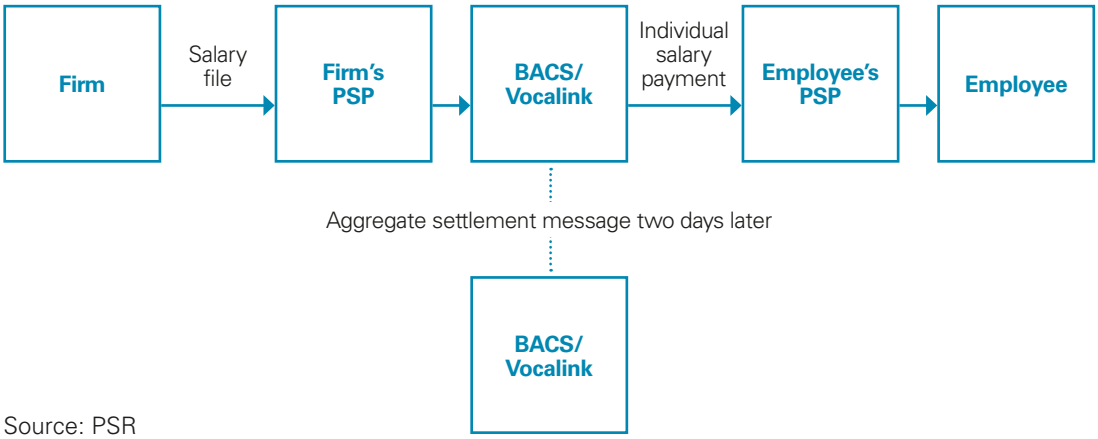
Bacs

4.21 A salary payment in Bacs is commonly known within the payments industry as a direct credit payment, and is a transaction moving money from a firm's account within a PSP to their employees' accounts, usually at multiple PSPs. The firm will submit a file that contains each of the individual salary payments, either directly to Bacs or via a third-party bureau service provider. The Bureau will submit the file on the firm's behalf into the Bacs system. Alternatively, the remitting firm could submit the transactions via a product provided by their PSP.

4.22 A Bacs payment message is based on a proprietary standard called Standard 18. This is an old payment standard which is based on a fixed number of fields within the payment message as well as the number of characters in each field. In essence, this means that there is a limited amount of data within the Bacs message. A Bacs credit file will contain a debit transaction to the sort code and account number of the firm making the salary payments. The salary payment will include, among other things, the amount, the name of the submitter, the employees sort code, account number and the employee's name.

41 This analysis for each system only considers a single type of transaction (out of the various transactions that the systems are capable of providing) for illustrative purposes. The analysis does not take account of future changes due of the introduction of the NPA.

Figure 1: Bacs Direct Credit – Simplified salary payment



Source: PSR

4.23 The Bacs system processes these files and will send on the payment information to recipient PSPs who will be able to credit their customers (i.e. the employees) accounts with their salaries on the correct date. Bacs also keep a record of each of their Direct Participant PSPs multilateral net settlement position in the system, for example how much they owe or are owed.

4.24 A payment entered into Bacs on Day 1, will be processed on Day 2, applied to the destination account and settled on Day 3. The settlement is on a multilateral net basis (so each PSP either has an amount of money it needs to pay, or an amount it will receive). Settlement occurs through the Bank of England's Real Time Gross Settlement (RTGS) System.

4.25 Data used in Bacs transactions can be classified into two categories:

a. **Personal data:** The payee's name and the sort code and accounts numbers involved in the transaction are included.

b. **Non-personal data:** The date and amount of the transaction are included.

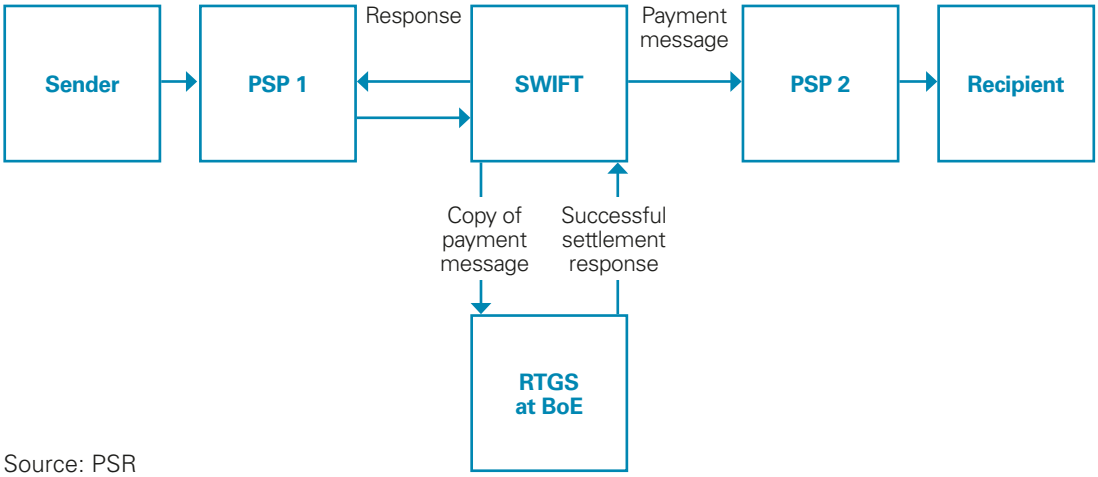
4.26 BPSL publishes global data on the aggregate volumes and values processed across the Bacs system, by product type such as direct credits and Direct Debit payments.[42]

CHAPS

4.27 CHAPS payments clear and settle simultaneously, across the Bank of England (the Bank) RTGS system. Most high value payments will be initiated by a financial institution or business rather than an individual, and could be for many reasons such as a housing purchase, the payment of a large invoice for goods or services, or as part of a financial transaction such as an unsecured money market loan.

42 www.bacs.co.uk/Resources/FactsAndFigures/Pages/AnnualProcessingStatistics.aspx

Figure 2: CHAPS – Simplified high value payment



Source: PSR

4.28 Currently, CHAPS payments use a SWIFT messaging standard called MT, and a 'customer' payment is an MT103 message. An MT103 message has a number of mandatory fields that need to be filled in for the payment to be made, and a number of optional fields that could be used if relevant, or to aid reconciliation. Within an MT103 payment, there is an an element of both structured fields, where the structure of the field is prescriptive, and free format fields where it is possible to have anything populated in it. For this reason, the amount and type of data sent across the system, in making the payment, can vary significantly.

4.29 In a CHAPS MT103 payment, the mandatory fields are: a transaction reference number, the value date, the amount (and currency), information about the sender and recipient, routine information called a Business Identifier Code (BIC) and details of any charges.[43] Optional fields include: remittance information (although the majority of MT103 CHAPS payments contain this); information on any intermediaries (i.e. other PSPs) in the chain and information to allow the PSPs involved to route the payment correctly.

4.30 While making a CHAPS payment, a direct PSP will send the MT103 to SWIFT, who will then take a copy of the message and send it to the Bank of England for settlement in RTGS. The sending direct PSP account will be debited and the receiving PSP credited with the funds. RTGS then notifies SWIFT that the transaction has been settled, at which time SWIFT sends the payment message to the receiving PSP, and a response back to the sending PSP that the payment has been made.

43 www.iso9362.org/

4.31 Data used in CHAPS transactions can be classified into two categories:

a. **Personal data:** The majority of CHAPS payments are between financial institutions or corporates but where individuals are involved in the payment, the payee's and payer's names and typically the sort code and account numbers are provided. Personal information may also be entered into a free format text field.

b. **Non-personal data:** The date and time of the transaction, the amount of the transaction, the institutions involved in the transaction and potentially addresses will be captured.

4.32 Both SWIFT and the Bank store the payment messages thereafter. SWIFT do this in case there are any discrepancies and/or investigations that either PSP needs to make. The Bank provides a Business Intelligence tool to CHAPS Direct Participants allowing them to see payment trends and download additional information.

4.33 The Bank has recently published a consultation paper which sets out its plans for the design of ISO 20022 messages within CHAPS. This proposes a format for a new, common messaging standard to payments made in CHAPS, Faster Payments and Bacs, which will also be aligned with other international systems. The core credit message (CCM) will be capable of carrying a wider range of information, and in a more structured format, including greater information on the identities of those involved in the transaction, the purpose of the transaction and remittance information. Specifically for CHAPS, the Bank proposes making it mandatory to include the Legal Entity Identifier and to identify the purpose of specific types of transaction. This is expected to drive widespread change across the payments industry, delivering benefits to the entire payments chain.

Faster Payments

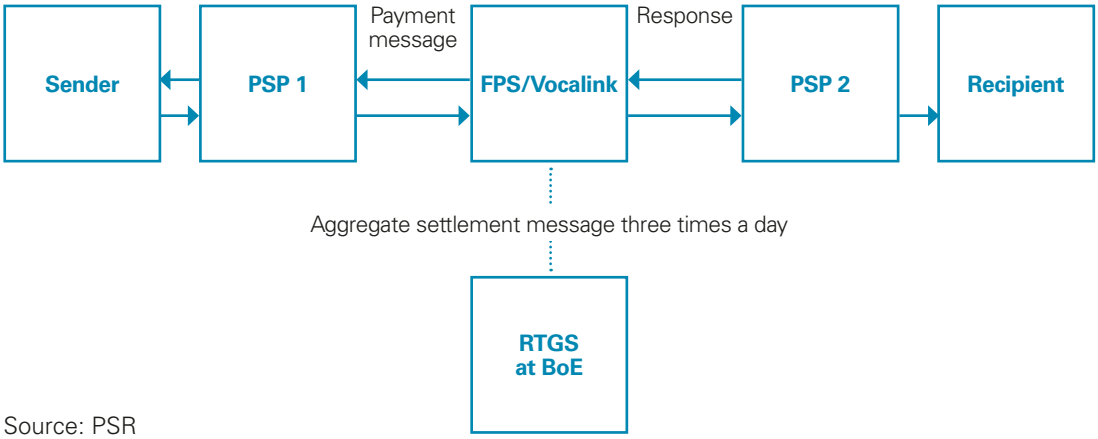
4.34 The most common payment type used within the Faster Payments system is a Single Immediate Payment (SIP). SIPs are payments that customers make when using mobile apps, telephone or internet banking. All payments processed by Faster Payments are sent and received in almost real-time between accounts. These payments are most often consumer payments, although corporates are now making higher value payments across FPS too.[44]

4.35 Typically, a consumer will not require a significant amount of information to make a SIP payment through their PSP. They are only required to enter the beneficiaries account number and sort code (or only mobile number if using the Paym service).

4.36 Faster payments use a variant of an ISO8583 message, a standard typically used for cards. The reason this is used is that, when FPS was implemented, this was the standard that allowed messaging to give an almost immediate response to the sender to say that the payment has been successful, or not. The payment message will be populated with system information from the senders PSP which will include information about the account the payment was sent from (the name of the account that the SIP was sent from and is being sent to). In addition, there will be date and identification fields; which can be used for tracking down payments should there be an issue, such as fraud or a disputed payment.

44 Corporate customers are also now more frequently using SIPs as the Faster Payments channel allows larger value payments to be processed (currently up to £250k).

Figure 3: Faster Payments – Simplified single immediate payments (SIPS)



Source: PSR

4.37 The first step in a SIP payment is the payer sending the payment via their PSP. The payment is then processed by Faster Payments, who then direct it to the correct payee PSP using sort codes. On receipt of the payment, the payee's PSP has to either credit the account or reject the payment and issue a response. They can also issue a qualified acceptance (if, for example, their system was down), which would mean that they have accepted the payment but haven't been able to credit the account straight away.

4.38 Data used in FPS SIPs transactions can be classified into two categories:

a. **Personal data:** The payer's and payee's name will be captured, including the sort codes and account numbers involved in the transaction.

b. **Non-personal data:** The date and time of the transaction, the amount of the transaction, along with the institutions involved in the transaction.

4.39 FPSL publishes global data on the aggregate volumes and values processed across the FPS system.[45]

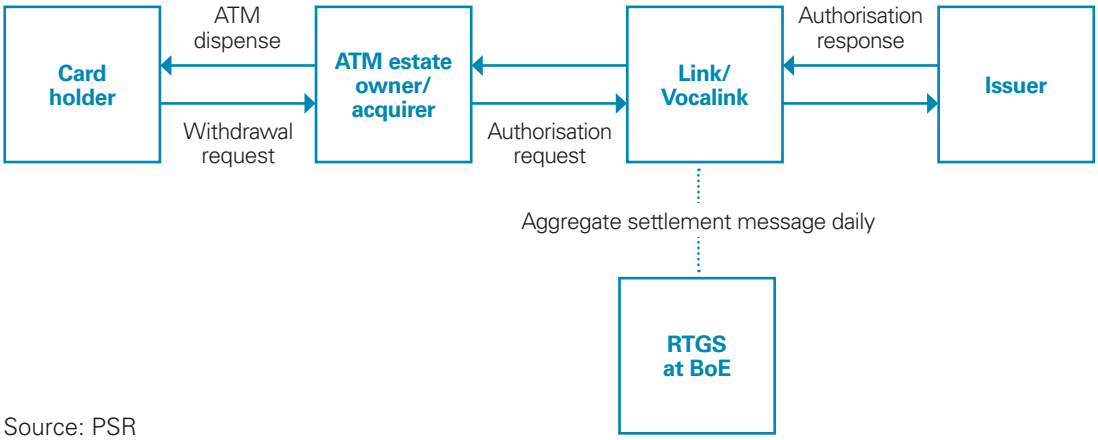
LINK

4.40 When making a cash withdrawal using a debit card from a ATM owned by a different PSP than that of the card issuer, a message needs to be exchanged with the card-issuing PSP in order to ensure that the cardholder has the funds or credit in order to withdraw the cash. An authorisation request is routed from the ATM machine to the issuing PSP and a response is sent either authorising the transaction (and money will be dispensed) or not.

45 www.fasterpayments.org.uk/statistics

4.41 The only interaction the cardholder has is correctly placing a PIN with the ATM and then the amount of cash of other services requested. No significant data is entered by the cardholder, and the information contained in the message is information about the card using the PAN number on the card (Primary Account Number) for routing to the card-issuer and account information about the ATM such as location, brand etc. and amount requested. This allows the card issuers to make a decision on whether to authorise the transaction; or whether it is fraudulent or an error.

Figure 4: Simplified LINK cash withdrawal



Source: PSR

4.42 Data used in payment Link transactions can be classified into two categories, which present three different sets of considerations:

a. **Personal data:** Authentication data required to identify the payment card and verify that its use is authorised is required. As examples, this type of data includes the card number (PAN) and the cardholder's PIN.

b. **Non-personal data:** This includes data such as the date and time of the transaction, the amount of the transaction and the location of the ATM

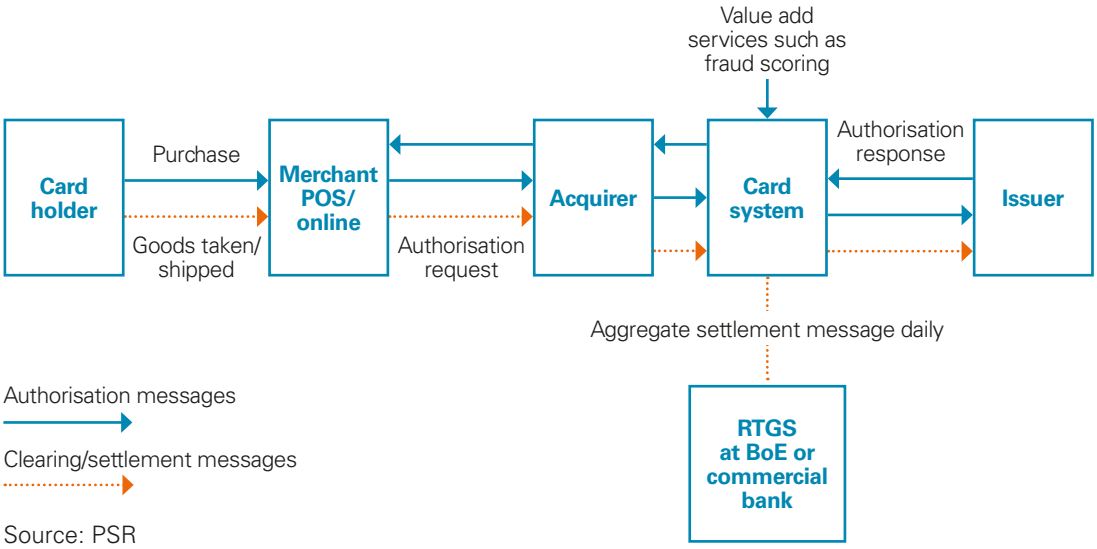
Cards payments

4.43 When a cardholder presents a payment card (credit, debit or prepaid) to purchase goods from a merchant, before any data is transmitted onwards by the merchant, the use of the card is authenticated.[46] Various methods of authentication exist for card payments: if the cardholder is using a point of sale terminal, they may be prompted to enter a PIN so that the PIN entered can be checked against the encrypted value held on a card's EMV chip.

46 For contactless mobile payments (CMP), a process named 'tokenisation' takes place. Tokenisation is a security method used in CMP Apps – a process by which a card's Primary Account Number (PAN) is replaced by a Digital Primary Account Number (DPAN). Only 'tokenised' information is ever transmitted between the mobile device and merchant's POS terminal.

4.44 If the cardholder is making a purchase from an online merchant, their name and address may be validated with their bank. For any 'card not present' transaction (that is, any that does not take place at a physical point of sale terminal), the cardholder may be asked to provide the CVC printed on the back of the card.

Figure 5: Simplified card payment



Source: PSR

4.45 If the cardholder authenticates the card and the transaction goes ahead, an authorisation message is routed from the merchant, to the merchant's bank (acquirer), on to the card scheme and eventually to the cardholder's bank or issuer. The issuing bank must decide whether the transaction is fraudulent, whether the cardholder has sufficient funds in their account to allow the transaction, and whether there is any other reason why the transaction should not be authorised. If these checks are passed, the issuing bank returns an acceptance message via the scheme and the merchant's acquirer to the merchant. These messages are sent and received in real time between the time of the customer presenting the payment card and the merchant accepting the sale. At time of receipt of this authorisation message the issuing bank will normally earmark the worth of the transaction against the customer's account but will not debit the account.

4.46 Merchants will submit card transactions to their acquirer in batches. The acquirer will batch together all transactions from all its merchants and submit these to the scheme. The scheme separates the transactions by card issuer and forwards all transactions for a given issuer to that issuer. These settlement messages are used by issuing banks to give the final amount of the transaction to be debited from the customer account, and to confirm their settlement liability to acquirers. The PSOs also send aggregated data to issuers and acquirers to assist with settlement.

4.47 Payments made using card networks are generally pull transactions: cardholders give their consent for merchants to debit funds from their card accounts. This has meant that a rule set governing how a merchant can show that the customer has allowed the payment has evolved, covering many different situations. A customer may use a payment card with an online merchant, at a point of sale terminal, via a digital wallet or at a contactless terminal. Each of these different methods of using payment cards requires different behaviour by the cardholder and the merchant, and as a result the data required for a card payment transaction needs to be flexible and comprehensive enough to allow information on how the card was authenticated and whether the transaction is likely to be fraudulent to pass between participants.

4.48 Data used in payment card transactions can be classified into three categories, which present two different sets of considerations:

a. **Personal data:** Although the cardholder's name and address are generally not used in the core payment messages, online merchants may share the customer's name and address with the issuing bank to provide an additional level of customer authentication. However, data that is required to identify the payment card and verify that its use is authorised is sensitive data, the use and transfer of which is carefully controlled. As examples, this type of data includes the card number (PAN), the cardholder's PIN and CVC code. Card security standards limit the use and distribution of this data: stolen card credentials can be used to initiate fraudulent card transactions.

b. **Non-personal data:** Data such as the date and time of the transaction, the amount of the transaction and the location of the merchant is also included in card payment messaging. 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.

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?

5 How is payments data used?

Data can create economic value in the payments sector in a number of ways. These include the selling of raw data, insights gained from data analysis and the application of these insights.

PSPs and other payment organisations also use payments data for purposes such as:

- providing services, including processing payments
- tailoring products
- identifying cross-selling opportunities
- preparing and selling statistical reports
- meeting regulatory responsibilities
- fighting fraud

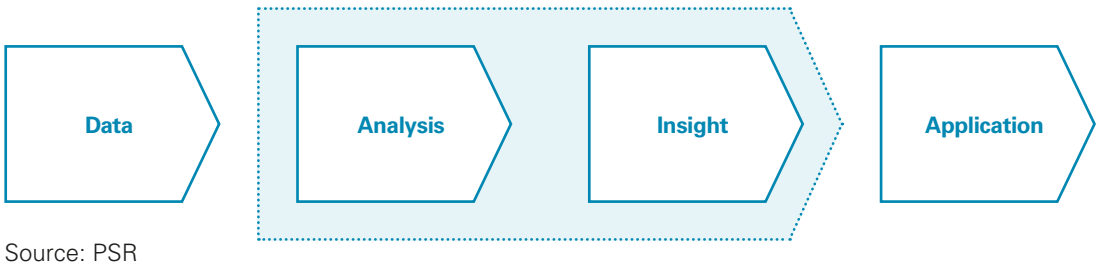
Introduction

5.1 In this section, we consider how payments data can be used. In our view, there are three general ways for data to create value in the payments sector:

- the sale of raw data
- insights from data analysis
- the application of insights

Figure 6 shows how each step informs the next.

Figure 6: Value chain of payments data



Source: PSR

Use of payments data by PSPs and other organisations

5.2 Insights from payments data can benefit the organisations that gather them as well as end-users. We describe the main benefits below.[47]

Providing personalised products and services

5.3 Personalised banking is on the increase thanks to insights gained from data. Marketing, for example, can be targeted according to an individual's specific behaviour. This is more likely to be effective than marketing based on general demographics because there can be large variations in attitudes and behaviour within these broad groups.

5.4 PSPs can use payments data to provide and manage their services. They can also use this data to build customer profiles that more accurately reflect people's habits and preferences. This allows PSPs to offer better tailored products and services that increase customer satisfaction and demand. Some PSPs, for example, share data with customers to help them understand their spending behaviour and save money.[48]

Developing and improving products and services

5.5 PSPs can also use payments data to innovate and improve their products and services. This benefits end-users because it results in better quality, greater choice and lower prices. It also encourages competition.

5.6 PSPs can use payments data to identify unmet market demand and develop products and services to meet this. Also, as markets become more competitive and data analysis becomes more sophisticated, companies will be able to track product performance and customer satisfaction more effectively. This will be particularly valuable for companies developing new products and services. It will also help companies decide if they should go ahead with high-risk products.

5.7 The potential to develop new products and services may be increased by PSD2. This allows for the introduction of new Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) who can provide customers with innovative new aggregator and payment services (see Annex 2). Sophisticated new entrants who are able to deploy new technologies may be better at analysing and drawing insights from payments data.

47 Based on an analysis of a set of standard terms and conditions of a few major PSPs across the payments value chain.

48 This Is Money article, *Lloyds launches online Money and Manager*, (February 2011).

Cross-selling non-payments based products and services

5.8 PSPs can use insights gained from analysing payments data to cross-sell products and services that are not based on payments. For example, a PSP could share someone's data (with their consent where appropriate) with its mortgage or insurance division, which could then try and sell them products.

5.9 Research by the McKinsey Global Institute shows that PSPs can use Machine Learning (ML – see Box B) to increase revenue from existing customers by as much as 10-15%.[49] Square, a financial services firm that provides merchant account and mobile payment services, uses ML insights to sell high-margin products such as loans and payroll management to current clients.[50]

Box B: Machine Learning (ML)

Machine Learning (ML) is one of the methods companies use to analyse payments data. With ML, a computer models patterns of behaviour found in huge amounts of data. It can identify differences between irregularities and patterns and use this learning to revise its models. There are two types of ML:

1. Supervised ML is Supervised learning requires that the algorithm's possible outputs are already known and that the data used to train the algorithm is already labeled with correct answers.[51] For example, the computer could be given data about people's known shopping habits and it can make accurate predictions according to how these habits change.
2. Unsupervised ML is more about finding new models and patterns in data that was previously believed to be unrelated. This helps humans learn how systems are structured.

From a payments perspective, ML can be applied to:

- Data mining
- Pattern recognition
- Recommendation engines
- Fraud detection
- Increasing revenue

49 McKinsey & Company, *Beyond the buzz: Harnessing machine learning in payments, September 2016.*

50 Barron's Next, *Square's Machine Learning Obsession is Paying Off, July 2017.*

51 Datascience.com, Supervised vs. Unsupervised Machine Learning, July 2017.

Preventing and detecting fraud

5.10 PSPs and other payments organisations can use data to identify suspicious transactions with a view to preventing fraud. Some PSPs can now apply ML to analyse data in near real-time.

5.11 One example is PayPal's Braintree Auth payments tool. This combines information about credit card transactions and verifications such as location, fingerprinting and transaction speed with more general data. The results are sent to a third-party (Kount) which creates a fraud score for each request. PayPal then uses this score to decide how it should handle each transaction.[52] Another example is Mastercard's early detection system, described in Box C below.

5.12 The Payments Strategy Forum launched initiatives such as transaction data analytics, which are designed to tackle problems including identity theft, maliciously misdirected payments and 'mule' accounts, which are used to illegally transfer money. In particular, the proposals on transaction data analytics could detect money laundering or other illegal or suspicious activity. This, in turn, will help reduce financial crime.

Box C: Mastercard Early Detection System

In October 2017, Mastercard announced a new predictive tool to help PSPs prevent fraud. The Early Detection System uses Mastercard network insights, predictive capabilities and internal and external data to determine if a card or account is at risk. It then sends a risk level score to the card issuer who can use it to decide on the action it should take. This could range from watching transactions more closely to sending out a replacement card.[53]

Mastercard's Early Detection System is available to card issuers globally. It identifies activities such as criminal trading of account data, fraudulent cards being tested before use and lower-level cases where accounts appear to be at risk.

Prepare and sell statistical reports

5.13 Some payment organisations use the payments data they collect to compile anonymised reports for internal use or sale to third parties (when in compliance with data protection laws and ICO guidance). For example, one major PSP compiled a report on the number of customers who use their contactless cards to pay for tube fares.

5.14 Another card scheme sells anonymised payments data to retailers. This allows them to send targeted messages to existing or potential customers based on their previous credit card transactions. Those targeted agree to receive the adverts in return for discounts and other incentives.

52 Braintree, Advanced Fraud Tools Overview, PayPal, 2017.

53 Mastercard, Mastercard Arms Issuers with Predictive Tool to Combat Account Related Fraud from Data Breaches, Press Releases, October 2017.

Comply with regulations

5.15 PSPs can also use collected data for regulatory checks (for example, anti-money laundering, Know Your Customer, Fund Transfer Regulations and the Foreign Account Tax Compliance Act) and to ensure regulatory compliance.[54] ML, for instance, is used to work out which data has the biggest impact and the highest value. This can be grouped according to GDPR requirements and then shown only to the appropriate internal stakeholders. This could help to ensure compliance with data privacy legislation and also streamline the organisation's work.[55]

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?

54 Steven Lewis, For banks, customer data is the new king, Retail Banker International, September 2013.

55 InfoWorld, How machine learning can be a pathway to compliance, July 2017.

6 Potential PSR policy issues

As the UK's economic regulator of payment systems, one of our objectives is to seek to ensure that payment systems take account of the interests of those that use them.[56] We also work closely with other regulators to ensure that our work is aligned. There are a number of industry, policy and regulatory initiatives, all of which have data at their core, that could positively impact on issues relevant to the PSR's objectives. These include various initiatives of the Payments Strategy Forum (the Forum) relating to payment message data flows, data pooling to improve trust in payment services and the adoption of common message (data) standards in clearing infrastructure; the Open Banking Initiative which followed from the the Competition and Markets Authority's (CMA's) retail banking market investigation; and requirements under PSD2 that PSPs provide access to customers' payments data (subject to consumers providing consent) to certain types of third party provider.

Against this background, we have identified three potential data-related areas which could directly affect the PSR's objectives, and where the PSR could consider developing policies or otherwise taking action.[57] First, we recognise that some end-users may be reluctant to share data with overlay service providers if they have concerns that their data may not be treated appropriately. This could have the effect of restricting the potential benefits that some end-users may derive through, for example, newer and more innovative payment services.

Second, we want to ensure that access to global transaction datasets is not limited only to one firm or a very small group of firms, as this may limit the scope for competition and innovation, and reduce the benefits the development of overlay services can bring to end-users. In particular, we recognise that sharing data across the industry could allow for the development of new ways to combat fraud and financial crime, but that this may be impeded if access to global data is limited, or if there is ambiguity about whether such data sharing is compliant with data protection laws.

Finally, some of the developments envisaged by the Forum, particularly around enhanced data, leverage the payment systems to provide better and more diverse customer products and services. We want to ensure that there are no unnecessary impediments to those benefits being realised.

We have also identified a number of other issues that could potentially affect our objectives in a more indirect way. These issues are either a function of market competition and technological change, or issues where other regulatory agencies have the lead role. These include the impacts of the high fixed costs in collection and use of data, and the potential for enhanced price differentiation. To the extent to which these issues materially affect our objectives, where appropriate, we propose working with other regulators to jointly address any issues.

56 Our other two objectives are competition and innovation. We also have regard to the importance of maintaining the stability of, and confidence in, the UK financial system.

57 Where action is required, we will endeavour to apply our powers in a proportionate and appropriate way. See also: PSR, *A new regulatory framework for payment systems in the UK* (March 2015).

Introduction

6.1 In this chapter, we focus on how our objectives relate to the different ways organisations collect, analyse, share and use payments data.

6.2 As the economic regulator of payment systems, we have three statutory objectives under the Financial Services (Banking Reform) Act 2013 (FSBRA):

- promote the interests of those that use or are likely to use payment systems
- promote competition in payment systems
- promote innovation in payment systems

6.3 As described below there are a range of opportunities for the use of payments data to bring significant benefits to end-users, such as new products and services suited to consumers' needs. This could encourage innovation and enhance competition in the payments industry, and therefore be consistent with our objectives. We want to ensure that there are no unnecessary impediments to the benefits associated with the use of data being realised.

Industry, regulatory and policy initiatives that could affect our objectives

6.4 In Chapter 3, we noted that the UK payments sector is evolving rapidly, in part, because of industry, policy and regulatory initiatives which have payments data at their core. In this chapter, we set out some of the potential opportunities we have identified where our objectives could be advanced, while Annex 2 provides a fuller discussion of each of the policy and regulatory changes.

6.5 The Forum has also proposed various measures that should have an impact on how payment sector participants collect, use and share payments-related data. They include:

a. **Improvements to payment message data flows to respond to end-user needs:** These include enhanced data, request to pay and assurance data. These richer payment products mean that it will be possible for new forms of data about the end-users to flow through the payment systems and potentially to be accessible to PSPs and other service providers. It is also expected that new types of entrants will want access to payments data, such as providers of transaction data analytics solutions or other 'overlay' services that will connect to the central infrastructure of the Forum's proposed new payments architecture (NPA).

b. **Data pooling to improve trust in payment services:** This involves the pooling of transaction data, customer data and other data held by PSPs with the aim of improving trust in inter-bank payment services. Among the possibilities identified for data sharing are:

- a repository for sharing payment transaction data and analytics capability
- a central utility that allows PSPs to share and store non-competitive, encrypted 'know your customer' (KYC) information
- sharing typologies and trends for anti-money laundering (AML) and other financial crime among PSPs on a near real-time basis

c. **Improving the quality of data that PSPs and other service providers have about their users/end-users:** This includes the use of common guidelines to verify and authenticate the identities of payment service users, and enhancing the quality of sanctions data.

d. **Common message (data) standards end to end:** The Forum proposed the adoption of the ISO 20022 standard for payment messages in the UK interbank systems, supporting end-to-end interoperability, innovation and alignment with international payment messaging standards.[58]

6.6 The Forum proposed the creation of the NPA, which over time will replace the current interbank payment systems (FPS, Bacs, C&CC). The NPA has a layered model that should allow third-party service providers and PSPs to plug into it and provide 'overlay services such as request to pay and confirmation of payee'. This accessibility should make the provision of new overlay services much more competitive and innovative.[59]

Open Banking

6.7 Open Banking allows customers of the UK's nine largest banks and building societies to provide third-party providers with secure access to certain current accounts in order to obtain payments and other data. The scheme was launched in early 2018 following the CMA's retail banking investigation. Open Banking establishes a set of application programming interface (API) specifications and data standards for secure financial data sharing across the UK. These specifications and standards will allow parties to develop their own apps and interfaces, leading to new products and services that will allow end-users to better manage and control their data and finances. For example, third-party providers could offer an app that allows end-users to monitor their spending habits and make payments. Alternatively, an end-user might authorise a third-party provider to use its access to its data to authorise the movement of money across accounts to avoid overdraft charges, or to make suggestions about other savings products.

58 In June 2018, the Bank of England published a consultation paper setting out proposals for the design and implementation of a messaging standard to be used in CHAPS. This also proposed a common adoption of the messaging standard across the retail systems, Bacs and Faster Payments, to be implemented in the New Payments Architecture (NPA).

59 Payment Strategy Forum, *Blueprint for the Future of UK Payments, A Consultation Paper* (July 2017), pages 5 and 7.

PSD2

6.8 The EU's second Payment Services Directive (PSD2) also requires PSPs that maintain account and payment data to provide access to that data (subject to consumers providing consent) to two specific types of third party providers: payment initiation service providers (PISPs) and account information service providers (AISPs). This change is expected to lead to entry by new players offering new and innovative services (including, potentially, social media networks, telecommunication companies and fintechs). As discussed in Annex 2, while both Open Banking and PSD2 are similar insofar as they require banks to make the data they hold on customer accounts available, the scope of the data to be made accessible and the parties affected differ between the two initiatives.[60]

Assessment

6.9 We have oversight of the Forum's proposals, including the development of the NPA, while the implementation of the other initiatives and policies are principally overseen by other competition and regulatory bodies such as the Financial Conduct Authority (FCA) and the CMA.

6.10 Nevertheless, the success of the Open Banking and PSD2 initiatives have the potential to interact with our own objectives. For example, the entry of third party providers who can access and utilise end-user data could expand the range of providers of payment services, and the types of services that they offer, and therefore serve to promote effective competition in payments markets.

6.11 Both Open Banking and PSD2 are expected to lead to entry by new innovative providers of payments services, which could also reinforce our efforts in advancing our innovation objective. Finally, all of these initiatives could bring substantial benefits to service users – by giving them more control over their data, and through the introduction of services that utilise payments data to provide more bespoke and innovative products and services.

Payments data-related issues that could directly affect our objectives

6.12 While the responsibility for ensuring compliance with data protection laws rests with other regulatory agencies, particularly the Information Commissioner's Office (ICO), how data is collected, processed and used can affect our objectives.

60 See figure 6 in Annex 2.

6.13 In this section, we set out three potential areas we have identified where data use could directly affect our objectives, and where the PSR could consider developing policies or otherwise take action. These areas include:

a. **End-user willingness to share payments-related data required for the development of overlay services:** End-users may be reluctant to share their data with providers of overlay services if they have concerns that their data may not be treated appropriately. This may limit the potential benefits that end-users may derive through newer and more innovative payment services.

a. **Access to 'global' datasets including for the development of new industry-wide fraud and AML prevention measures:** Global datasets combine all of the transactions in a payment system. Analysing global datasets can be valuable, as it provides insights about the totality of transactions processed through the system. In particular, access to certain global transaction data could facilitate the development of new ways to combat fraud and financial crime, new methods for avoiding scams (which will benefit end users), and new approaches to AML compliance (which could potentially lower costs, increase access to payment systems, and enhance competition and innovation).

a. **Realisation of the benefits of enhanced data:** Some of the services that the Forum anticipated in its 2016 strategy for payments[61], particularly enhanced data, will make it possible for new forms of data to flow through the payment systems. Our engagement with stakeholders, and evidence from the Forum's consultation, indicated that certain factors could could affect the adoption of these services.

End-user willingness to share payments-related data for the development of overlay services

6.14 As outlined above, the NPA will be designed to allow third party service providers and PSPs to provide overlay services to end users. Ultimately, these opportunities should generate benefits for end-users, such as innovative and better-quality services and lower costs for some users. However, for these benefits to be realised, end-users need to be willing to use the new overlay services, which may involve giving consent for some of their payments-related data to be shared with the providers.

6.15 Two examples of such overlay services are confirmation of payee and request to pay. Both these services require access to data from an account that is maintained by another PSP. For example, in confirmation of payee, point to point APIs may be required to enable a payer's PSP to directly query the payee's PSP to verify that the account belongs to the intended payee.

61 Payment Strategy Forum, *A Payments Strategy for the 21st Century* (November 2016).

6.16 If consumers do not consent to their data being accessed or shared, or only provide consent in certain cases or to certain parties, this could hinder innovation in the provision of overlay services. Our research into this issue broadly supports some of the conclusions of other bodies such as the FCA (e.g. in relation to PSD2) in finding that end-user willingness to share data can be influenced by various factors, including:[62]

- concerns about data protection
- levels of trust in overlay services providers
- end user ability to adopt digital payments technology

6.17 If these issues are not resolved in related initiatives such as PSD2, they may affect the development of overlay services associated with the NPA in the future.

Concerns about data protection

6.18 Some end-users might be reluctant to consent to their data being shared with third-party overlay service providers because of concerns about data protection. Specifically, end-users may be concerned about how their personal data will be used and shared by overlay service providers. Some emerging evidence indicates that, at a general level, end-user concern about how their data is shared could potentially be significant.[63]

Levels of trust in overlay service providers

6.19 Evidence suggests that trust is an important issue in determining who end-users share their data with. At a general level, the ICO's 2016 Annual Track Survey showed that only one in four adults said that they would trust businesses with their personal information. Of all the businesses considered, high street banks were the most trusted.[64]

6.20 Higher levels of trust in more established brands, such as high street banks, is confirmed by other surveys. For example, a recent Mintel study found that most people are reluctant to share their financial data with providers other than their main bank. In particular, the study finds that, only 12% of consumers were willing to share their financial data with new banks, and just 10% with financial management apps.[65] In addition, 85% of consumers interested in financial aggregation services said that they would prefer to access this type of service through their main bank's website or app.[66]

6.21 Taken together, this suggests that established PSPs that develop and offer overlay services may have a 'head-start' in attracting consumers to trust them and to share their data with them, enabling them to innovate and enhance their competitive advantage over new providers.

62 For example, the FCA has acknowledged issues of consumer trust in relation to data sharing under PSD2, www.fca.org.uk/news/speeches/payments-after-psd2-evolution-or-revolution

63 ICO, *Annual Track* (April 2016). Deloitte, *Data Nation 2012 – Our Lives in Data (July 2012)*, page 12. Marketing Week, *People Power* (March 2014).

64 ICO, Annual Track (April 2016).

65 Mintel, *Consumers and Data sharing in financial services* (February 2018), page 10.

66 Mintel, *Consumers and Data sharing in financial services* (February 2018), page 12.

End-user ability to adopt new digital payments technology

6.22 Although there has been a widespread shift towards the use of digital payments in the UK (see Chapter 3), there is a risk that certain groups might be excluded from accessing and benefitting from data-based digital services. This could be because of:

- their aversion to technology
- Inability to access technology (e.g. due to cost considerations)
- poor geographic coverage of communications infrastructure (as enablers of digital payments)

6.23 We commissioned research that shows that people in rural areas often feel excluded from technological advances and the level of choice in payment services available in urban areas of the country (such as Apple Pay, for example). Similarly, FCA research shows that older consumers and those with a disability are most likely to face challenges in accessing the Internet, and many are still unwilling to bank online due to concerns around security.[67]

6.24 As new payment solutions develop in the future and there is a widespread shift towards their usage, we expect the opportunity cost for those end-users who are unable, or unwilling, to adopt these services to increase. This is particularly likely to affect older or more vulnerable consumers. This could have implications for our service-user objective. The request to pay end-user solution in the NPA is one example of a new and innovative digital payments service that is designed to deliver advantages for end-users. However, request to pay is only likely to benefit those end-users who have digital access and are willing and able to use online and mobile banking.

Action we could take to address this issue

6.25 Overall, end user reluctance to provide access to their data due to lack of trust, data protection concerns or aversion to technology could potentially restrict demand for new overlay services, negatively affecting competition.[68] It is imperative that customers only provide this access having given their explicit consent, and it must always be their choice to do so.

6.26 Nevertheless, various stakeholders are of the view that more consistent, public information and education material needs to be made available, in order to ensure customers can make well-informed decisions, and to ensure public trust is built. We are interested in stakeholders' views on the extent of customers' reluctance and the need for action to address this.

6.27 We are also interested in views on the role of payment schemes, such as the New Payment System Operator (NPSO) and industry trade associations in providing customers with such information, as well as that of public bodies and regulators. A range of public authorities and stakeholders have an interest in this and have already issued information to customers to date.

67 FCA, *Access to financial services in the UK*, Occasional paper (August 2017), May 2017.

68 Particularly where consumers trust larger incumbents to address these issues over new entrants.

6.28 We consider that there is potentially 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. This could help end users make informed decisions about data sharing and consent. Campaigns could be launched by individual PSPs, or might be organised centrally, through an industry body such as UK Finance or through the NPSO, or by public authorities (such as the Money Advice Service).

6.29 Any consumer education campaigns could be run alongside, or be incorporated into, existing industry initiatives promoting the benefits of Open Banking and PSD2.

Access to 'global' transaction datasets

6.30 Transactions in payment systems typically involve electronic messages being sent or received, generating data about that transaction. The transactions can be combined in different ways to form different 'global' transactions datasets – data about transactions across the whole system – with varying degrees of complexity and comprehensiveness.

6.31 Most PSPs have access to their own data, and do not generally have access to global transaction data. As such they do not see the 'bigger picture' of the other transactions being processed in the system. Similarly, other service providers wanting to provide services that rely on that global data – such as third-parties that are not the operator of the payment system do not typically have access to the combined global transaction datasets.

6.32 Global datasets combine all the transactions in a payment system. Analysing them can provide valuable insights about the totality of transactions processed through the system – either within a specific period in the past, or on an ongoing, real-time basis as more transaction data is generated every second. Access to global datasets can be particularly useful in developing fraud and financial crime prevention measures. It could also be potentially useful for providers of other services such as data analytics firms, innovators or future overlay services providers.

6.33 As we discussed in Chapter 5, one of the ways in which PSPs currently use payments data is to monitor and detect any suspicious transactions with a view to preventing fraud. However, this ability is currently limited to the information available to individual PSPs, rather than than industry-level data. Global datasets can be useful in improving anti-money laundering (AML) and financial crime detection and monitoring, and reducing fraud. This could lower compliance costs for PSPs dealing with these regulatory requirements. It could also enhance competition and innovation.

6.34 A specific example of where access to global transaction datasets could be critical is for the development of transaction data analytics services. One of the Forum's proposals was to encourage the development of transaction data analytics which could help firms to meet their regulatory obligations (for example, on AML or KYC). This could also help them to reduce the incidence of fraud. For example, applying new analytical methods to global transaction datasets could allow PSPs to develop new methods for avoiding scams, which will directly benefit end users.

6.35 We have identified one case study on transaction data analytics solution in Box D, but note that in the future it may be necessary to consider the potential benefits of extending access to global transaction datasets beyond Faster Payments to other retail payments systems. This would allow such transaction data analytics services to be applied to instances where funds are effectively hidden through other payment systems.

6.36 Currently, it is our understanding that only two entities could potentially have access to global transaction datasets:

a. **PSOs:** The PSOs have the legal right to access the global data processed for their payment systems. The processes and mechanisms for this depends on their commercial agreements with their central infrastructure providers.

b. **Central infrastructure providers:** These have full technical access because they process the transactions for the payment systems. However, they have less flexibility in how they can use the data, as they are contracted by the PSO to perform specific services. This means they will generally be unable to use personal data for any other purpose without the consent of the relevant data owners.

6.37 In principle, the fact that only two entities in each payment system could potentially have access to the global datasets may make it difficult for third parties to enter the market and compete to provide overlay services that rely on that data.

6.38 These third parties may find it hard to obtain the same dataset from other sources. The challenges that they might have to overcome include:

a. **Lack of alternatives:** There is no alternative source of comparable global transaction data, given its specific characteristics (vast volumes, real-time, etc).

b. **Technical requirements:** Because of how the data is structured and stored, retrieving it can be costly. In addition, the formats and types of data available can be limited.

c. **Legal requirements:** The process of securing consent from different parties can be challenging and onerous, and may require significant legal resources.

d. **No incentive:** To protect their competitive advantage, the PSOs 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.

e. **Cost:** It could be costly for third parties to access global datasets from the central infrastructure provider, given the technical requirements, systems and processes that need to be developed for the infrastructure provider to enable access. Depending on the cost, this could serve as a barrier to entry for providers of overlay services.

6.39 Overall, these factors could affect the level of competition in the market for overlay services. They could also combine to give those who have access to global transaction datasets a degree of market power in the provision of access to this data.

Implications for the design of the NPA

6.40 A key feature of the NPA is its layered architecture and common international messaging standards, which should allow third party service providers and PSPs to provide end-user overlay services. However, the proposed NPA design also includes a centralised infrastructure for processing and clearing payment messages, which is similar to the current structure. As such, there may still be potential restrictions and barriers to developing overlay services that depend on access to global transaction datasets.

Action we could take to address this issue

6.41 We are considering if and how such potential restrictions in the access to global transaction datasets may create risks to our objective of promoting competition and innovation in the interests of service users. Where such risks exist, we are considering options so that access to global data is not unduly or unnecessarily restricted.

6.42 One option we are considering is placing a requirement on the NPSO to consider how the central infrastructure provider for the NPA can facilitate the safe and efficient sharing of global payments data with service providers using secure open access APIs. This could be similar in principle to the data sharing requirements of PSD2 and Open Banking.

Box D: The Payments Strategy Forum's proposal for a data analytics solutions

The Forum's transaction data analytics solution intends to address a wide range of fraud and financial crime threats which occur through the misuse of payments data. Its objective is to detect and prevent current and potential financial crime by creating an industry-wide function to analyse payment transaction data from all retail interbank payment systems.[69]

Real-time analysis of fraudulent payment data across all payments providers would allow providers of such services to map the payment networks and therefore accounts used by criminals. Building and understanding these networks would then allow for development of predictive algorithms, leading to real-time prevention of payment scams and other types of fraud and crime. In addition to detecting and preventing fraudulent activity, transaction analytics can also help banks get victim's money back when a fraudster is discovered and there are still funds available.[70]

The solution requires three key components:

- access to all payment transactions between paying and receiving PSPs
- a mechanism to retrieve the information and make it available for analysis
- specialist analytical engines with machine learning capability

Transaction information, financial crime information and analytical engines are currently available. However, the only means of connecting these components at industry level and for all payments types are in closed systems, normally provided by a single or consortium supplier.

As such, to reduce the risk of harm, it is proposed that the components of the solution should be connected through open-standard API technology, building on work done for Open Banking and the NPA.

This should allow third parties to access the required data, enabling multiple analytics providers to compete effectively in the market for data analytics services.

6.43 This could be achieved by including open access API requirements in the procurement requirements for the NPA's central component. In addition to addressing the access issues described above, this approach would also mitigate any competitive advantage that the central infrastructure provider might have as a result of operating a central clearing system.

6.44 Sometimes, it may be unclear what information and data can be shared under data protection laws or other commercial arrangements. One option to address this is for us to work with industry, the ICO and other relevant bodies to develop a common understanding about what data can be shared, and in what form.

69 Payments Strategy Forum, *Blueprint for the Future of UK Payments* (July 2017), page 71.

70 See PSR consultation on Authorised Push Payment (APP) scams.

Realisation of the benefits of enhanced data

6.45 The NPA is expected to drive innovation by allowing new third-party providers of overlay services into the market. One service that the Forum identified in its strategy was 'enhanced data'. This is the technical capability to add, associate, retrieve and access increased amounts of information to payment instructions, in a form that is structured and standard.[71]

6.46 Enhanced data will involve the use or transfer of payments data within the NPA. It will be facilitated by the adoption of the ISO 20022 messaging standard.[72]

6.47 The Forum's assessment was that enhanced data will generate significant benefits for end-users. The majority of these benefits will come from reduced manual and invoice reconciliation for payees.[73] However, for these benefits to materialise, enhanced data must not only be provided by suppliers in the market but also be adopted by end users (including businesses).

Box E: Enhanced Data[74]

The Forum's enhanced data end-user solution can reduce manual and invoice reconciliation costs for end-users such as corporates, government and charities.

Enhanced data will enable end-users to add more information in payment messages, avoiding the need for remittance data to travel separately from basic payment details (by post or email) as is currently the case. Users would no longer need to process and reconcile payments manually.

The Forum estimates that, between 2019 and 2031, businesses could save between £3.7 billion and £4.5 billion in invoice reconciliation costs.

However, adopting enhanced data is expected to cost end-users about £20 million. In addition, third-party PSPs and PSPs could incur additional capital costs of up to £10 million (for example, implementation costs to include additional data in payment fields).

In addition, only around 5% of large and medium sized organisations are expected to take up enhanced data at launch. This could rise to about 30% over ten years. Small and micro businesses are not expected to be large enough to justify the investment required to realise the benefit of the solution.

71 Payments Strategy Forum, *NPA Design and Transition Blueprint* (December 2017), page 63, paragraph 5.4.

72 Payments Strategy Forum, *NPA Design and Transition Blueprint* (December 2017) page 64, paragraph 5.4, page 64.

73 Excluding the benefits generated from the continuation of the existing Bacs, FPS and C&CC services. Payment strategy forum, *Cost Benefit Analysis of the NPA, NPA Blueprint*, (November 2017), pages 7 and 8.

74 Payment strategy forum, *Cost Benefit Analysis of the NPA, NPA Blueprint* (November 2017), pages 8, 9, 18 and 19.

6.48 Our engagement with stakeholders, and evidence from the Forum's consultation, acknowledged that the adoption of enhanced data may be impeded by barriers relating to:[75]

- **Costs:** Firms may require significant investments to upgrade or migrate existing systems to implement these solutions. They may be unwilling to do so unless there are cheaper alternatives available (such as systems that provide API 'bridges' communicating with the existing systems). Moreover, if the costs are such that only larger or established firms can incur them, this could have implications for the wider adoption of enhanced data.
- **Demand from end users:** Stakeholders also emphasised the need for sufficient demand to justify the substantial cost of building and implementing these solutions.

6.49 These potential impediments might also apply to other end-user solutions identified by the Forum such as request to pay and confirmation of payee.

Action we could take to address this issue

6.50 In order to address these issues, and facilitate adoption of the enhanced data, the NPSO may have a role in developing and deploying mechanisms to enable interoperability and market contestability, and end-user take up.[76]

6.51 We will monitor any potential impediments to enhanced data, and may take other action if we consider that more could be done to realise the benefits.

Payments data-related issues that could indirectly affect our objectives

6.52 We have identified a number of other payments data-related issues which could potentially affect our objectives in a more indirect way. These are either a function of market competition and technological change (such as high fixed costs of data collection and analysis), or where other regulatory agencies have a lead role (Open Banking and PSD2).

75 Payment strategy forum, *NPA Implementation Plan*, December 2017, Section 3.3, Page 20, 21, 22, 23, 24

76 Payment strategy forum, *NPA Implementation Plan*, (December 2017), Section 3.3, pages 22, 23 and 24; Payments Strategy Forum, *NPA Commercial Approach and Economic Models, NPA Blueprint*, (November 2017), pages 7 and 8.

High fixed costs

6.53 Collecting, storing and using payments data can be costly for firms. Costs can include data analysis, secure storage and research and development activity. The more cost efficient that firms are, the more likely they are to be competitive in the market.

6.54 In particular, larger firms may be able to generate economies of scale and scope when collecting, sharing and analysing payments data. This could potentially put smaller firms and new entrants at a competitive disadvantage.

6.55 At a general level, evidence suggests that data-based business can involve substantial fixed costs and low marginal costs.[77] Firms using payments data as part of their business model will need to make large initial investments in technology, infrastructure and operational requirements. One large PSP told us that is has already made very significant 'big data' investments, including in analytics capabilities and technology experts etc. Another smaller PSP also told us that it plans to make significant investments in data analytics and artificial intelligence capability in the future. One card scheme told us that it is currently investing a lot in machine learning and artificial intelligence capability to identify fraud in real time.

6.56 High fixed costs mean that larger firms that currently collect and process a large volume of payments data will enjoy lower per customer costs in comparison to smaller firms and new entrants. New entrants in the payments market may not be able to afford these costs. If these costs are too high, firms considering using data analytics may be discouraged from entering the market, which could restrict competition and innovation.

6.57 However, as a result of cloud technology and other cost-effective storage solutions, data storage costs are decreasing.[78] Cloud technology allows firms to store significant amounts of data without needing to invest in costly IT infrastructure, and it does not discriminate against smaller firms.[79] Moreover, incumbent banks do not necessary have a competitive advantage over new entrants with regards to technological development. Many large incumbents may require substantial investment to develop and upgrade existing legacy IT systems and migrate to new ones. This might level the competitive playing field for participants.

6.58 Given the recent implementation of PSD2 and Open Banking as future drivers of increased data collection and analysis, the nature and impact of this potential barrier is still evolving. Because of this uncertainty, we propose to monitor developments in this area in conjunction with the FCA and CMA.

77 CMA, *The commercial use of consumer data: report on the CMA's call for information*, (June 2015), page 75

78 Telegraph, Cloud tech is helping small firms to tap into big data (July 2017)

79 CMA, The commercial use of consumer data: report on the CMA's call for information (June 2015), page 86

Enhanced ability to price differentiate

6.59 Some payment firms will be able to use increased data capabilities to create a detailed profile of consumers' tastes, habits and purchasing preferences.[80] Because data will flow across different markets, firms, especially those that operate in more than one market, may collect data from one market and use it in another. Combining and analysing data related to consumers' habits and preferences could therefore potentially allows firms to use payments data to price differentiate – charging different customers different amounts for the same goods and services – both inside and outside the payments sector as an effective way of increasing profits.[81]

6.60 Although such differentiation could also occur in non-payments markets, this issue is potentially relevant for us because these practices are enabled by the data collected from consumers as they use payments products and services. This means it could touch on our service-user objective.

Such price differentiation can occur in different forms. For example, data collected when consumers use payment services may be used by PSPs to cross-sell other non-payments products and services that firms believe they might be interested in on the basis of their current habits. Such cross-selling may involve the provision of discounts to such customers, which may not be available to other customers, to encourage them to purchase these products and services.[82]

Although this can generate benefits for consumers, there can also be detrimental effects given that customers are less price aware when they receive product recommendations in comparison to instances when they are buying a standalone product. Without shopping around for a better deal therefore, certain consumers can end up paying more.

6.61 Similarly, by using data to build a profile of consumers' tastes, habits and purchasing preferences, firms may be in a better position to assess individuals' willingness to pay for products and services. On one hand, it could be good for people's overall welfare as customers who are less willing or able to pay could be offered low prices to encourage them to use product or service. Firms could also provide targeted discounts or offers on certain products or services that may be of interest to customers based on their habits. These types of effect can lead to benefits from increasing overall output and access to payments services.

80 Townley, C, Morrison, E, Yeung, K., *Big data and Personalised Price Discrimination in EU Competition Law*, King's College London Law School Research Paper No. 2017-38

81 This practice is opposed to traditional price discrimination where differing prices reflect the different costs of providing a product or service to consumers.

82 CMA, *The commercial use of consumer data* (June 2015), Paragraph 3.66, Page 92.

6.62 On the other hand, such price differentiation can have negative effects. For example, particular groups of consumers who are less informed or less engaged may be adversely affected as they are less able or willing to shop around for better deals and display a lower responsiveness to price changes. As a result such groups of consumers may end up paying more.

6.63 The GDPR includes provisions around the profiling of consumers through data analysis. Firms are prohibited from making fully automated decisions that have a legal standing, unless they have gained explicit consent from consumers and are transparent in disclosing their activities.

6.64 We have an interest in how data is used and propose to monitor developments in this area, in collaboration with other regulators, for example, under the auspices of the UK Regulators Network (UKRN).

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?

7 Next Steps

Responding to our discussion paper

7.1 We welcome views and evidence which will help to inform our assessment of the key questions outlined in this discussion paper.

7.2 If you would like to provide comments, please email these to us by 5pm on 3 September 2018 at PSRPaymentsDataProject@psr.org.uk. Alternatively, please write to us at:

PSR Payments Data Project Team
Payment Systems Regulator
25 The North Colonnade
Canary Wharf
London
E14 5HS

7.3 We will consider your comments on this report when preparing our response to this consultation.

Disclosure of information

7.4 Generally, we will seek to publish views or submissions in full or in part. This reflects our duty to have regard to our regulatory principles, which include those in relation to:

- publication in appropriate cases
- exercising our functions as transparently as possible

7.5 As such, we would ask respondents to minimise those elements of their submission which they wish to be treated as confidential. If respondents include extensive tracts of confidential information in their submissions, we would ask that they submit non-confidential versions which they consent for us to publish. We will also not accept blanket claims of confidentiality, and will require respondents to identify specific information over which confidentiality is claimed, and to explain the basis on which confidentiality is sought. Despite this we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request.

7.6 Respondents should note that we will not disclose confidential information that relates to the business or affairs of any person, which we receive for the purposes of our functions under the Financial Services (Banking Reform) Act 2013 (FSBRA), unless:

- The information is already lawfully publicly available.
- We have the consent of the person who provided the information and, if different, the person to whom it relates.
- The information is published in such a way that it is not possible to ascertain from it information relating to a particular person (for example, if it is anonymised or aggregated), or there is a 'gateway' permitting this disclosure. Among the gateways is the 'self-help' gateway whereby the PSR will be able to disclose confidential information to certain third parties to enable or help it (or the third-party recipient) to perform its public functions. Those receiving information disclosed under the gateway are still bound by the confidentiality regime.

7.7 Our data privacy notice applies to our handling of personal information and is available to view on our website: www.psr.org.uk/privacy-notice.

Annex 1:

Work on payments data by other bodies

1.1 The CMA has carried out two studies related to the issues in this discussion paper:

a. In 2015, it published a report on the collection and commercial use of consumer data. Although not specifically about payments, it considered the benefits and risks – to consumers, companies and the economy – of increased data collection and analysis. The report looked in particular at the impact of competition and regulation on data collection and analysis.[83]

b. In 2016, it published the conclusion of its retail banking market investigation. One of its proposed solutions was the creation of Open Banking, which would allow third parties to access customer data.[84]

1.2 Payments UK, now a part of UK Finance, previously considered the issue of data in the payments sector:

a. In March 2017, it published a report focused exclusively on data.[85] This explored the increased use of data, including what that meant for the payment industry and consumers. It also considered the growing importance of data in the payments industry, the main reasons for this change and how the industry could respond.

b. UK Finance also produced a report focused on enhanced data. This considered the need for enhanced data, how it would improve the payments experience, and ways to support its delivery in the UK.[86]

83 CMA, *The commercial use of consumer data*, (June 2015)

84 *CMA paves the way for Open Banking revolution* (August 2016): www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution

85 Payments UK has been incorporated into UK Finance (UKF); Payments UK, *Changing Payments Landscape: A focus on payments data* (March 2017)

86 Payments UK, *A vision for World Class Payments in the UK: A focus on Enhanced Data with payments* (March 2016)

1.3 The European Union has carried out several pieces of work focused on data:

a. In December 2016, the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) published a joint committee discussion paper on the use of Big Data by financial institutions.[87] This considered the collection and use of data, including the analytical methods and technologies used across the banking, insurance and securities sectors. The paper gave an overview of the potential benefits and risks of Big Data for consumers and financial institutions.

b. In January 2017, the European Commission (EC) published 'Building a European data economy'.[88] This report recognised the data-driven transformation of the EU economy and stressed that data access and transmission issues are central to the emergence of a data economy.

c. In April 2017, the EU Parliament Committee on Economic and Monetary Affairs released a report on fintechs. This called for the European Commission to 'investigate the possibility of a European data sharing strategy with the aim of putting consumers in control of their data'.[89]

d. In May 2017, the EC published the final report on its e-commerce inquiry. The inquiry did not focus in particular on data-related competition concerns. It did, however, confirm that the collection, analysis and use of large amounts of data is increasingly important for e-commerce.[90]

1.4 The Organisation for Economic Co-operation and Development (OECD) has also carried out work on data in the past few years:

a. In 2014, the OECD published a consumer policy guidance paper focused on mobile and online payments.[91] This acknowledged that access and use of payment data can benefit consumers and help businesses shape services to fit customers' needs. However, because data can be misused, the OECD also set out guidance for businesses that will help them protect consumer interests.

87 Joint Committee Discussion Paper, T*he Use of Big Data by Financial Institutions*, JC 2016 86.

88 Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Building a European data economy*: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC009 FinTech: the influence of technology on the future of the financial sector.

89 *FinTech: the influence of technology on the future of the financial sector.*

90 Report from the Commission to the Council and the European Parliament, *Final report on the E-commerce Sector Inquiry – Staff working document* (paragraph 5.1).

91 OECD, '(2014), OECD Digital Economy Papers, No. 236, OECD Publishing, Paris.

b. In 2016, the OECD published a report about Big Data and its impact on competition policy. This recognised the potential for Big Data to create benefits such as new business models, product development and better customer targeting. But it also highlighted the possibility of monopolies being established.[92] This is because businesses need to be large enough to benefit from the economies of scale that data offers.

c. In January 2017, the OECD's Directorate for Science, Technology and Innovation (DSTI) published its report into the key issues for digital transformation in the G20. It identified data as 'an important 21st century infrastructure'. It concluded that access to and use of data could become a new source for growth.[93]

92 *Big Data: Bringing competition policy to the digital era.*

93 *Key Issues for digital transformation in the G20, Berlin, Germany*, 12 January 2017.

Annex 2:

Data-related industry, regulatory and policy developments

Our work on the Payments Strategy Forum

2.1 We set up The Payments Strategy Forum (the Forum) in 2015 to create a strategy for collaborative innovation in the payments industry. In 2016, the Forum published its strategy proposing measures that will affect how payment sector participants collect, use and share payments-related data.[94] They include:

- Improvement of payment message data flows to respond to end-user needs
- data pooling to improve trust in payments
- improving data quality
- common message (data) standards in clearing infrastructure

2.2 The package of solutions to end-user needs includes proposed changes to the data attached to end-to-end payment messages in legacy and new interbank payment systems. Examples include:

a. **Enhanced data:** This allows all information relating to a payment to be held in a single point of reference. End-users can also attach additional data to the payment message (such as an e-invoice or video clips). This contrasts with the current practice of having multiple points of reference.

a. **Request to Pay:** A request for payment sent through the payment system. This will give customers (or payers) greater control over automated payments and let them choose when and how to pay.

b. **Assurance data:** This is the confirmation from a payee that will allow payers to track payments once they have been made. This will help people guarantee they have paid the right person, avoid fraud and manage cash flow on a real-time basis.

2.3 These will allow new forms of data about transactions and users to flow through payment systems – and potentially be available to PSPs. For example, richer messages can be attached to a payment.

94 Payments Strategy Forum, *A Payments Strategy for the 21st Century* (November 2016).

2.4 New overlay services providers, such as data analytics providers, are also likely to have access to the data going through payment systems. This is because of the way new payments architecture (NPA) will be structured, how services will be procured, and how easy it will be for providers of new overlay services to connect to the Simplified Payment Platform (SPP).[95]

Data pooling to improve trust in payment services

2.5 The Forum also recommended that PSPs pool their transaction, customer and other data to improve trust in interbank payment services. Solutions proposed include:

a. Payment transaction data sharing and 'big data' analytics: Creating a central resource for sharing payment transaction data and analytics capability. This would aim to reduce criminal and fraudulent payments in the interbank systems, such as fund repatriation and money mule account activities. It would also help with confirmation of payer and payee issues. The data would be only used for detecting financial crime.

b. Trusted Know Your Customer (KYC) data sharing: Creating a central resource that allows PSPs to share and store non-competitive, encrypted KYC information.

c. Financial crime data and intelligence sharing: Near real-time sharing of types and trends related to fraud and anti-money laundering (AML) among PSPs in a central resource. They would also share confirmed, attempted, suspected or at-risk fraud cases. The data would be matched, mined and analysed by PSPs to identify and profile customers centrally.

Improving the quality of data

2.6 The Forum also proposed other solutions to improve the quality of user data held by PSPs or PSOs. These included:

a. **Common guidelines for identity verification and authentication:** To verify the identities of payment service users and PSPs.[96]

b. **Enhancement of sanctions data quality:** Improving data and processes for collecting and managing customer data. This would improve PSPs screen customers against the Treasury's consolidated list of financial sanctions targets.

95 The NPA will have a two-tier structure: a basic infrastructure (a thin 'core') that only performs basic push payment and only processes basic data such as bank account details, payment amount and a reference code, and centres of 'overlay services' that provide the end-users solutions and sit outside the core.

96 They include regulation such as the fourth Anti-money laundering Directive, PSD2 and industry initiatives such as Mobile Identity Authentication Standards (MIDAS), Electronic Identification and Signature (eIDAS), OIX, TISA, gov.UK Verify, etc.

Common message (data) standards in clearing infrastructure

2.7 The Forum proposed the adoption of the ISO 20022 standard for payment messages in the UK interbank systems. This would enable end-to-end interaction, innovation and compatibility with international payment messaging standards.[97]

2.8 In the NPA, common governance and technical standards using ISO 20022 will make it easier for PSPs or other participants to connect directly to the clearing infrastructure at a lower cost. This could also attract payment systems infrastructure providers in other countries, which tend to focus on ISO 20022-based infrastructures, to bid for tenders.

2.9 Since the publication of the initial strategy in 2016, the Forum has since concluded its work and delivered its final Blueprint.[98] Its work has now been handed over to the New Payment System Operator and UK Finance to deliver its vision.

Open Banking Standards Initiative

2.10 Part of the CMA's remedy package, which followed its Retail Banking Market Investigation, called for the nine largest current account providers to apply Open Banking standards.[99] These are guidelines for secure financial data sharing across the UK.

2.11 Where customer consent is given, each of the nine banks is required to give third-party PSPs secure access to specific current accounts through secure and open application programming interfaces (APIs).[100] Open Banking Limited was set up to enable this change by developing API standards for different software from different financial institutions to interact and exchange data.

2.12 The Open Banking Standards Initiative, which only applies in the UK, has a similar general objective to PSD2 (discussed below) in that it requires banks to provide access to their customer account data. However, the scope of this data and the parties affected differ slightly from that of PSD.

97 In June 2018, the Bank of England published a consultation paper setting out proposals for the design and implementation of a messaging standard to be used in CHAPS. This also proposed a common adoption of the messaging standard across the retail systems, Bacs and Faster Payments, to be implemented in the New Payments Architecture (NPA).

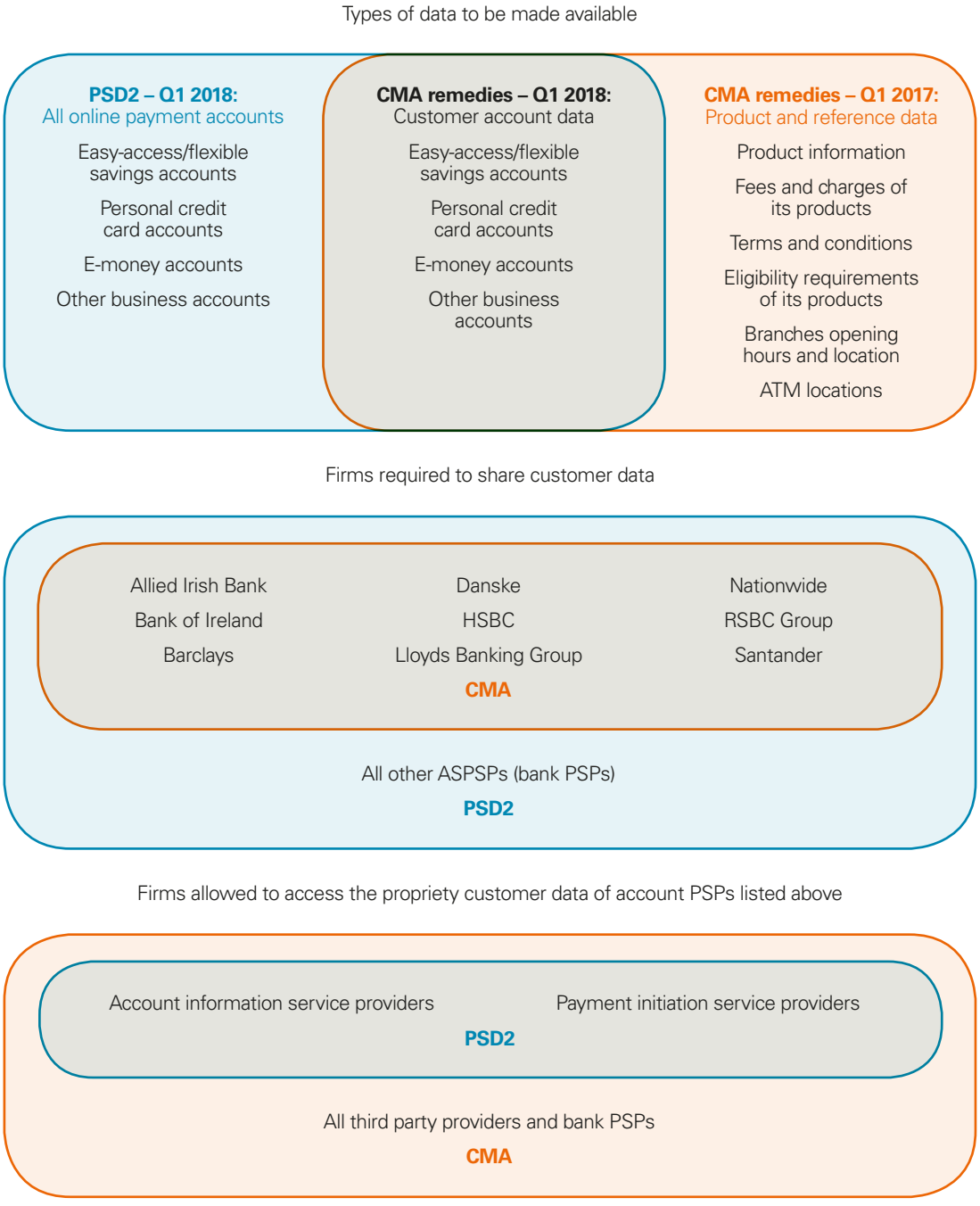
98 https://implementation.paymentsforum.uk/key-documents

99 The nine parties affected include: Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group and Santander.

100 This is in addition to a requirement for certain standardised product and reference data to be made available to authorised third parties (open data). Information Age, *Open Banking creates opportunities for banking services which were literally impossible to realise prior to January, but carries with it new risks* (April 2018): www.information-age.com/open-banking-securely-bold-world-123471686/

Figure 6: Comparison of data access requirements in Open Banking Standards and PSD2

Data access requirements in Open Banking and related initiatives: PSD2 and CMA remedies



Source: PSR

The second European Payment Services Directive (PSD2)

2.13 PSD2 came into force on 13 January 2016 and EU Member states were required to make it a legal requirement by 13 January 2018. The Financial Conduct Authority (FCA) leads on data-specific aspects of PSD2 and the PSR is involved with access issues.[101,102]

2.14 The main data-related element of PSD2 is the requirement for PSPs to provide access to customers' payments data – subject to consent – to two types of third-party providers (TPPs):

a. **Payment initiation service providers (PISPs):** PSPs that allow users to initiate payments from bank or other payment accounts held in the users' ASPSPs.[103]

b. **Account information service providers (AISPs):** PSPs that bring together information from users' bank or payment accounts held in different ASPSPs.[104] They are commonly known as account aggregators.

2.15 These requirements are aimed at preventing account-holding PSPs from restricting access to customers' payments account data without a legitimate reason.

2.16 As described in Box F, PSD2 seeks to level the playing field for new providers by ensuring that existing PSPs do not impose unnecessary barriers. This should promote competition and innovation, and payments data will have a key role to play.

Box H: PSD2 creates a new playing field for competition

One way PSD2 could improve competition is by making it easier for TPPs to compete with Card Schemes. This is because payment processing in the TPP network will not depend on the major card scheme networks. As a result, TPP payments may be highly attractive to merchants keen to avoid service charges. Large merchants could be particularly likely to wield this power by influencing customers' payment choices. This could lead to lower fees and influence the evolution of payment systems in general.

The Card Schemes have not remained passive, however. In the UK, Mastercard moved into the non-card payments sector with its acquisition of VocaLink, which enables non-card payments via its Pay by Bank mobile application. Meanwhile, in the US, both Mastercard and Visa have joined the bank-operated clearXchange P2P payments network. This puts them in a good position to support non-card payments if PSD2 and similar initiatives become popular.

101 FCA, *Payment Services and Electronic Money – Our Approach* (September 2017), page 210.

102 See www.psr.org.uk/sites/default/files/media/PDF/PSR-PSD2-Approach-and-PPG-September-2017.pdf

103 A payment initiation service is 'a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.' (Article 4 (15) of the Directive (EU) 2015/2366).

104 An account information service 'online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.' [Article 4 (16) of the Directive (EU) 2015/2366].

The EU's General Data Protection Regulation (GDPR) and the Data Protection Act 2018

2.17 From 25 May 2018, new data protection laws came into force across the EU in the form of the GDPR.[105] The GDPR aims to strengthen citizens' rights in response to developments in the digital, data-driven economy. It also introduces more privacy considerations for organisations and simplifies rules for companies in the digital single market. In the UK, the Information Commissioner's Office (ICO) is the authority primarily responsible for ensuring compliance with the GDPR. In addition, the UK Data Protection Act 2018 modernises data protection laws in the UK. Amongst other things, the Data Protection Act applies the EU Law Enforcement Directive and extends data protection laws to areas not covered by the GDPR.[106] The GDPR and Data Protection Act should be read side by side.

2.18 There are six data protection principles in the GDPR. These require personal data to be:[107]

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in ways that are incompatible with these purposes; further processing for archiving in the public interest, scientific or historical research or statistical purposes will not be considered incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, in regard to the purposes for which it is processed, is erased or rectified without delay.
- Kept in a form which can identify data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

105 General Data Protection Regulation (EU) 2016/679.

106 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

107 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Glossary

Term or abbreviation	Description
Account information service providers (AISPs)	PSPs that bring together information from users' bank or payment accounts held in different ASPSPs. They are commonly known as account aggregators.
Aggregate data	This is data that is obtained by combining the data of multiple individuals into a group. This is generally a type of non-personal data.
Anonymous data	This is data that is collected and used at the level of individuals but there is no information from which someone could be personally identified. This is a type of non-personal data.
AML (anti-money laundering)	The package of initiatives and regulations directed at preventing money laundering, including The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
Application programming interface (API)	A set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service.
ATM	Automatic teller machine.
Bacs	The regulated payment system which processes payments through two principal electronic payment schemes: Direct Debit and Bacs Direct Credit. The payment system was previously operated by Bacs Payment Schemes Limited (BPSL) but is now operated by the New Payment Systems Operator (NPSO).
the Bank	The Bank of England.
Bank of England settlement account	A settlement account in central bank money.
Cheque and Credit Clearing (C&CC)	Payment system providing net settlement of cheques and paper credits between financial institutions. The payment system was previously operated by the Cheque and Credit Clearing Company Limited (C&CCCL) but is now operated by the New Payment Systems Operator (NPSO).
CHAPS	The UK's sterling high value payment system. It is operated by the Bank of England. The CHAPS system is designated for PSR regulation, however, the PSR's regulatory powers do not apply to the Bank as operator or infrastructure provider.
CHAPS MT103	This is a SWIFT MT103 message 'customised' for the UK HVPS.
Closed data	Data that is accessible only to its subject, owner or holder.

Term or abbreviation	Description
Confirmation of Payee	A capability which will provide a payer with assurance that the account to which they are making the payment belongs to the intended payee.
CMA	Competition and Markets Authority.
End user	Those who use, or are likely to use, services provided by regulated payment systems.
Enhanced Data	This is the technical capability to add, associate, retrieve and access increased amounts of remittance information to a payment instruction in a form that is structured and standard.
FCA	Financial Conduct Authority.
FPS (Faster Payments Scheme)	The regulated payment system that provides near real-time payments as well as Standing Orders. It was previously operated by Faster Payments Scheme Limited (FPSL) but is now a wholly owned subsidiary of, and operated by, the New Payment Systems Operator (NPSO).
FSBRA	Financial Services (Banking Reform) Act 2013.
Infrastructure provider	Any person who provides or controls any part of the infrastructure used for the purposes of operating a payment system (see s.42(4) FSBRA).
Interbank (payment system)	The regulated Bacs, C&CC, CHAPS, FPS, LINK and NICC payment systems (i.e. it does not include card payment systems).
ISO 20022	An international standard for the development of financial messages.
LINK	The regulated payment system which enables end users to take cash out of their accounts (amongst other activities) using the network of ATMs in the UK. It is operated by LINK Scheme Ltd.
Mastercard	The regulated payment system supporting payments made by cards and operated by Mastercard Inc.
The New Payment System Operator (NPSO)	The NPSO is the UK's retail payment operator. The NPSO was established in 2017 as a company limited by guarantee and regulated by the Payment Systems Regulator and the Bank of England. In 2018, the NPSO consolidated Bacs Payment Schemes Limited (BPSL), Faster Payments Scheme Limited (FPSL), and the Cheque & Credit Clearing Company Limited (C&CCL). The NPSO is also responsible for the delivery of the New Payment Architecture, adopted from the Payment Strategy Forum in December 2017.
Non-personal data	This is data that is usually collected and processed in a way that identification of specific individuals is not possible. Non-personal data can either be anonymous, pseudonymous or aggregate data.
(our) Objectives	The PSR's statutory objectives as set out in ss.50 to 52 FSBRA – these are the competition objective, the innovation objective and the service-user objective.

Term or abbreviation	Description
Open data	Data that is 'readily accessible (usually published online) and available in machine-readable format. This type of data has a license permitting anyone to access, use and share it.
Operator (payment system operator)	In relation to a payment system, any person with responsibility under a payment system for managing or operating it; and any reference to the operation of a payment system includes a reference to its management.
Payment initiation service	A service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
Payment initiation service provider (PISP)	A PSP pursuing business activities of providing payment initiation services.
Payment service provider (PSP)	A PSP, in relation to a payment system, means any person who provides services to consumers or businesses who are not participants in the system, for the purposes of enabling the transfer of funds using that payment system. This includes direct PSPs and indirect PSPs.
Payments Strategy Forum (the Forum)	A forum made up of payment industry and end-user representatives with the aim to develop a strategy for payment systems in the United Kingdom. The PSR, the Financial Conduct Authority and the Bank of England attend the Forum as observers.
Payment system	A system which is operated by one or more persons in the course of business for the purpose of enabling persons to make transfers of funds, and includes a system which is designed to facilitate the transfer of funds using another payment system. Only payment systems which are designated by the Treasury are 'regulated payment systems'. (See also section 41 of FSBRA).
Payments UK (formerly known as Payments Council and now UK Finance)	An industry trade association representing the UK payments industry. Historically, it was a membership organisation set up following the OFT's Payment Systems Task Force, which included a focus on payment systems.
Personal data	This is data that relates to an identified or identifiable living individual.
Pseudonymous' data	This is data that contains personal information but identifying fields are replaced by one or more artificial identifiers ('pseudonyms'). This is generally a type of non-personal data.
PSR (Payment Systems Regulator)	The Payment Systems Regulator Limited, the body corporate established by the FCA under section 40(1) of FSBRA.

Term or abbreviation	Description
Real time gross settlement	The accounting arrangements established for the settlement in real-time of sterling payments across settlement accounts maintained in the Bank of England system.
Regulated payment system	Any payment systems designated by the Treasury in accordance with s.43 FSBRA. As of the date of publication, this included Bacs, C&CC, CHAPS, FPS, LINK, NICC, Mastercard and Visa.
Request to Pay	A flexible payment and bill management service concept that offers payers more control over bill payments that is initiated by the payee.
Semi-structured data	Does not conform to a specific model but elements or even fields within this data can be identified with markers or tags.
Settlement	The completion of a transaction or process to discharge obligations and settle claims and liabilities that arise between participants in a payment system.
Shared data	Consists of public access, attribute-based access and named access data. Public access data is available to anyone under terms and conditions that are not 'open'. Attribute-based access data is available to specific groups that meet certain criteria. Named access data is available only to named people or organisations.
Single Immediate Payment (SIP)	A payment set-up to be paid straight away.
Structured data	Follows a model that defines a number of fields. These fields each contain a specific type of data, for example address, and relate to each other in a structured way as in a database. Financial data held on individuals by Credit Reference Agencies are an example of this.
SWIFT	Society for Worldwide Interbank Financial Telecommunication, a global provider of secure financial message services.
The UK Competition Network (UKCN)	The UKCN is an alliance of the Competition and Markets Authority (CMA) with all the UK regulators that have a specific role to promote and enable competition within their sectors. The network aims to promote stronger competition across the economy for the benefit of consumers and to prevent anti-competitive behaviour in the regulated industries.
The UK Regulators Network (UKRN)	The UKRN is a network formed by 12 of the UK's sectoral regulators. The UKRN was established by its members in 2014, to provide the structure for regulators to consider common issues and policy projects with relevance across utility, financial and transport sectors.

Term or abbreviation	Description
Unstructured data	Does not conform to a specific model but is almost impossible to organise systematically. Only more recent algorithms are able to do this successfully enough to extract significant commercial value. A utilities customer's payment record could be an example of this.
Visa (Visa Europe)	The regulated payment system supporting payments made by cards and operated by Visa Europe and Visa UK Limited.

PUB REF: DP18/1

25 The North Colonnade
Canary Wharf
London E14 5HS
Telephone: 0300 456 3677
Website: www.psr.org.uk