

End User Needs Group Report Update

Draft for discussion: 03rd June 2016

‘To improve the end user experience of UK payments’

Contents

Approach taken to date.....	3
High level Description	7
Solution Description.....	8
factors for consideration	11
Cost Benefit Analysis	14
Benefits: Further Detail.....	17
Sequencing	18

Approach taken to date

This paper sets out the proposed solutions developed by the Payments Strategy Forum's End User Needs Working Group (EUNWG) to address a set of detriments identified as arising for end users – both individuals and organisations - through the PSR's consultation with the Payments Community. It records the approach taken by the EUNWG to identifying and understanding both the root causes of these detriments and how the UK's payments industry needs to adapt if effective and workable solutions are to be identified and implemented.

The Payments Strategy Forum allocated the following detriments to the EUNWG at its workshop on 13th November 2015:

1. Detriments requiring solutions to provide greater control:

- a. Poor flexibility or ease of use to control push and pull payments
- b. Difficulty in handling exceptions/failures because of lack of control
- c. No real-time pull functionality
- d. Existing payments mechanisms not keeping up with pace of change with work and living habits – for example Direct Debits
- e. Account charges for bounced Direct Debits and unauthorised Direct Debits etc. affects the disadvantaged
- f. Unlimited Direct Debit guarantee makes it difficult to provision for risk or acts as a barrier for non-Direct PSP's and end users to offer the service
- g. Direct Debits are too rigid/lack transparency for customers with unpredictable incomes ; no control over exact dates or amounts; no part payments or flexibility causing exclusion from discounts and returned payment fees
- h. Security measures have technical problems and are too complicated for consumers – this is leading to high rates of sale-abandonment

2. Detriments requiring solutions to give greater assurance:

- a. Lack of confirmation of receipt on payments
- b. Corporate service users would like to know where payments are at all times (if they are not real time) or if not have the ability to track payments at any time in the process
- c. No real-time balances causing financial detriment (overspending causing returned payments, fees)
- d. Investigation to solve issues around misdirected payments too complex
- e. Difficult to know who you are paying leads to misdirected payments and fraud
- f. Missing reference data causing misdirected payments/expensive in management of exceptions
- g. Data – limits on the extent of input and output data and no third party reporting

3. Detriments requiring solutions to support financial capability:

- a. Cost differentials between Chaps, Bacs and FPS (esp. for wholesale)
- b. Customer education – needed on channels

- c. Lack of transparency / clear information on types of payments (and products) for consumer to be able to select best choice with confidence
- d. Lack of confidence in shift to online and shift to digital – lack of trust increases costs, reduces engagement, slows move to non-cash; excludes certain users
- e. Data acts as a barrier to getting products and services – lack of transparency
- f. Transparency of users for services in corporate space
- g. Limited access to Free-To Use ATMs in some areas (Rural, out of town estates) – challenge is often lack of commercial space
- h. Difficult to make electronic payments for the unbanked causing increased cost due to use of cash
- i. Risk appetite around fraud / AML excludes many vulnerable / ‘non-standard’ customers from access
- j. Access to products and services difficult for people who don’t have ‘standard’ ID / Address or credit history causes exclusion and additional costs

The EUNWG took these sets of detriments and, using the prioritisation analysis framework provided by the PSR, ran a series of discussions to understand the specific ways in which users experience these detriments arising and where, when and why these detriments arise. This analysis led to the following grouping of the detriments into four broad themes:

1. The need for users to have greater control over the timing and amount paid: “Request to Pay”

The detriments raised by the Payments Community, along with existing research evidence, shows that control is a major concern for end-users – both payers and payees. Current solutions for both pull and push payments are not responsive enough to the needs of payers and receivers - especially in a modern labour and SME market where variable income and trading receipt patterns are increasingly the norm.

At the corporate end, in those circumstances, it is not always optimal to have to rely on a fixed mandate with risk of non-fulfilment. There are also costs and business process detriments in reconciling payments to specific invoices or customers.

For recurring payments such as utility bills, around 70% of households in the UK make use of Direct Debits and enjoy a discount from their supplier for using this payment method. However there are an increasing number of people in the UK with variable incomes, including the c4.5 million self-employed people. For many people on a variable income, the fixed nature of a Direct Debit in its current form carries a significant risk that the payment may bounce, incurring additional fees and charges. Hence this significant population of users currently pay by other means (cash, cheque, or card) and do not enjoy the benefits of a discount from their supplier. This ‘poverty premium’ can be significant; in 2012 Save the Children estimated that the average ‘poverty premium’ is around £1280 per household across all their financial interactions.

For spontaneous payments, the dominant payment form is currently the debit card, which carries a range of fees for the merchant and can result in delays to receiving payment.

There is therefore a need for a capability which allows the user to decide:

- Whether to pay (e.g. an unexpected payment date or amount, or from an unexpected source)
- When to pay (including deferring a payment to accommodate flexible income patterns)
- How much to pay (including splitting payments or querying unexpected amounts)

The EUNWG described this functionality as “Request to Pay”.

2. The need for users to have greater assurance over who they are paying and the status of their payment: “Confirmation of Payee” and “Assurance Data”

The detriments raised by the Payments Community, along with existing evidence, shows that users feel vulnerable to the risk of a payment being either misdirected or lost due to the lack of accurate information about the exact identity of the payee and the status of the payment. Thus the incentive for end users to take advantage of the benefits of paying electronically is reduced when what happens after they authorise a transaction is invisible to them. End users need more assurance that their intentions in originating or requesting payments were followed through. This goes beyond just the specifics of avoiding misdirected payments, but the prevention of any outcome other than that intended by either payer or payee.

Whilst figures for misdirected payments are not easy to pin down, the consequences for the originator of sending money to the wrong account are significant, with the banks often tied by their own confidentiality rules about what they can say to the originator and also in what they can ask of the recipient. Similarly separation of payment and transactional data processes cause large costs to industry (reconciliation, debt management), to government (tax and welfare data processing), and to individuals (tax and welfare reporting).

The lack of real time data about card payments also means that the consumer has less visibility of their true balance as debit card transactions may not be shown in the customer balance until the day following the transaction. At present it is not possible to pay in real time easily from a consumer bank account because of the lack of data carried with a Faster Payment to allow merchants to reconcile the payment with a specific purchase.

The EUNWG considered a range of information which may meet the need arising from the detriments to provide more assurance:

1. Real time balance- are there sufficient funds to cover this proposed transaction and if not pre-warn the payer?
2. Intended recipient- is the payment going to the intended recipient (and from the intended payer)? This may need to go beyond just the existence of a valid account number.
3. Intended time of transaction completion: if not immediate, is the payment on track to reach the intended recipient at the time specified?

The EUNWG named this functionality “Confirmation of Payee” and “Assurance Data”.

3. The need to be able to attach contextual data linked to a payment to facilitate better reconciliation and processing of the payment: “Enhanced Data”

Capacity to attach data to the payment providing information on “what does this payment relate to?” This included ways that an end user - typically a business or a 3rd party such as a government department - can accurately reconcile the payment with their internal systems (e.g. allocating a payment to a debt due or assessing the tax or welfare implications of its having been made).

The EUNWG named this functionality “Enhanced Data”.

4. The need for payments to play a positive role in supporting the financial capability and inclusion of users: “Financial Capability Principles”

Payments are a mechanism for moving money from a payer to a payee, usually (but not always) in exchange for receiving some good or service. Within the context of the UK’s wider financial inclusion and capability strategy, payments should enable users to make payments as effectively and efficiently as possible. The detriments raised by the Payments Community demonstrated that there is significant room for improvement so that payments:

- Are designed around real humans rather than idealised rational economic beings and are thus “simple to use”
- Maximise the value of the transaction to the payer and payee; in brief, the payment should enable the transaction rather than undermine it or leak value from it.

The EUNWG named this approach “Financial Capability Principles”.

Identifying potential solutions

Having defined these four themes, the EUNWG then ran workshops to consider in more detail existing solutions, either in development or already in the market. The EUNWG drew the following conclusions:

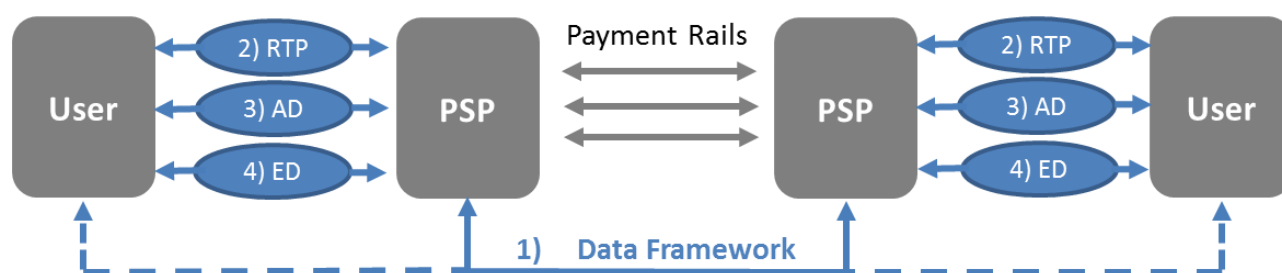
1. Whilst there are a range of emerging payment products which give the payer more control over when to make the payment and how much to pay, these solutions have not yet nor are likely to be able to provide ubiquitous and scalable solutions without industry-wide data standards.
2. Once analysed in more detail, both “Request to Pay” and “Confirmation of Payee”/“Assurance Data” essentially require payments to be linked to Enhanced Data, thus enabling the payment mechanism to provide more contextual information and facilitate greater control and information over and about the payment. Thus the three themes “Request to Pay”, “Confirmation of Payee”/“Assurance Data” and “Enhanced Data” all require a new enhanced data functionality.
3. However, merely providing new technical functionality within a competitive space may not lead to users being provided with the desired functionality; whilst the competitive market might lead to some users being able to access products with more control and assurance, the PSF’s role is to

ensure that these requirements are met for all users who need them. Thus the EUNWG came to the conclusion that some level of minimum product provision would be required to ensure that technical functionality was turned by the competitive space into a supply of appropriate products for all users.

4. Similarly to 3 above, the EUNWG concluded that the industry should voluntarily adopt a set of principles around payments design and delivery to ensure that payments benefit UK Plc, including its individual citizens, incorporating good practice and emerging knowledge around enhancing and maximising financial capability. Whilst some might argue that this work sits squarely in the competitive space, the EUNWG judged that taking a collaborative approach to agreeing core principles to ensure that payments support the UK's Financial Capability Strategy goals would ensure that the payments industry was acting responsibly in the best interests of the UK, as well as ensuring that developments in UK payments continue to be world class. The EUNWG have therefore produced a suggested draft set of Financial Capability Principles to underpin the Strategy.
5. Finally, a small set of other detriments from the original EUNWG list were, after close analysis, passed to other working groups:
 - Security measures have technical problems and are too complicated for consumers leading to high rates of sales abandonment – for Financial Crime Working Group
 - Unlimited DD guarantee makes it difficult to provision for risk or acts as barrier for non-Direct PSPs and end users to offer the service –for Simplified Access to Markets WG
 - Risk appetite around fraud/AML excludes many vulnerable no-standard customers from access - for Financial Crime Working Group
 - Access to products and services difficult for people who don't have standard ID address or credit history - For Financial Crime Working Group
 - Inflexible collection accounts cause input errors and additional costs for customers and agency banks - for Simplified Access to Markets WG

HIGH LEVEL DESCRIPTION

The aim is to create a framework for the movement of data linked to payments between PSPs, enabling new solutions requiring enhanced data and delivering against the stated detriments. The industry would then launch a number of industry wide propositions that specifically respond to the end user needs detriments



Each of the 4 elements in the model depicted above is described below:

1. Broad data framework - enabling the industry to flow data associated with payments in a consistent, secure and efficient way outside the scheme rails
2. Request to Pay – Enabling Payees to request payment from a Payer
3. Assurance Data – Enabling Payers and Payees to confirm natural identities and to use natural identities to find 3rd parties and receive confirmation of a payment's progress
4. Enhanced Data – Enabling Payers and Payees to send contextual data regarding payments linked to one or multiple payments, attaching invoices, remittance advice, warranties, financial crime data, etc. This would also provide institutions with the ability to meet their regulatory obligations, e.g. Anti-Money Laundering.
 - Key to this framework is a common reference (or link) that is used to directly associate payments with the relevant data, so that payment and data are intrinsically linked.
 - The framework will cover payments to and from all payment actors (Personal, Corporate, Retail and Government) and be capable of working with all payment types (Chaps, Bacs, FPS, CCC&C, Link and Card rails).
 - For Request to Pay, Assurance Data and Enhanced Data there will need to be a minimum level of functionality and experience that is ubiquitous across the industry, leaving user experience enhancements and alternate uses in the competitive space.
 - For consultation we have laid out how these solutions could be constructed. However it should be noted that detailed design of the resulting user experience and requirements will have to be conducted, including user testing across a wide variety of user types and user cases. We expect that constructing a detailed, robust implementation roadmap including this design phase will be part of the final KPMG report.

SOLUTION DESCRIPTION

1. Technical Standards for a data framework that is associated with payments would need to include consideration of the following:
 - PSR has posited a single such standard and the industry has for some time had a strategy to move to ISO20022, while the SAM WG had also identified a managed move to this standard

as desirable. There would be a requirement to go beyond the existing standards and engage the appropriate bodies to create an appropriate standard and mappings. (There is currently no mapping from JASON to ISO.)

- There are currently multiple market initiatives all suggesting the need for a co-ordinated data transfer mechanism (PSD2, OB) and we suggest these are considered together with recommendations from the PSF ensuring the industry develops a consistent mechanism and language for communication.
- Include appropriate Governance, Regulatory and legal standards and frameworks
- Include appropriate SLAs and industry communication and oversight forums
- Architecture to include modern flexible systems (web services), transparent API based access between users/clients
- Be open to all PSPs to use, easily and simply
- Support all payment actors: personal, retail, corporate and government
- Work across any payment type: BACS, Chaps, Faster payments, Cheques, cards and Link
- Be flexible to enable currently envisaged and future use cases
- Be fast and efficient (may limit use case if not real/near-real time)
- Be secure
- Be extendable to allow for yet to be identified use cases
- Have some form of guarantee around delivery
- Be ubiquitous and interoperable

2. To enable Requests for Payments to be sent between entities (RTP) the following features are necessary:

- Payee PSPs to have ability to create a payment request instruction that is sent to the Payer PSP and is able to be understood by a Payer PSP, which allows them present it to their Payer
- The Payer would have the ability to accept, decline, hold and respond to RtP. The Payer would also have the ability to return information to the requester (e.g. to advise they intend to pay a different amount to that requested).
- The request to include: the amount, the timeframe for responding, the preferred / allowed method of payment, whether it is of a recurring nature, and a link to enhanced data about the request. This link would enable the Payee to see more information about the request (without all of that information having to travel inside the RtP).
- Rules and Standards for encoding this information, functionality and messaging between PSPs would need to be agreed.
- Central storage of data requirements still to be determined, expected to be in competitive space. However the use of a common reference or link and associated security protocols for both the request and their associated payment must be agreed collaboratively.

- Since the solution does not require the removal of any existing payment types (such as DD), choice will continue, and competition will dictate the direction of the market (in fact a request for Payment could be a request for a DD to be set). However it is likely that at some stage the industry would have to consider whether it needs to simplify existing products/services or “turn things off” otherwise operational efficiency may be compromised.
- Consideration will need to be given to any required legal framework regarding user rights in terms of error or misuse as with DDs. Placing Payees in control of their payments and permissions through their PSP while ensuring controls and consequences are clear should enable a simplified legal framework.
- A mechanism will need to be in place to limit fraudsters setting up plausible sounding requests to defraud vulnerable customers.
- Both the request and response to have the ability to incorporate Enhanced data and operate with Authentication data.
- Payers should have the ability to set up recurring permission for 3rd party requestors with appropriate controls that can subsequently remove if required (time period, amount, and frequency).
- RTP to be real-time to enable user cases in time critical environments such as retail and transport / access.
- Each RTP to have a unique reference that would be used when sending the actual payments back to the Payee thus enabling more straightforward reconciliation. A communication will also be sent if the Payer declines the RTP with any additional data available.

3. To enable assurance data (both of customer identify and status of payment) (AD):

- Payee PSP to provider messages to Payer PSP regarding receipt of payment, processing of payment and final settlement of payment. Payer PSP to provide this information back to Payer to enable tracking of payment.
- Payer PSP able to request confirmation of Payee details to validate prior to executing payment.
 - For example, a Payer enters expected details of Payee (using a proxy such as a mobile number or sort code and account number) and receives confirmation that details match details PSP hold on the payee
 - Potential solutions include:
 - Validating payee based on previous transaction history held by schemes (links to work in the Financial Crime Working Group)
 - An industry-wide proxy service (phone numbers and emails) (link to Financial Crime Working Group proposition on a central Know Your Customer database), leveraging KYC at each end of the transaction
 - Challenge/response using an API (as per the Paym model, Gov ID, etc.)

- Payers able to address payment or RTPs to pre-known contacts utilising details such as email and mobile number (service could expand to other details in future)
- Payers and Payees will be provided enhanced information in the event of a misdirected payment to enable parties to investigate and ultimately rectify a misdirected payment.
- Careful consideration will need to be given to Data Protection, as well as putting the consumer or entity in charge of their data and permissions in order to avoid increasing the opportunity for phishing or other attacks. This consideration will need to be balanced against the need to provide a clear and simple customer experience.

4. To support multiple enhanced data solutions for consumers and corporates (ED):

- PSP must be able to link a payment to a data package, ideally through use of a unique reference
- Multiple opportunities then exist that could include: tax data / ref, personal data / ref, remittance data / ref, warranties, PDFs of invoices, Word documents, pictures, advertising materials etc.
- Free form data (pictures, data files, remittance information etc.) to be linked to payments so consumers can review through multiple channels of their choice in line with the associated payment
- Enable Structured data for accountancy services, standard remittance formats, e-invoicing
- Customer experience at its most basic would be to receive a secure notification that a data package has been sent to the customer. This would either be independent of a payment (so an initial RtP for example) or linked to an actual payment, with a link to retrieve the data. PSPs would then be able to offer a variety of enhanced experiences for their users, that could include integration with 3rd parties to further use that data
- Enhanced Data would include transit of data to support the user cases outlined in the April Financial Crime, Data & Security Working Group report

FACTORS FOR CONSIDERATION

- The lever of co-ordination verses competition
 - We believe industry must co-ordinate across the framework and establish a minimum core customer proposition on Request to Pay, Assurance Data, and Enhanced Data, leaving the industry to compete on Value Added services and enhancing the user experience
 - However we have an overarching need to ensure that combination of collaborative and competitive services result in a simple and compelling end user experience. If our recommendations are adopted, an appropriate industry body should be appointed to design

these industry-wide products and features along with designing an implementation plan for building and launching these new collaborative industry capabilities

- The degree to which all banking providers must offer these new industry capabilities will require some thought, however our view is that, in order to provide the minimum customer experience and build trust, all PSPs should be required to offer these capabilities. In terms of implementation, a decision will be required on whether the capabilities should be implemented concurrently by all PSPs or rolled out over an agreed timescale
- We believe to be successful a high level of coverage is required, enabling a network effect that drives frictionless adoption, use and user confidence.
- There is a trade-off between simplified access to markets and ensuring the end user need detriments are fully met by the industry. However our current belief is that the minimum requirements must be met by all PSPs .
- The extent to which the underlying payments infrastructure must change to fully realise these benefits:
 - Limitations exist in the current schemes regarding their ability to provide a reference to link a payment to an associated data packet. Faster Payments has a field but it is used in mobile payments and not available from the initiator, and other schemes do not have that capability.
 - For instance a request to pay could be agreed by a payer; however the resultant payment would not be able to hold a reference detailing that it originated from the RtP to support reconciliation.
 - Currently, we are taking an agnostic approach to any developments of the existing scheme rails offering 3 stages of development for Assurance Data:
 - Fuzzy matching - Payer PSP would be able to respond to the Payee PSP detailing that the RTP was fulfilled and providing detail of that payment to enable a mapping (time, amount, bank account, scheme, etc). This mapping would not be completely error free, as such the RTP (and other products) would need to be designed with this in mind
 - Add reference to existing Schemes – Changing the existing schemes just to enable an end to end reference we consider to be very costly. However it may be necessary for the industry to do this to meet the requirements for PSD2.
 - Simplified Payment Platform (as articulated in the Data and Standards report) would enable this reference data to flow with the payment enabling full reconciliation, however the timescale for this is probably 5-10 years out.
- The extent to which these solutions overlap with other regulatory initiatives:

- PSD2 with its payment initiation and aggregation models will bring about industry wide functionalities and capabilities that could enable many parts of the solution. In particular article 95 would seem to require a unique identifier that travels with a payment.
- Open banking APIs would also offer a potential framework to enable Assurance Data and structure for the overarching data framework.
- As such we strongly suggest these initiatives are considered together to ensure efficiency in the resulting payments system and work is conducted in step.
- There may be implications from 4th Anti Money Laundering Directive resulting in enhanced sanctions screening for enhanced data that would need to be considered.
- Consideration will need to be given to data Protection, including stronger controls arising from EU General Data Protection Regulation
- Consideration of other solutions:
 - Other options were discussed in the EUNWG. However these were discounted because they would not meet the requirement for industry wide, interoperable and ubiquitous capabilities.
 - Leave solving the end user needs detriments in the competitive space. However it was the opinion of the EUNWG that, left in the competitive space, these detriments would not be fully met across the industry.
 - Examples of products such as Pingit and Paypal that are not interoperable across banks (but are open market) create closed loops of (very satisfied) users but had not achieved reach and ubiquity across the industry. This is due, we believe, to users not wanting to set up new products to use these features, creating a dampened network effect stopping these solutions from gaining ubiquity.
 - It was felt that to be successful these features should be accessible to users without the barrier of setting up a new product or relationship.
 - Examples such as bPay in Australia or E-Lasku in Finland were seen as bank-wide initiatives that had been successful. Focus should be given to Belgium's Zoomit as the product has not taken off.
 - Develop these solutions into the existing scheme rails:
 - The EUNWG considered this but felt the cost and complexity of changing existing payment schemes and the channels by which those systems are accessed on a piecemeal basis would be prohibitive and not aligned to current architectural best practise or the likely long term direction of the payments industry. However it is recognised that more detailed solution design needs to be undertaken and therefore, changes to the existing systems may still be required.

COST BENEFIT ANALYSIS

£ Cost

- Based on a high level analysis the cost of implementing this solution could reach **£1.5bn across the industry**. See Cost analysis section for further information on assumptions used. The “rule of thumb” here is that approximately 10% of those costs will be central and collaborative while the rest will be incurred by individual PSPs to enable their individual payment systems and channels to take advantage of enhanced central capability.
- However we also consider that similar functionality and work will be required for PSD2, Open Banking and for recommendations coming out of other working groups (fin crime and access to markets)
- PSD 2 in particular puts payment security at the heart of the changes it proposes. Article 95 states *“Payment services offered via internet or via other at-distance channels, the functioning of which does not depend on where the device used to initiate the payment transaction or the payment instrument used are physically located, should therefore include the authentication of transactions through dynamic codes, in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising”*. We interpret that to mean that to be secure, each electronic payment must carry with it a unique identifier that travels with the payment through to the receiving PSP and TPPP. We further assume that HMT would not compromise the security of payments in the UK by not enacting this article into UK law in line with this interpretation. On that basis we consider that the costs associated with our solution as set out in more detail below can be seen as additional to those required to meet the regulatory requirements of PSD 2 (and the CMA Open Banking Data requirements).
- As such we would expect significant synergies to be achieved if considered together which would significantly reduce the cost attributable solely to the requirements of this EUNWG. We consider this attribution to PSD2 and other extrinsic regulatory demands to be **in the region of £900m across the industry leaving an attributable additional cost to these solutions of around £600m**.

£ Benefit

- There are a number of user experience benefits that these solutions answer however there are also economic advantages to be gained.
- Reviewing “Benefits of World Class Payments for the UK” a report commissioned from Cambridge Economics by the Payment Council and delivered in 2015, provides us with a high level benchmark we can use in the UK. This report follows the same “green book” principles that are used by Treasury in the initial assessment of policy initiatives, such as CASS, FCM, and indeed the setting up the PSR.
- This report suggests a benefit (to the UK overall – not specifically to PSPs) in the region of **£1.6bn to £3.2bn per annum over a 10 and 20 year horizon** across improvements in information, efficiency, security and inclusion.
- The case for investment thus to a great extent hangs on the timing of benefit realisation compared to the investment profile. However, as stated above our solutions can and should be

delivered by creating additional capability in changes required by PSD 2 “while the bonnet is up” as it were. The timetable for investment is therefore driven as much by the regulatory timetable as that of the normal investment cycle. Furthermore, since PSD 2 is designed not only to increase security but to increase customer benefit by opening up the TPP market, it may thus be the case that those who take advantage of the enhanced central capability soonest will have a competitive advantage and there will be a market drive for early adoption and a bringing forward of the benefits. The validity of these assumptions and the economics of the case need further (and expert) analysis.

Based on these high level estimates it would seem that the economic business case of these solutions would depend largely on the level of cost synergy achieved with other mandated changes. Although we have not yet conducted an analysis to benchmark this we would expect it to be a very significant cost.

Cost - High Level Assumptions

- Past major projects (Chip & PIN, Faster Payments, CASS and Paym) have all broadly ended up with a central collaborative cost of approximately 10% of the overall implementation cost, the other 90% being shared across the industry.
- The costs of banks to implement is not formally tracked however under CASS Payments UK performed a review that confirmed that 90% of cost was by individual industry participants (Estimate for CASS £750m with central cost being just under £70m) so we have assumed only 10% of cost is central.
- Estimates are based on items below having more or less of an impact than CASS as the benchmark.
- As stated above, we have attributed to these solutions the costs additional to those that would be incurred to ensure PSD 2 compliance and the meeting of the CMA’s open banking data requirement.

Cost - Data framework / APIs

- Need to spend central effort on gaining agreement, building the framework, agreeing critical security measures and getting buy-in and sign off, easier than CASS, but also requires build of an industry permissioning database/system - £15m.
- Each of the banks to build APIs into their product and information (e.g. branches) systems (across the whole industry) less intrusive than CASS - £25m.
- Each of the banks to build APIs into their core systems to access individual account data (across the whole industry) similarly intrusive as CASS but the bulk of this capability will be required by CMA open banking – of the £200m overall estimate we attribute £50m specifically to our requirements.
- NO IMPACT on corporates, existing users and no decommissioning of any existing systems.

- So overall £90m

Cost - Assurance data (both on validating a 3rd party, a proxy service and data on payment status)

- The front end of assurance – so confirmation of payee we are assuming a solution based on an expansion of the Paym database in the centre (£3m) and all banks to check and clean their data and upload all their customers (though some might opt out) £25m.
- The back end assurance (what is called ‘Visibility of the Payments Journey’ in the World Class Payments Project) is much more intrusive. This asks each bank to build new systems that customers (or TPPs) can access information from so allowing them to ‘look into’ bank systems to see the status of payments. Given that there may need to be messages flowing between banks and this may require some central switch (although it may be APIs) there is a lot of design work across the industry as well as individual build. Not quite as intrusive as CASS, but pretty intrusive, estimate £200m but most of that will be attributable to PSD 2 so we attribute £20m to our specific additional requirements.
- The effort to do this for the smaller institutions e.g. building societies with very old systems may be prohibitive and we would expect HMT to take that into account when drafting the necessary legislation. However, in line with our ubiquitous provision principle, we would expect all PSPs to become compliant over time.
- Overall an attributable cost of £45m – we have not costed the risk to older and small institutions they must consider their business model in a post-PSD 2/OBD world.

Cost- Confirmation of Payee

The “dynamic code” dictated by PSD 2 provides post-payment assurance, functionality for Real-time confirmation of payee would require additional investment but could leverage the work elsewhere – on enhanced data, RTP and by reusing APIs. Cost £100m

Cost - Enhanced data

- The central effort on gaining agreement, designing the standards and getting buy-in and sign off (including some work with ISO the standards body) around £5m.
- We assume that we would only need to change Bacs and FPS to carry a bigger reference field – based on the changes to FPS for CASS and assuming that because of the old architecture Bacs would be more complex estimate £25m.
- Assume the new Image Clearing System requires reengineering add £5m.
- Assume that no change to CHAPS since can already carry more data.
- For the whole industry to modify their channels to allow customers to input longer/bigger/different references is perhaps the biggest overall change required but, again, this is a fundamental requirement of compliance with the PSD 2 legislation as anticipated. Across the industry we expect the overall cost of Article 95 implementation to be some £500m

of which we attribute £50m to the additional data handling capability not provided by PSD 2 mapping and vocabulary requirements.

- There will also be substantial impact to users who we assume will migrate over time but with the support of their new PSP and TPPP and existing ERP suppliers; we assume additional attributable costs of £50m.
- **So overall £135m**

Cost - Request to pay

- If the solution are taken in sequence then two precursor components Assurance and Enhanced Data will be in place in PSD 2 compliant format. There will thus be only a core RtP service required.
- There will be a need to spend central effort on gaining agreement, building the overall processes to meet the different use cases, extensive consultation (banks, corporates and customer groups) and putting together a service definition. Note this is for the core, so I am assuming £10m
- We assume the need for some sort of central database build because there will be a lot of volume from corporates. Individual requests might work through API model £10m.
- All of the banks to build the messaging systems to receive, present and allow customers to respond to RtP messages. A lot of work especially in the channels. Say £100m across industry
- Requesters (e.g. utilities) to build systems to send and receive RtP to customers via a bank another £100m
- **So overall £220m**

BENEFITS: FURTHER DETAIL

API Data framework

The CMA's proposals for open banking data API development are predicated on their capacity to increase customer engagement with benefit from the payments systems. As such we do not consider it necessary to go into the details of a separate economic case for these. We would just mention that we support the proposal for a separate and dedicated body to see these into standardised development and we see no reason why that body could not become the principal delivery mechanism for the proposals in this document.

Assurance

We have not had time to consider in detail the proposals in the CMA open banking data report, but there is an argument that any measures that opened up competitive payment service provisions to ensure safe and secure transfers of funds on only one leg of the transaction would leave the benefits behind the report at risk of being unfulfilled. Again we consider that those moving quickly to provide assurance at both ends would gain a competitive advantage and that market forces would produce

the means by which central changes would be exploited fully and quickly. We remain committed however to a solution that operated regardless of the capabilities of the individual PSP, hence the focus on the central collaborative payment system.

We thus consider that the benefits outlined in the Cambridge report could well be realised more broadly and more quickly bringing the cost and benefits horizons closer together and making the business case more compelling.

Enhanced Data

Benefits here depend on PSPs TPPPs and other intermediaries in the payments and data processing worlds being able to develop solutions that would lead to immediate and effective usage. In the corporate area we think that may lead to collaboration across the sectors to provide joined-up end-to-end solutions in the ERP space which again would lead to the earlier realisation of calculated benefits for corporates and government. On the retail side the bringing forward of benefits could be effected by some sensible dirigisme on the part of government. This will be taken forward through appropriate channels.

SEQUENCING

We have identified the following order of implementation. We consider a strategic approach from the start is the best mechanism to realise real end user benefits, but elements on an incremental basis. We expect that the KPMG report will lay out a detailed roadmap of activity including design, testing, build launch and governance activities

A logical sequence for development would be as follows. However we would expect a partially agile rather than purely waterfall approach to be optimum

1. Overall Data framework and communication standards to be agreed, followed by (in order)
2. Confirmation of payee
3. Enhanced data
4. Request to pay