payments strategy forum

December 2017

Collaborative Requirements and Rules for the End-User Needs Solutions

End-User Requirements and Rules Blueprint

Project/Programme Manager:	Duncan M. Ng'enda
Sponsor:	Payments Strategy Forum
Date of Final Approval:	30 11 2017
Approved by:	Sian Williams

Version / Document History

Version No	Date	Author	Comments
1.0	20 07 2017	Duncan M. Ng'enda Ignacio Badiola Sean Doherty Tanuja Kanade Emilie Akiki	Version 1
2.0	24 11 2017	Duncan Ng'enda Emilie Akiki Tigeest Geremew	Version 2

Contents

Executive Summary

In the November 2016 strategy, 'Putting the needs of users first', the Payment Strategy Forum (PSF) identified three End-User Needs (EUN) solutions. These solutions focus on solving detriments identified as affecting some end-users of payments systems. These solutions are: Request to Pay, Assurance Data and Enhanced Data.

Request to Pay addresses the lack of control, flexibility and transparency in payments. It does this through the introduction of a messaging system as part of the payment process, allowing improved communication between payee and payer on the specifics of the payment, and enabling the payer to control how much, how and when they want to make the payment.

Assurance Data aims to provide payers and payees with adequate information throughout the payment lifecycle to assure them that they: have sufficient funds to make the payment; are making the payment to the right payee; and have visibility of the position of the payment in its journey to the payee. The three components, real-time balance, confirmation of payee and payments status & tracking, make up the components of the Assurance Data solution.

Enhanced Data proposes an increase in the amount of data that can be added to a payment and a standard structure that is uniform across the payment industry. This should enhance payments reconciliation, especially for businesses. In addition, the ability to carry more data will stimulate new opportunities in areas such as data analytics and data intelligence that are currently inhibited by the limited nature of current systems.

In its second phase, the Forum set out to develop requirements and rules for the three EUN solutions. These would serve as a collaborative standard for the industry whilst providing a base on which the competitive market could then build compelling propositions for end-users. This activity fell under the scope of the Requirements and Rules workstream of the NPA Design Hub (EUN Working Group).

We adopted a user-centric approach to the definition of requirements and rules, making sure our outputs always addressed the identified end-user needs. We validated and involved various end-users through work with our core advisory group made up of end-user experts, intensive workshops with end-users and one-on-one interviews. The approach was based on a set of nine principles that ensure the resulting designs: put the payer in control; are transparent, allow for competition and innovation; provide the needed levels of interoperability and standards required for ubiquity; consider existing and near future regulation such as GDPR[1]; and, most importantly, allow creation of accessible, scalable, secure and resilient EUN solutions.

For each of the solutions, we identified the core use cases relevant to address the detriments identified. For each of the use cases, we defined associated requirements and rules. In the spirit of the Forum's approach to identifying where collaboration was required in order for the competitive market to work well for all users, our work was deliberately restricted to the definition of the core set of use cases only, with the expectation that the competitive market will define and develop the bulk of the solutions. As such, the core proposition defined should be viewed as a thin standard on which the competitive market can build rich and compelling propositions to the benefit of end-users.

To complement the use cases, requirements and rules mentioned above, we also created end-to-end journeys that neatly illustrate the component stages of each of the solutions.

We identified that the success of these solutions is dependent on other enablers who, in concert with the requirements and rules, provide a suitable environment fostering mass adoption, ubiquity, innovative extensibility and competition. Some key enablers identified and highlighted in the consultation document are: data privacy and protection regulations which are especially relevant in the case of Confirmation of Payee and Enhanced Data; the need to ensure all cash accounts can be confirmed via Confirmation of Payee (otherwise the utility of this solution to guard against fraudulent or accidental misdirects will be diminished); and a governance mechanism that ensures the competitive players offering these solutions meet the base requirements stated herein. The enablers highlighted form part of a complete set detailed in this document with accompanying recommendations.

The cumulative output of the work carried out by the Forum and detailed in this document will be handed over to the New Payment System Operator (NPSO) for further implementation and detailing.

[1] General Data Protection Regulation.

1 Introduction

In the Strategy we prioritised the collaborative development of requirements and rules for 3 end-user solutions. These are:

- 'Request to Pay' which addresses detriments arising from a lack of sufficient control, flexibility and transparency in the current payment mechanisms to meet the evolving needs of some end-users.
- 'Assurance Data' which addresses: the lack of adequate assurance to the payer that they have sufficient funds to make a payment; that they are making the payment to the intended payee's account; and status of the payment once they make the payment.
- 'Enhanced Data' which addresses the limited capacity in current payment systems to carry more structured data alongside the payment.

Development of the requirements and rules was achieved collaboratively through numerous workshops and interviews with various representatives of the main end-user groups: government, charities, consumer groups, corporates, retailers, housing associations, Payment Service Providers (PSPs), and Payment System Operators (PSOs). In addition, we incorporated further research by various organisations already working on these solutions both within and outside the UK.

Figure 1: EUN Principles

We have identified and prioritised the essential use cases that any implementation of these solutions must meet to address the detriments identified in the Strategy. Prioritisation of this set was guided by 9 design principles against which each requirement was tested. These principles are listed in Figure 1. For each use case, we have proceeded to design the associated requirements and rules. Any provider of the three EUN solutions would have to meet these requirements and adhere to these rules.

This set of use cases, requirements and rules developed are a minimum set, sufficient to show how the detriments identified are addressed, and allow the creation of interoperable, accessible, scalable, secure, and resilient EUN solutions. This core set of use cases, requirements and rules will be owned and administered by the New Payment System Operator (NPSO). Every service provider of these three solutions will have to meet these minimum requirements and rules. We expect that service providers will build on this core set and create additional functionality that results in richer competitive products to the benefit of end-users.

2 Requirements Approach and Design Principles

2.1 Design Principles

We defined 9 design principles that would guide the definition of requirements and rules. These rules are:

1. **Payer is always in control**
   - For each of the EUN solutions (Request to Pay, Assurance Data, and Enhanced Data) the payer should be provided with appropriate control throughout each step of the journey and the associated outcome.
   - In the case of Request to Pay, the payer must have control over whether to pay or not, how much and when. For Confirmation of Payer in the Assurance Data solution, prior to making the payment, the payer must have ultimate control on whether or not to make the payment, how much and when based on the information provided. Similarly, the payer has ultimate control over what data they choose to provide as part of the Enhanced Data solution.
   - Granting the payer control does not in any way replace the role contracts play between a payer and a payee.
2. **Transparent**
   - The EUN solutions should provide end-users with clear, relevant and appropriate information, ensuring the end-users are clear on current actions, their consequence and outcomes at all points in the process. In turn, a payee should be aware of who has paid them and the related details associated.
3. **Available, secure and stable**
   - Each of the EUN solutions should be designed such that it is highly available and secure. EUN solutions should strive to meet best in class benchmarks especially around data security and privacy, stability, and predictability in their nature with an assured certainty of outcome throughout the process, including when they fail. EUN solutions should match at least the security and resilience of existing systems.
4. **Common rules and standards**
   - The EUN solutions should be designed to a common set of standards and rules. Common standards will facilitate the creation of competitive solutions that are interoperable and capable of ubiquity.
   - The design should adopt or build upon existing standards and regulations such as ISO 20022 and the Application Programming Interface (API) standards adopted by the industry for PSD2 and Open Banking orders.
5. **Open to competition and innovation**
   - The set of common requirements and rules for each of the three EUN solutions should be defined to an appropriate level of detail necessary to allow development of interoperable and ubiquitous solution(s). The level of the specification will be such as to leave enough headway for a competitive market, including payees, to create innovative but interoperable products.
6. **Regulatory compliant**
   - For each of the EUN solutions, the requirements and rules defined must be compliant with existing and anticipated regulation e.g. PSD2, GDPR, OB, AML4.

7. **Payment agnostic**

- Each of the solutions will be designed to be agnostic of the type of payment used. Where possible they will be designed to allow any instrument to be utilised and not give an unfair advantage to a particular payment instrument.

8. **Accessible and inclusive**

- Each of the solutions will be designed such that they are accessible and inclusive.

9. **Scalable, future-proof**

- The design should be robust enough to leave room for future extensibility in response to emergent needs.

In addition to the general principles, we defined the following four design principles which are solution specific.

10. **Real Time (Confirmation of Payee and Request to Pay)**

- Responses to Confirmation of Payee or Request to Pay should be presented to the payer in real time.

11. **Definitive (Confirmation of Payee)**

- Responses to a request to confirm payer/payee should be unambiguous and clear, bar unavoidable limitations such as regulatory restrictions.

12. **Available 24/7 365 days (Confirmation of Payee)**

- The utility of the Confirmation of a payer/payee solution is dependent on it always being available at the point of need.

13. **Integrity of data maintained throughout (Request to Pay and Enhanced Data)**

- At all times, the integrity of the data carried must be assured.

2.2 Requirements Approach

To define and gather requirements, we conducted meetings and working sessions[2] with a variety of end-users and stakeholders. These engagements helped refine the use cases, requirements and rules.

The approach we utilised is summarised in Figure 2.

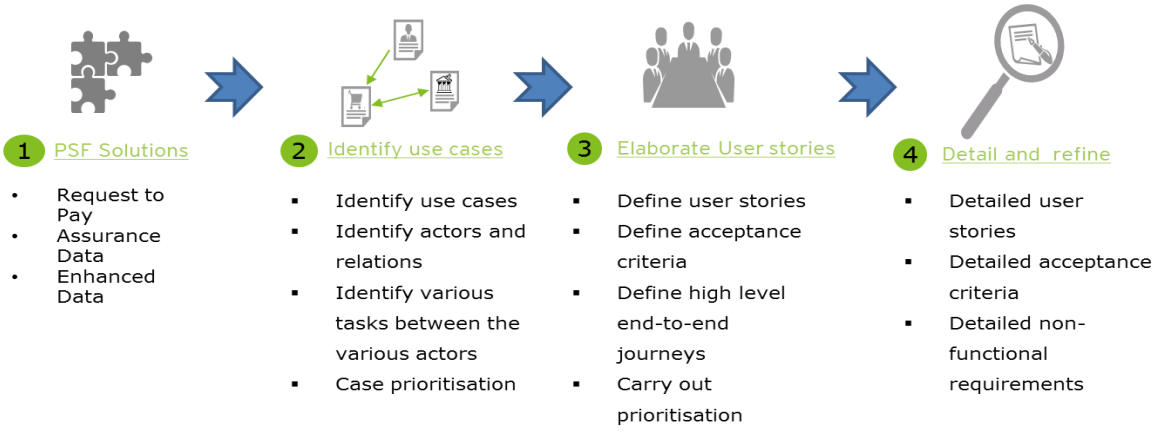

Figure 2: Requirements Approach

The requirements approach:

- Is based on the Agile Methodology (Requirements and rules presented as use cases, user stories and rules)
- Places the end-user at its heart
- Encourages a collaborative approach to requirements definition from the various stakeholders

The outputs of this work are:

1. **Use case diagrams:** Use cases are high-level representations of the functions, actors and their relations for each of the solutions. They form the basis for the requirements and rules. They are illustrated as Unified Modelling Language (UML) Diagrams.[3] The diagrams present a complete set of use cases identified for each of the solutions based on workshops held with various end-users.

   The workstream terms of reference dictate the development of requirements and rules only for essential use cases necessary to address the detriments identified by the Forum in the Strategy. Use cases have been classified into a core set and a competitive set. We proceeded to define user stories and rules for this core set. Though no more development has been done on the competitive set, the expectation is that the competitive market will take them up and create compelling propositions over and above the core set.

2. **User Stories:** The user stories are a detailed articulation of the functional requirements of each actor per use case. A standard notation has been used to structure each user story – 'As an Actor X, I want to do X, so that I can achieve X.'

3. **Rules:** The rules qualify each user story and provide constraints where needed. Extending the example above, a user fulfilling a user story X, can only do it in a certain way dictated by a rule.

For each solution, we have provided the use cases, user stories and rules. In addition, we defined the applicable scope for each solution.

[2] The complete list of sessions and meetings held with end-users and stakeholders is available in Appendix 10.

[3] The Unified Modelling Language (UML) is a general-purpose, developmental, modelling language in the field of software engineering that is intended to provide a standard way to visualize the design of a system.

3 Request to Pay

For the majority of people, the technical aspects of payments are invisible. They run in the background supporting various activities in our lives that require the movement of money. Examples include receiving an income, paying bills, making a mortgage or rent payment, or buying groceries. The way we make payments and interact with payment systems has changed dramatically in the last few years. We identified these changes in the Strategy and acknowledge that a growing number of end-users' needs are not completely met by the current payment systems. A predominant theme was the need for end-users to have:

- More control over their payments;
- More flexibility over how much, when, and how they pay;
- Increased transparency in their interactions with payments.

There is broad consensus that a Request to Pay service will help address the detriments mentioned above and bridge the growing needs gap. We proceeded with the design of a Request to Pay service that specifically addresses these detriments.

3.1 Detriments Addressed by Request to Pay

Request to Pay aims to solve the following detriments:

ID	Detriment Group	Detriment
1	Customer Control	Payers and payees need more flexible mechanisms for collecting and making recurrent and ad hoc payments.
2	Customer Control	Payers and payees need more mechanisms for payments that give greater control to the payer and more certain outcomes for the payee.
9	Customer Financial Capability	Some financial products are overly complex and lack transparency, leading to avoidance by unconfident users.
10	Customer Financial Capability	Access to cash remains important for many users (due to either low or unpredictable incomes or mistrust of electronic payments due to lack of transparency) and will continue to be so while non-cash products do not meet their needs for control and transparency.
11	Customer Financial Capability	Competition is not currently meeting user needs for simplicity.
12	Customer Financial Capability	Competition is not currently meeting user needs for transparency.
13	Customer Financial Capability	Competition is not currently meeting user needs for control.
15	Corporate Customers	There is a lack of realistic alternative payment options other than cards available to merchants/retailers.
16	Corporate Customers	Online payments – there is a lack of access for business users for alternative rails (i.e. need more availability of credit transfer payment online).
22	Corporate Customers	Reconciliation costs and treasury management for businesses; also government reporting costs.

Table 1: Request to Pay Detriments

3.2 Scope

3.2.1 In Scope

#	Item	Description
1	Only British Pounds (£) payments	The requirements will cover payments denominated at their origin in Sterling pounds. However, this should not restrict innovation where other currencies might be needed.
2	UK only	Restricted to payments occurring within the UK (FCA geographical area of jurisdiction).
3	Users: Individuals, Consumers, SMEs/Charities, Corporate, Government, PSPs, Clubs and Societies	This list of users is not immutable. Where a user not listed is capable of participating, it automatically becomes part of the scope.
4	Payment types: Credit, Debit & cash (physical note and coins) where conclusion/reconciliation of a payment is electronically done	All credit, debit and cash (physical note and coins) payments that end in an electronic transaction. As soon as any of these enters the electronic environment it automatically becomes part of the scope.
5	All channels: online, mobile, telephone, intermediaries, branch, paper, etc...	All channels are a possible mean for Request to Pay.

Table 2: Request to Pay In-Scope

3.2.2 Out of Scope

#	Item	Description
1	Securities	Any security payment or financial instrument of this type.
2	Cash (physical notes and coins) End to end process	Cash payments that do not enter the electronic environment at any point.
3	Market infrastructure payments	For example, the settlement of transactions.
4	Payments in kind	Any payment made in a non-monetary form.
5	Direct Carrier Billing	Payments made by charges made to a customer's account (i.e. mobile account).
6	Pre-payment (tokens)	Prepaid tokens such as a prepaid electricity meter.
7	Store / Loyalty cards	Closed loop loyalty cards - not white labelled store cards.
8	Digital currency	Currency that does not equate to British Sterling Pounds (i.e. bitcoins).
9	Anything in the competitive realm	All functionalities open for competitiveness.

Table 3: Request to Pay Out of Scope

3.3 High-Level Use Cases

The high-level functional overview of Request to Pay use cases from the payer's and payee's view are depicted in Use Case Diagrams Figures 3 and 4. They are classified into use cases identified as minimum 'core proposition' for customers to ensure consistent experience and 'competitive' use cases that are open for innovation to offer more value to the users and promote healthy competition in the market. The Forum has not defined requirements and rules for the competitive cases.

Use cases are represented as UML diagrams accompanied by Tables 4 and 5 providing a short description of each use case.

3.3.1 Payee Use Cases Overview

The use case diagram presents the payee's use cases.

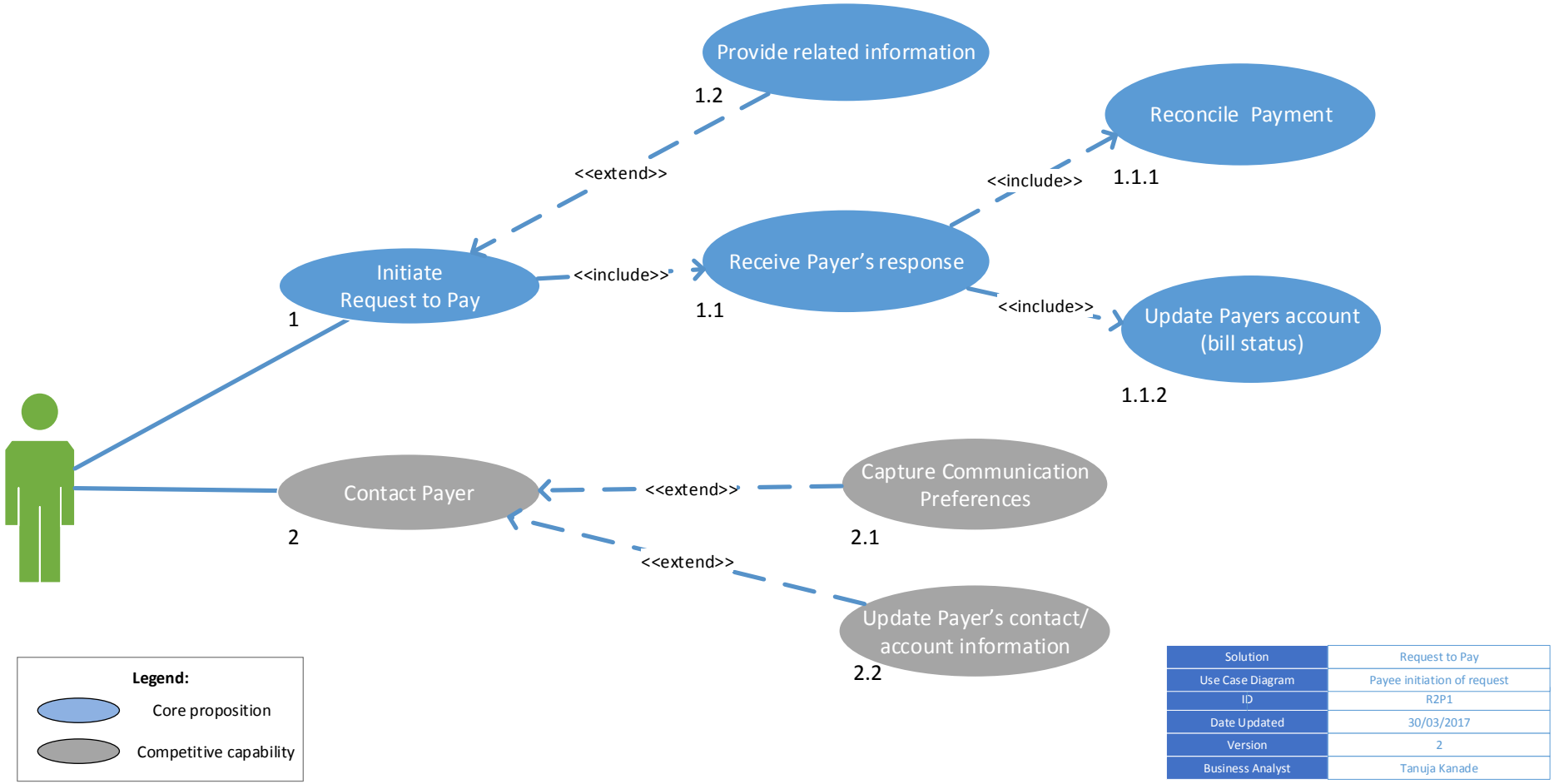

Figure 3: Request to Pay Payee Use Case Diagram

3.3.2 Payer Use Cases Overview

The use case diagram presents the payer's use cases.

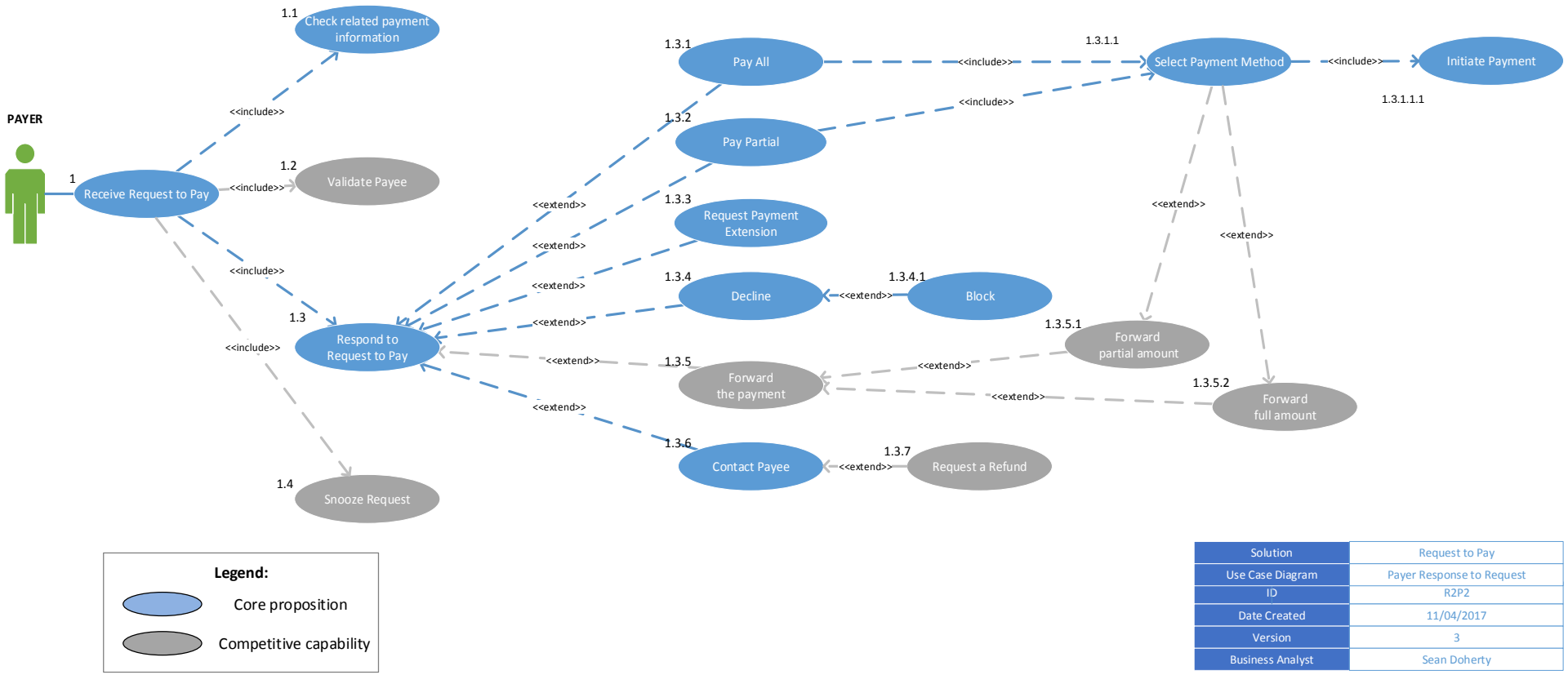

Figure 4: Request to Pay Payer Use Case Diagram

ID	Use Case	Description
1	Initiate Request to Pay	The payee creates a Request to Pay message with appropriate details such as payee's name, payee's bank account details for payment or other payment options, payer's name, amount, due date and sends it to the payer using an agreed communication channel.
1.1	Receive payer's response	A payee should be able to receive the payer's response once they respond to a request the payee has sent to them.
1.2	Provide related information	Request to Pay service should enable a payee to attach/provide additional payment data such as an invoice or receipt to inform the payer.
1.1.1	Reconcile payment	Payees can reconcile payments to the original associated Request to Pay.
1.1.2	Update payer's account (bill status)	Once a payer has responded to a request the payee should be able to update the payer's account accordingly. E.g. Capture a payment made, update a payment period and capture a decline.

Table 4: Request to Pay Payee Use Cases

ID	Use Case	Description
1	Receive Request to Pay	The payer receives a Request to Pay message from the payee through an agreed communication channel.
1.1	Check related payment information	In cases where the payee has provided additional information, the payer should be able to determine the existence of additional information and access this information.
1.3	Respond to Request to Pay	The payer responds to a Request to Pay.
1.3.1	Pay All	Accept a request for payment and proceed to initiate a payment equivalent to the total amount (or more when allowed) asked for in a request.
1.3.2	Pay Partial	Accept a request for payment and proceed to initiate a payment equivalent to a portion of the amount asked for in a request; this can be done multiple times until full amount is matched.
1.3.3	Request Payment Extension	Request a payee for an extension to the payment window to give a payer more time to pay a request (within terms of contract).
1.3.4	Decline	Decline a request for payment and inform the payee they (payer) will not be paying a request.
1.3.6	Contact Payee	Provides a way for a payer to contact the payee that has sent a request.
1.3.4.1	Block	Stop a payee from being able to send you requests in the future. Payees will be notified in this instance.
1.3.1.1	Select Payment method	The payer should be able to select the payment method they choose from those available when responding to a payment request.
1.3.1.1.1	Initiate Payment	If a payer chooses to pay a request, a payment is initiated automatically.

Table 5: Assurance Data Payer Use Cases

3.4 High-Level User Stories and Rules

Users of Request to Pay are acting as either a payer or a payee. A payer or payee could be an individual, corporate, government, charity or SME. To achieve the key Request to Pay outcomes, namely increased control, flexibility and transparency, a Request to Pay solution will meet, as a minimum, the following requirements and rules set out below. The requirements and rules are classified into payee and payer requirements.

To support the service, there will be a Request to Pay service provider and a governing body. The service provider will undertake the technical provision of the Request to Pay service. This role will be performed by the payee or another entity with whom the payee would contract to do so on their behalf. We expect several providers to competitively provide the Request to Pay service.

A governing body will provide a thin layer of governance aimed at ensuring that the objectives of the service are met and the end-users are protected. This is achieved through ensuring that the minimum end-user and technical standards are met by stakeholders and the service is not abused or used for fraudulent purposes.

3.4.1 Payee User Stories and Rules

1. Initiate Request to Pay

	As a payee, I want to be able to:
Create a Request to Pay message to be sent to the Payer	1. Create a Request to Pay, so that I can send it to the payer I wish to pay me. 2. Initiate a Request to Pay through the payer's preferred communication channel. 3. Add a recipient to the request so that the request is sent to the intended person. 4. Include a description so that the payer is able to identify what they are being requested to pay for. 5. Include the amount associated so that the payer knows the amount they are being requested to pay. 6. Include the associated payment's due date or payment window end date so that the payer knows when they are supposed to pay. 7. Include the choice of payment methods (and price differentiation if any) so that the payer can see which payment options are available to them. 8. Include associated information needed to use accepted payment methods (e.g. bank account details) so that the payer has enough information to submit a payment. 9. Include a unique reference so that I can track and reconcile the request throughout its lifecycle. 10. Include contact details for payers to use so that a payer can contact me if necessary. 11. Determine the successful or unsuccessful sending status of a request so that I can confirm a request has been sent.
Rules	1. A request must have at least one recipient. 2. The amount requested cannot be less than £0; a payee can set a maximum amount if they so wish[4]. 3. A request's due date or payment window end date cannot be in the past. 4. A request must specify at least one payment method that a payer is able to use should they wish to make a payment. 5. A request must have a reference ID.

[4] Some payees may want to limit the ability to overpay. This is due to their particular business models or contractual arrangements. Example: HMRC, Mortgage Companies.

2. Provide Request Related Information

	As a payee, I want to be able to:
Include additional data in a request	1. Include additional information in a request so that I can provide the payer with additional information related to the request.
Rules	1. Additional information is not necessary to send a request. 2. Additional information provided should only be accessible to the intended recipients.

3. Receive Payer's Response

	As a payee, I want to be able to:
Receive response from Payer for applicable payer responses	1. Be informed of a payer's response that requires an action from me so that I am aware of any changes in status to a request. 2. Be informed of a payer's chosen payment method and resulting total amount of a request due so that I am aware of the amount owed to me if any.
Rules	1. Where multiple payment options are provided, a payer cannot be prevented from making multiple partial payments via different agreed payment methods.

4. Reconcile Payment

	As a payee, I want to be able to:
Payees can reconcile payments made to Request to Pay requests	1. Link payments made by a payer with the associated request so that I can reconcile requests to the payer's account and payments made.

5. Update Payers Account (bill status)

	As a payee, I want to be able to:
Receive a request from Payer to update their billing account with the latest bill status details	1. Link responses to a request with a payer's account information so that I can ensure their account is up to date. 2. Link the outstanding request amount to the payment method chosen so that I can ensure the correct total is used should it differ per payment method.
Rules	1. A request is considered closed when a payment (or set of partial payments) has been initiated that cover the amount being requested.

6. Initiate Debt Recovery

	As a payee, I want to be able to:
Link up with Payee's internal debt recovery procedures as necessary	1. Link the request with related processes such as debt recovery so that I can trigger the correct process when appropriate.

3.4.2 Payer User Stories and Rules

1. Receive Request to Pay

	As a payer, I want to be able to:
Receive a Request to Pay message from a Payee	1. Receive requests from payees so that I can view requests sent to me. 2. Receive requests through my preferred communication channel so that requests are delivered through the most convenient channel for me. 3. I must be able to check the validity of the sender.

1.1 Check Related Request Information

	As a payer, I want to be able to:
Identify and access related information connected with a request	1. Identify when additional information is provided with a request so that I can then proceed to view it if necessary. 2. Access the request's related information so that I can review and see more detailed information on the request.
Rules	1. Where additional data has been provided it must be accessible by the end recipient in at least the medium the request is delivered.

2. Respond to Request to Pay

	As a payer, I want to be able to:
Respond to a Request to Pay message to the Payee	1. Respond to a request so that I can specify which action I wish to take. 2. Respond to a request at any time when that facility is available prior to the due date or before the payment window end date so that I can respond when convenient to me.

2.1 Pay All

	As a payer, I want to be able to:
Pay the total amount of any outstanding request in one single payment	1. Choose to pay the entire amount requested so that I can then attempt to pay the entire amount. 2. Choose when I pay all of the amount requested so that I can pay at a specific point in time that suits me. 3. Choose to pay through any channel accepted by the payee so that I can select the payment channel most suitable for me.
Rules	1. Once payment for the full amount is initiated the request is considered “closed”. 2. Where a payee has provided a maximum amount payable, a payer cannot pay more than this amount.

2.2 Pay Partial amount

	As a payer, I want to be able to:
Pay a portion of the total requested amount, prior to the final due date. Payment can consist of multiple instalments.	1. Choose to pay a partial amount of a request, so that I can pay a partial amount of the total requested. 2. Choose how many payments I make, so that I can pay the full amount in smaller sizes. 3. Make any number of partial payments at any point in time prior to a final due date and within the payment window so that I can pay the total amount in many partial payments. 4. Pay through any channel accepted by the payee so that I can select the payment channel and/or payment type most suitable to me.
Rules	1. Partial payments can be any portion of the total amount. 2. A payer can make as many partial payments as they wish, up to the maximum request amount, before the payment window end date and before the due date. 3. A request is considered “closed” once the last of the partial payments amounting to the total request sum is initiated.

2.3 Request payment extension

	As a payer, I want to be able to:
Request payment extension	1. Ask for an extension to the request due date or payment window end date so that I can push back the request due date within the bounds of my contractual agreement with the payee.
Rules	1. An extension can only be after the original due date or the payment period ends. 2. Payee must specify the time period of the extension and the period by which the payer has to respond to the request.

2.4 Decline

	As a payer, I want to be able to:
Choose to decline the 'Request to Pay' message[5]	1. Decline requests so that I can notify the payee I will not be paying the request.

2.5 Block

	As a payer, I want to be able to:
Choose to block a Payee's 'Request to Pay' message for any reason	1. Block requests, so that I can break the relationship with a payee and not receive future requests. 2. Block unrecognised or unsolicited requests from a payee with whom I have no relationship (spam). 3. Unblock a blocked payee, so that I can re-establish my relationship with a payee.

2.6 Contact requester

	As a payer, I want to be able to:
If the Payer wishes to talk to the Payee, then they can contact the Payee directly	1. Contact a payee so that I can request more information or discuss a request I have received.
Rules	1. Payees must provide at least one contact method.

3. Select Payment Method

	As a payer, I want to be able to:
Prior to initiating a payment, a Payer can select from methods accepted by their Payee	1. Choose a payment method accepted by the payee so that I can attempt to pay the selected amount. 2. Choose from various payment methods accepted by the payee so that I can choose the method most convenient to me.
Rules	1. In such a case that by choosing one payment method over the other, the payer is subject to a monetary benefit e.g. a discount, the payer should be clearly informed of this benefit in advance.

[5] Declining a request does not equate to the termination of a contact

4. Initiate payment

	As a payer, I want to be able to:
The Payer should be able to initiate a payment as a response to a Payee's request	1. Initiate the payment process once I have chosen a response that requires payment so that I can then make the payment. 2. Have the payment, request[6] and payee's information transferred automatically[7] from the request to the payment so that this reduces the need to re-enter the payment's information manually.
Rules	1. The payer must have knowledge of how their data is used, how long it's stored and a mechanism to request for the data to be deleted.[8]

3.5 Proposed End-to-End Journey

The end-to-end journey for a Request to Pay lifecycle will be broadly similar regardless of the types of actors involved. For example, peer-to-peer payments, between individuals, will typically follow the same flow as a business-to-consumer journey.

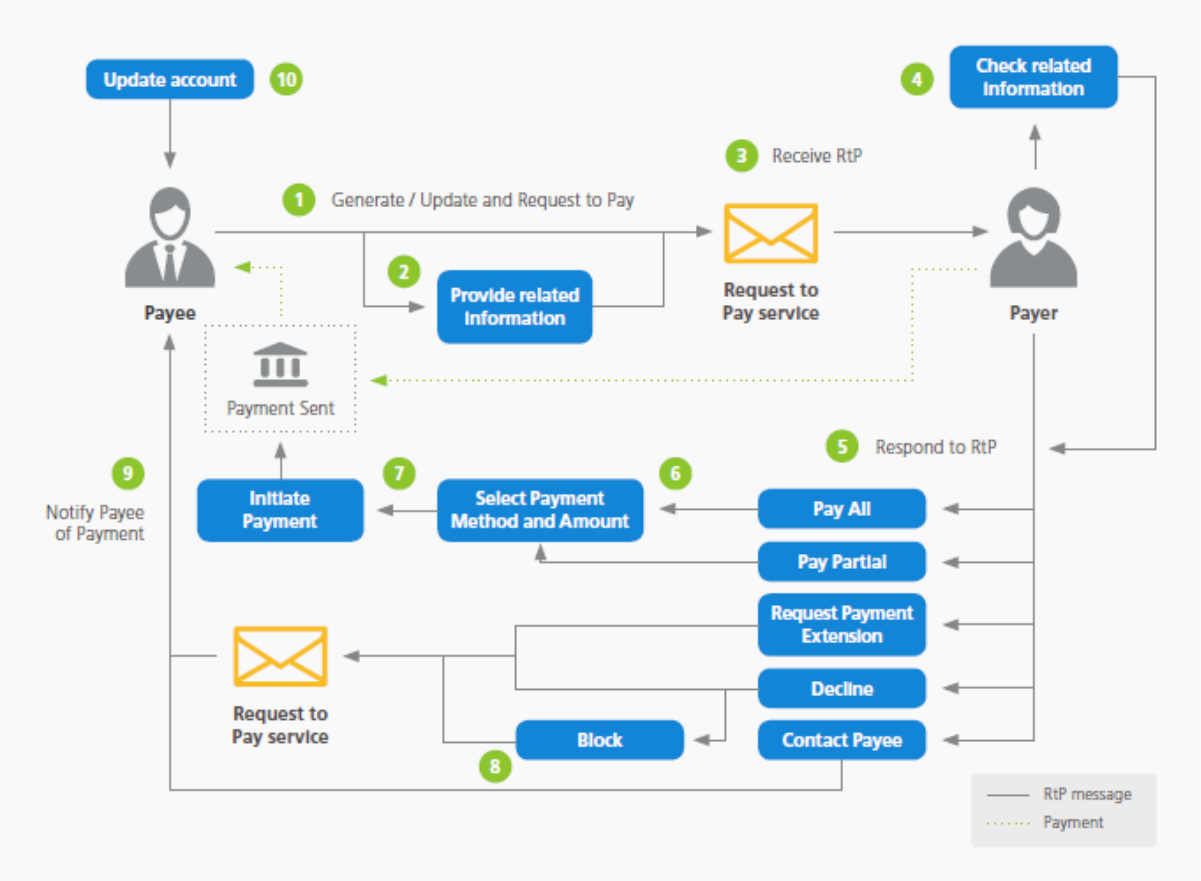

Figure 5: Request to Pay End-to-End Journey

[6] Request information including the reference ID.

[7] Automatic transfer of details could either be passing from app to payment method but also applies to scanning of a Request to Pay code by a third party e.g. Post Office.

[8] This is in line with data protection regulations such as GDPR. These requirements will be extended to all other applicable regulation enforced at present and in the future.

#	Step Name	Description
1	Generate Request to Pay	A payee generates a new request (or updates an existing request), which is then sent to the payer.
2	Provide related information	A payee has the option to provide additional information to the payer. This could take the form of a hyperlink to related information stored elsewhere or an attached document, for example.
3	Receive Request	The payer receives the request through their preferred channel.
4	Check related information	The payer reviews additional information related to the received request – if the payee has provided this.
5	Respond to request	The payer responds to the Request to Pay, at which point they have a number of options for payment; pay all, pay partial, request payment extension, decline or contact payee.
6	Select Payment Method	The payer selects the payment method they want to utilise from the payment options supported by the payee and their PSP. The payer can set the amount that they want to pay for a single instalment.
7	Initiate Payment	The payer initiates a payment.
8	Block	A payer can block a payee from sending requests to them. The payee will be notified, and any future requests will not be received by the payer (unless they choose to unblock the payee).
9	Notify Payee of Response	The payee receives a notification with the payer's response.
10	Update Account	Once the payment period is complete, the payee updates payer's billing account based on the information that has been received and any relevant back-office processes.

Table 6: Request to Pay End-to-End Journey

3.6 Assumptions

To successfully deliver the Request to Pay service as described, several assumptions were made. These are:

ID	Title	Description
001	Onboarding	It is assumed that to use Request to Pay, payers and payees alike will need to go through an onboarding and verification process.
002	Interface building	It is assumed that third parties will primarily be responsible for building Request to Pay consumer-facing solutions.
003	Contractual Obligations	It is assumed that Request to Pay and actions taken on requests by payers or payees in no way changes or absolves payers or payees of existing contractual obligations between one another.

Table 7: Request to Pay Assumptions

3.7 Key Risks and Considerations for Request to Pay

While developing the requirements and rules for Request to Pay, we identified key risks and considerations that must be made. For each of these risks, we have identified mitigations. The risks are summarised in Table 8.

Risk	Mitigation
1. Uncertainty of payment Request to Pay provides payers with the ability to defer or decline a Request to Pay; this creates a risk around the certainty of payments for a payee.[9]	Service contracts between the payer and payee must have rules in place specifying conditions and criteria under which the payer can defer a payment and the consequences of deferring or declining a payment. Request to Pay does not change the contractual relationship between the payee and payer.
2. Service failures There is a risk that failure of the service could result in potential harm, for example: If the request does not reach the intended payer resulting in a non-payment and the payer falling into debt. If the payer's response does not reach the intended payee this could result in a non-payment and payer falling into debt.	Request to Pay service providers must put in place measures to reduce the likelihood of technical failure of any of the Request to Pay components.
3. Service abuse and service fraud There is a risk that spammers, fraudsters or other malicious actors will misuse the service resulting in harm to the end-users.	Providers of the Request to Pay service should be registered/accredited as part of ensuring that the service is trustworthy and reduce the risk of fraudulent use. Also, governance should be in place that requires all Request to Pay services to demonstrate a minimum standard of information security.
4. Persistent debt There is a risk that payers will defer payments indefinitely which will result in payees not getting paid.	Service contracts between the payer and payee must have rules in place specifying conditions and criteria under which the payer can defer a payment and the consequences of deferring it.

Table 8: Request to Pay Potential Risks

Additionally, the following should be considered:

1. **Trust:** Request to Pay will provide a new payment tool. It is critical that the service is trustworthy and secure. We are recommending the following:
    a. **Request to Pay service providers' registration and accreditation:** Providers of the Request to Pay service should be registered/accredited as part of ensuring that the service is trustworthy and reduce the risk of fraudulent use.
    b. **Information Security:** Governance should be in place that requires all Request to Pay services to demonstrate a minimum standard of information security.
2. **Contractual terms and obligations:** In most cases, the payer and the payee will have existing contractual terms specifying obligations, penalties and consequences. In using Request to Pay, end-users will still need to be compliant with underlying contracts and

[9] Certainty of payment refers to the likelihood of a payee being paid by the payer for a request to pay sent. It should not be confused with the certainty of payment as it refers to a payment being settled. See next section for a more detailed consideration of Request to Pay and how it impacts payee certainty of payment.

necessary adjustments will have to be made where necessary. For example: To define payment periods and terms of payment extensions.

3. **Payment mechanism specific protections:** Request to Pay will be largely payment type independent, it is anticipated the standards, dispute resolution and liability arrangements of the underlying payment type will be followed and are not duplicated. Additional analysis should be conducted to understand if any features alter these existing arrangements.

4. **End-user interface design and experience:** Providers of the service will be tasked with determining the best way to present the functionality and capability to the end-user. In doing so, consideration must be made to ensure that these interfaces allow the end-user to interact and utilise the service in the most effective manner. Users of the service should get a minimum quality of experience whoever their service provider is.

5. **End-user awareness and education:** To aid in the adoption of the service, payers will need to be made aware of the existence of the service as well as receive education on how best to safely engage. Request to Pay will result in changes to how payees and payers interact. These changes will attempt to shift the cultural status quo. For example, increased payer flexibility on when they can make a payment will require both the payer and the payee to be comfortable with this.

6. **Branding:** Based on learnings from previous industry initiatives, end-users will expect a recognisable branding for the core set of services consisting Request to Pay. The nature, extent and details of the branding will be defined and owned by the NPSO.

3.8 Payee Certainty of Payment

Certainty of payment is a measure of the likelihood of a payee to be paid by a payer for goods or services rendered within a defined period.[10] The increase in flexibility and control afforded by Request to Pay to a payer must be counterbalanced by the need to ensure certainty of payment for the payee.

A lack of certainty of payment would have negative consequences for both the payer and payee. For payees, these could include cash flow issues, reduced operational capital, bank overdraft charges, and additional costs associated with debt administration and recovery operations. These consequences are particularly severe for SMEs due to their increased vulnerability to income disruption, but could also have a negative impact on adoption by other payees. Similarly, payers who fall into debt as a result of a late payment or non-payment may be liable to monetary penalties, negative credit reports, withdrawal of services and debt recovery processes as well as falling into disrepute with payees.

To ensure that certainty of payment is not compromised we have identified, along the Request to Pay journey, points where a certainty of payment might be compromised. For each of these instances, we have identified the risk and related mitigation against this risk. This is done in Figure 6 and Table 9 in the next section.

It is worth considering that many of these risks occur today in the case of a traditional paper bill. Request to Pay merely casts this in a new light.

[10] Note, technically certainty of payment could also be used in the context of a payment method, to measure the how likely it is that a payment transaction completed through the payment method will be completed and the payee will receive a certain payment amount within a defined period. Request to Pay is a not a payment method, and the former interpretation of certainty of payment should be considered for purposes of reading this section of the document.

3.8.1 End-to-End Journey Analysis

We identified potential positions along the Request to Pay end-to-end journey where certainty of payment may be compromised illustrated in Figure 6 below:

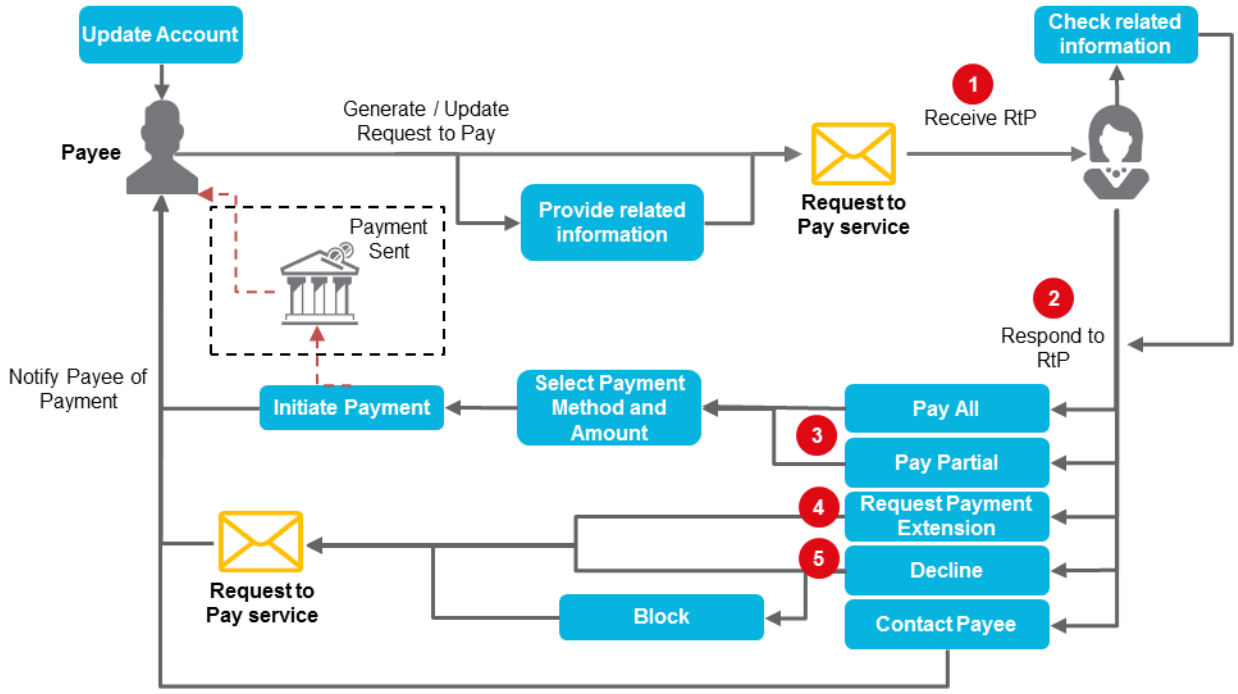

Figure 6: Potential Areas Causing Uncertainty to Payees along the Request to Pay End-to-End Journey

ID	Item	Description
1	Message not delivered to the payer	There is a risk that the Request to Pay is not sent and thus not received by the payer resulting in the payer not making the payment. For example, due to a technical fault in the system.
2	Payer ignores the message	There is a risk that the payer receives the Request to Pay, ignores it and does not make the payment.
3	Lack of funds	There is the risk that the payer chooses to honour the Request to Pay and make a payment but the payment fails due to a lack of sufficient funds.
4	Payer deferring indefinitely	There is a risk that the payer repeatedly asks for an extension to a payment, leading to them deferring the payment indefinitely and not making the payment.
5	Payer declines the request	There is a risk that the payer chooses to decline the Request to Pay and does not make the payment, despite the payment being correct and proper.

Table 9: Instances Where Certainty of Payment May Be Compromised

3.8.2 Tools Available to the Payee to Manage the Risk of Uncertainty of Payment

Payees can leverage several tools to mitigate against the aforementioned risks to the certainty of payment. In addition, in cases where the risk is realised payees can resort to several measures for protection. These tools and measures are illustrated in Figure 7 below:

Figure 7: Tools Available for Payees

Depending on the circumstance each of these tools and measures can be used in isolation or in combination as required.

For each of the risks identified earlier in Table 9, we will discuss and make recommendations on how to apply these tools and measures to mitigate the risk or make amends in cases where the risk materialises.

3.8.3 Risk of Uncertainty Due to the Payer Ignoring/Declining a Request or Non-Payment

To solve uncertainty due to the payer ignoring/declining a request or non-payment due to lack of funds, payees can rely on:

I. The contract between the payee and payer

Payers and payees will typically have a contractual relationship underpinning their commercial relationship. The contract will typically specify terms of payment, payment methods and associated outcomes including consequences of repudiation such as non-payment by the payer. Similar to existing payment methods, the expectation is that contract terms underpinning the commercial relationship between the payer and payee will apply to Request to Pay. Contracts are legally recognised instruments and thus must provide added assurance to both the payer and the payee.

Recommendation	1. Use existing contractual law and precedent as a protection tool Note: Request to Pay must allow for instances where the payer does not receive the request for reasons not in their control e.g. Technical failure of the Request to Pay service.

II. Existing regulations and codes of practice on non-payment

The law [11] currently describes a payment as being late after 30 days, for public authorities and business transactions, after either the payer gets the invoice or goods and services are delivered (if this is later). A payee can legally pursue the necessary steps to recover a late payment.

It is important to point out that a legal contract applies regardless of whether the payee bills or invoices the payer. The implication is that there is an obligation on the payer to pay a payee even if they do not receive a Request to Pay for goods or services rendered.

With this in mind, payees must be assured that Request to Pay does not compromise their right to a payment. In turn, payers must be educated and made aware that the increased flexibility provided by Request to Pay does not diminish their obligation to pay for goods or services received.

Recommendation	1. Use existing regulations to seek redress. 2. Abide by existing codes of practice to avoid mistakes, for example, the code of practice for accurate bills which is currently applied in the energy sector.

III. Technical design

Request to Pay service is designed to minimise the risks of undelivered requests. To reduce cases where a payer does not receive, ignores or declines a request, several design features within Request to Pay can be leveraged. [12]

Recommendation	1. Request to Pay providers must leverage a combination of a notification system and user interface design features to alert payers of pending unpaid requests. In instances where the message is not delivered due to a technical failure, payees must be made aware and allowed to remediate the problem or utilise alternative methods of communication. 2. A Request to Pay service must provide the payee with the capability to make a payer aware of the consequences of declining a due payment, receive a reason for the decline (e.g. already paid, etc) and respond to a request declined by a payer (e.g. contacting the payer to further discuss). 3. A payee must strive to action a declined request within a minimum time frame as defined in the contract/agreement between them and the payer.

IV. Education

Request to Pay is a new service being launched into the UK payment market. End-users will have to be educated on how to best to use the service in order to accrue the intended benefits. In addition, we make the following recommendations:

Recommendation	Educating payees and payers on: 1. How to use Request to Pay and the response options it offers.

[11] The Late Payment of Commercial Debt (Interest) Act 1998.

[12] Some design features are dependent or only applicable to the channel or medium through which the Request to Pay is delivered.

	2. The meaning and implications attached to each response. This includes any penalties and legal consequences and the tools that can be used by payees to ensure certainty of payment.

V. Liability and penalties

In the eventuality that a payer falls into debt, they will be contractually or legally liable to certain penalties, as is the case today. Examples include late payment fees and reduced credit score. Request to Pay does not shift the current liability framework and thus does not reduce the certainty of payment in comparison to other payment methods in common use today such as Direct Debit and card payments.

3.8.4 Risk of Uncertainty of Payment Due to Payment Extension

Payment extension is a mechanism that allows payees to offer qualifying payers the chance to extend the pay-by date of their bills. **It provides flexibility to payers on when they can pay and aims to support short-term cash flow constraints**. **Request to Pay's payment extension feature is not meant to address long-term financial distress.**

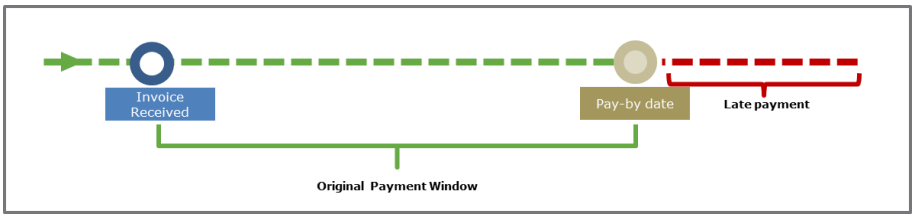

Figure 8: Current Payment Process

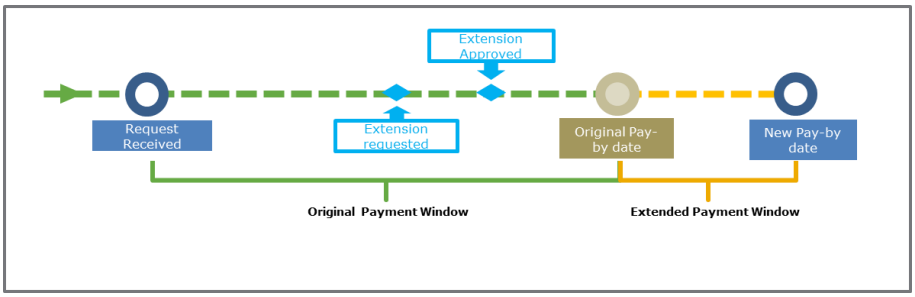

Figure 9: New Payment Process with Payment Extension

Payment Extension is a familiar concept in other countries and is already provided by many companies worldwide. An example of a Payment Extension offered by Vodafone Australia is provided in Figure 10.

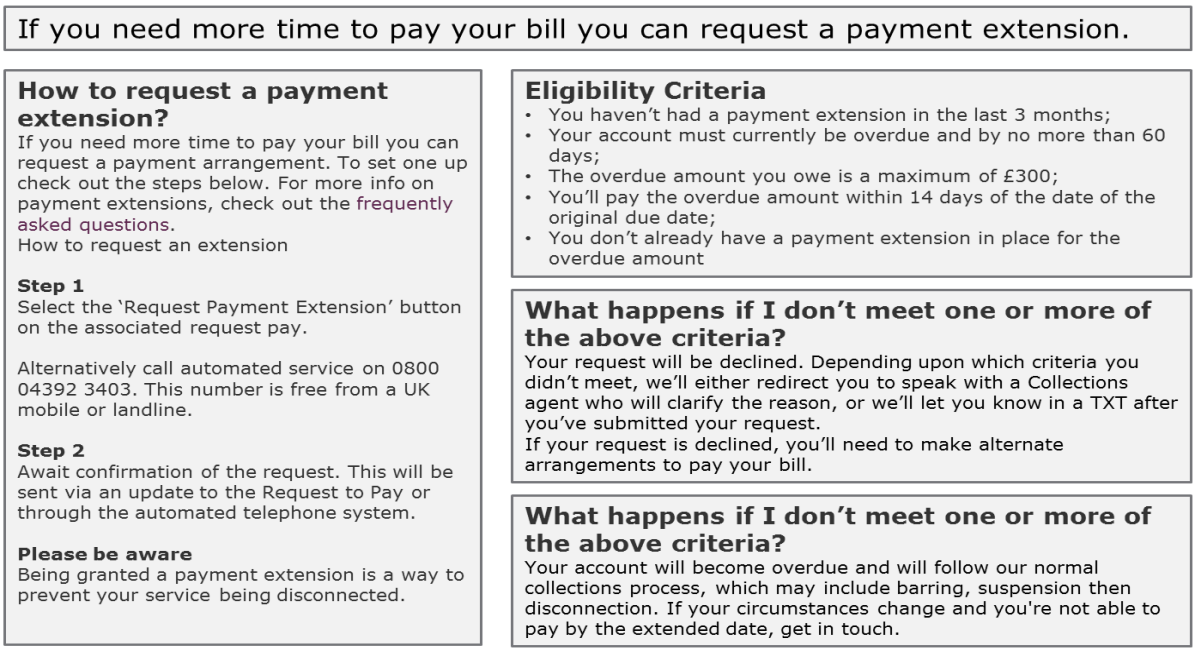

Figure 10: Vodafone Australia Case Study[13]

The payment extension feature of Request to Pay, prima facie, seems to provide the biggest threat to the certainty of payment and the increasing likelihood of a payer falling into debt. We believe that this risk, in reality, is overstated. Additionally, several tools can be applied to further manage this risk. These are listed below.

I. The contract between the payee and payer

As part of the Request to Pay service, payment extension terms must be formalised in the contract between the payer and payee. We recommend the following:

Recommendation	The payee must explicitly specify the terms of any payment extension arrangement in their contract with the payer. These terms must specify the following as a minimum: i. Eligibility to receive an extension and conditions for when a payer can apply for an extension. ii. Eligible length of an extension (maximum and minimum duration). iii. Number of times one can extend. iv. Applicable constraints. v. The means by which the payee and payer will communicate for purposes of payment extension. vi. Applicable timelines and service level agreements: ○ Minimum number of days before the end of the payment window during which a payer can request an extension. ○ Expected length of time that the payer can expect a response to their request for payment. A payee must strive to action a request for an extension within a minimum time frame as defined in the contract/agreement between them and the payer. vii. Any additional fees that might be incurred as a result of the extension where applicable.[14]

[13] https://www.vodafone.com.au/support/billing/payment-extension (As viewed on 19.11.2017)

[14] We do not expect payers to be charged fees for payment extensions. We are conscious that for some products such as interest yielding products, a fee will be necessary, similarly to today. The fees must be proportional to the value of the product offered and the amount of time and effort spent by the payee to provide the extension. This must be outlined in the contractual agreement with the payer and payee and the payer must be notified of any resulting fees and penalties.

II. Technical design

To complement the contract terms, Request to Pay providers can also make use of some technical tools designed into the Request to Pay service:

Recommendation	1. **User education:** Request to Pay providers must put in place the means to notify payers requesting a payment extension that it is meant to address a short-term cash flow deficits and must not be relied upon to manage long-term debt. In addition, Request to Pay providers must put in place the means to make a payer aware of the consequences of delaying a due payment prior to making the request. 2. **Notification**: Request to Pay providers must put in place a notification system to provide information on: ○ The status of the request for an extension, including a confirmation notification when the request is accepted. ○ New pay-by date after extension. ○ Resulting fees where applicable. 3. **Messaging:** In the case where the payee cannot offer an extension, they must provide the payer with a statement that they are unable to offer the service or in particular cases where a request for an extension has been denied.

III. Education

The payment extension feature is meant to tackle short-term cash flow management as opposed to long-term financial difficulty. In light of this, it is imperative to educate both payers and payees on how to use the payment extension feature to avoid any adverse outcomes.

Recommendation	Educating payees and payers on: 1. When and how to request a Payment Extension. 2. Eligibility criteria 3. Terms of a payment extension. This may include any penalties or legal consequences, if any. 4. Alternative and more suitable avenues to manage long-term financial difficulty.

IV. Penalties

Recommendation	1. Credit rating: A payer's credit rating must not be compromised on account of them receiving a payment extension. 2. Debt recovery: Similarly to today, existing debt recovery processes apply to a payer if payment is not made within the extended payment window.

V. Liability

Two scenarios present themselves where liability between the payer and payee requires clarification:

Scenario 1:
The payer denies the request for extension sent by the payer.

Liability:
The bill is due as per the original pay-by date and the liability stands with the payer. See section above on the legal standing on the payer's debt obligation for services and goods rendered.

Scenario 2:
The original pay-by date elapses while the request for extension is still under consideration.

Liability:
The liability falls on the payer. As long as the payment period remains unchanged, the payer is still liable for the payment as per the original terms. See recommendation above on payee best practice in particular response to payer SLAs.

Liability considerations pertaining to Request to Pay are covered in greater detail in the liability section later.

PAYERS IN FINANCIAL DIFFICULTY:

Payees should make considerations for payers in financial difficulty. Codes of practice and best practice approaches should be used to identify the best treatments for the situation.

3.9 Data Protection Impact Assessment

Privacy and Data Protection legislation and in particular the introduction of GDPR in May 2018, are critical elements that will shape overlay services such as Request to Pay. The document in Appendix 1 is the Data Protection Impact Assessment (DPIA) assessing the data protection consideration surrounding the implementation of this Service and identifying corresponding mitigating measures.

As part of this process, the assessment has:

- Considered the benefits that Request to Pay could deliver to data subjects;
- Identified what personal data is required to deliver these benefits, now and in the future;
- Considered the potential data protection risks and issues; and
- Identified safeguards to mitigate these data protection concerns.

To operate successfully, Request to Pay (the "Service", "RtP") will involve the collection and processing by a Request to Pay service provider of personal data including the name and surname of individuals, their date of birth, bank account name and sort code, email/phone number and possibly address. Key personal data (payee's name, bank account and the payer's name) are expected to be captured in Request to Pay messages created by payees and sent to payers using the Request to Pay service. In addition, there is a possibility that personal data captured by Request to Pay will be disclosed to third parties or organisations who have not previously had routine access to such information, for example, outsourcing the identity verification stage to third parties for purposes of verifying KYC information provided.

Personal data will be processed on the basis of consent as the lawful means for purposes of compliance with the General Data Privacy Regulations (GDPR). While the volume of personal data and data subjects in scope is not pre-determined, Request to Pay is expected to be offered across the UK market.

Third parties will primarily be responsible for building Request to Pay consumer-facing solutions including establishing enhanced mechanisms for data protection.

I. Summary of Data Risks, Considerations and Mitigations

While developing Request to Pay, potential data protection risks and related mitigating measures have been considered. The key findings are as follows:

Key Risks	Proposed Mitigations
Service Abuse, Service Fraud: There is a risk that spammers, fraudsters or other malicious actors wrongfully access the Service resulting in misuse of personal data and harm to individuals (i.e. identity theft, fraud).	Request to Pay service providers should be registered/accredited to ensure that the service is trustworthy and reduce the risk of fraudulent use.
Data Security Breaches, Service Failure: There is a risk of technical failure of the Service, exposure to external cyber threats or personal data being inadvertently shared with a third party outside the permissions given. This may lead to material personal data breaches.	Personal data should be encrypted while in transit to mitigate the risk of security breaches. Governance standards from the NPSO are expected to require Request to Pay service providers to establish a minimum standard of information security for the Request to Pay components (e.g. service failure backup plan).

Table 10: Summary of RtP Data Risks, Considerations and Mitigations

Request to Pay will be supported by a service provider and the NPSO as governing body. The NPSO will provide a thin layer of governance on which service providers will be expected to build technical provisions and additional functionalities. These will ensure the objectives of the Service and compliance with the GDPR's accountability and privacy by design requirements are met. The NPSO will also be responsible for registration and certification of Request to Pay service providers.

II. Consultation Process and Next Steps

Development of the NPA requirements and related new end-user solutions were achieved collaboratively through a public consultations, workshops and interviews with various representatives of the main end-user groups: governments, charities, consumer groups, retailers, housing associations, payment service providers (PSPs), and NPSOs.

This has enabled the achievement of an industry-wide position on data protection implications that affect the proposed solutions. In addition, planned consultation with the Data Protection Supervisory Authority may result in conducting further work yet to be defined. The output of these will be incorporated in the Data Protection Impact Assessment.

3.10 Liability Framework and Considerations

A key input into the design of Request to Pay is the identification of roles and responsibilities expected of each of the players in the ecosystem. The corollary is identifying along the Request to Pay journey each actor's responsibility; identifying scenarios requiring the assignment of accountability and finally identifying associated liability frameworks. Clear definition of roles and liability at the design stage is essential to the success of the solution.

Figure 11 below outlines the main players in the Request to Pay ecosystem; their relationship to one another and key obligations that each actor in the relationship model is responsible for carrying out. This is essential in identifying accountability and therefore liability when issues arise.

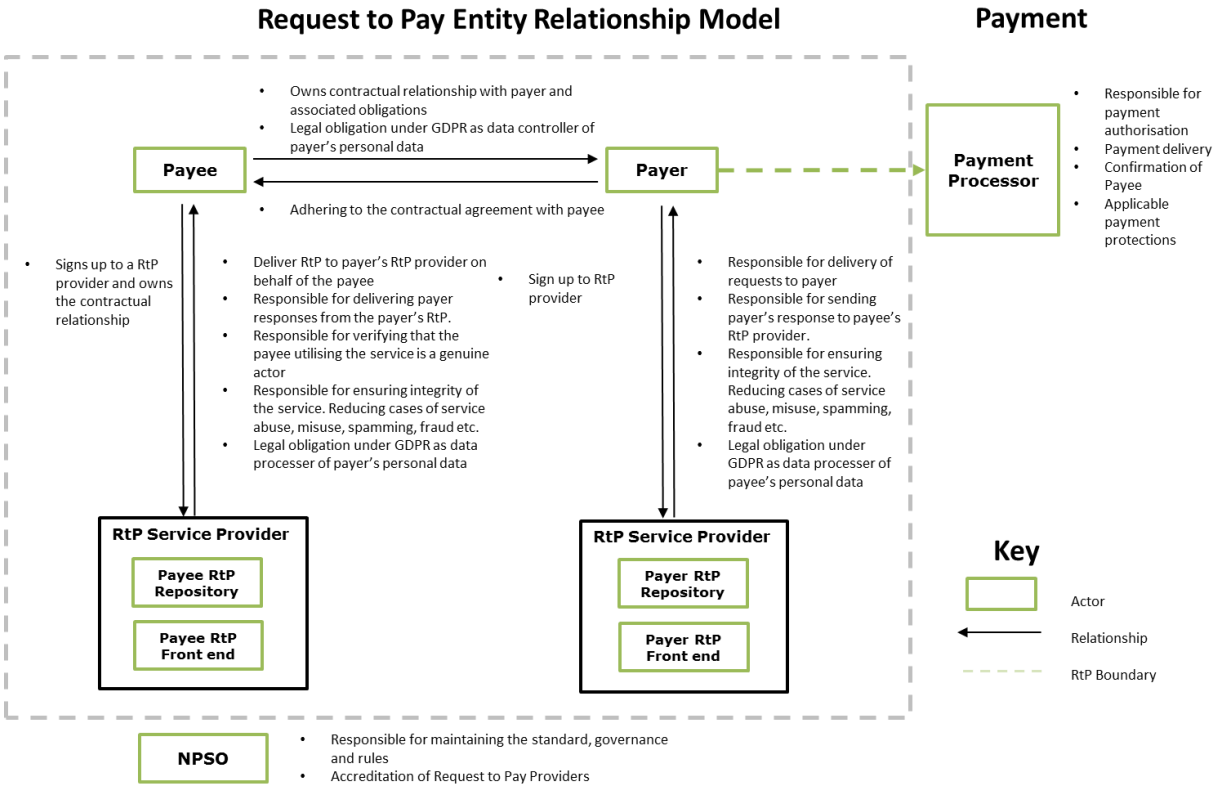

Figure 11: Request to Pay Entity-Relationship Model

3.10.1 Liability Matrix and Associated Assumptions

The matrix below outlines cases of liability, analysis of how this can occur, who is responsible and whether a model exists to address this.

The scenarios are classified into the following main categories: operational, technical and Financial Crime / Data Protection. In developing this matrix several assumptions are made:

I. Request to Pay is a messaging service and separate from the payment types utilised to make the payment associated with the request. As a result, it is assumed that associated liabilities and protections associated with the particular payment method used remain the same.[15]
II. Request to Pay providers will need to be registered payment service providers in line with PSD 2 requirements. In addition, they will be accredited by the NPSO to ensure they meet the standard requirements and rules as well as technical requirements such as security etc.
III. Corporate Request to Pay end-users will be verified before they can send requests. This will ensure that end-users can trust requests sent to them as being from trusted sources.
IV. A dispute resolution process will be put in place that aggrieved persons can utilise to air and resolve disputes.

[15] We recommend that a more detailed analysis is done to validate this assumption focusing on each particular payment method. In particular Direct Debits and Credit/Debit cards where particular liability and consumer protection frameworks exist. It should be understood if any of the final aspects of Request to Pay have any implications for the protections given by certain methods.

Liability	Description/Scenario	Existing liability model?	Where does liability lie?
Operational			
Non-payment	Request to Pay provides payers with the ability to defer or decline a request. This may create a risk that the payer does not pay the payee. In such a case, a liability framework should be in place to define who is liable for the related loss of income, cost of debt management etc.	Yes, there are existing frameworks that address this[16]. The relation between the payer and payee, using Request to Pay, would be underpinned by a contract as is the case today. Each party would be subject to the agreed terms. In the specific case where the payer does not pay the payee, the appropriate contractual terms would apply.	Due to the pre-existing contractual relationship, the payer is liable to the payee. However, it is important to note that in regards to the cost of debt recovery there are certain scenarios where the cost will not fall on the payer.
Persistent debt	There is a risk that payers will defer payments indefinitely which will result in payees not getting paid.	Yes. Similar to the aforementioned case, underlying contractual arrangements would apply. The payer would be liable for any legitimate arrears and associated debt as per current regulations and framework.	The payer is ultimately liable if payment is not made under the specified contractual terms. In some exceptional cases, the payee may be liable. For example, instances where a payee is a vulnerable person. See examples from Financial Ombudsman of this[17]. We do not expect Request to Pay to alter current liability frameworks
Customer interaction risks	Request to Pay is, for the most part, a new service thus there will be new customer journeys. As such it is possible that there are new liabilities arising from this. For instance: • Payers will need to be clear and made aware of the consequence of their actions along the Request to Pay journey. For example, Charges associated	To some extent, existing frameworks can be utilised There are consumer protection laws that state that there must be transparency so as not to mislead the end-user. For instance, the biller must clearly state the consequences of payment extension, [18]	There is a chance that liability lies on the part of the payee if they have acted in a way to deceive the end-user and cause consequential loss.

[16] The law (The Late Payment of Commercial Debt (Interest) Act 1998) currently describes a payment as being late after 30 days for public authorities and business transactions after either the payer gets the invoice or goods and services are delivered (if this is later). A payee can legally pursue the necessary steps to recover a late payment.

[17] Ombudsman news Issue 127
http://www.financial-ombudsman.org.uk/publications/ombudsman-news/127/127-vulnerable-consumers.html

[18] Consumer Protection from Unfair Trading Regulations 2008
https://www.legislation.gov.uk/uksi/2008/1277/contents/made

	with selecting a payment method, impact of selecting a particular response e.g. Decline etc.	Good technical build and UX design in line with consumer protection law and best practices would be needed to mitigate against this.	
Technical			
Service failure	There is a potential risk of harm to end-users (payer, payee) due to a failure of the service. For example: • Due to a service failure, the request does not reach the intended payer • Due to a service failure, the payer's response is not received by the payee and as a consequence, the payee is not made aware of the payer's intention. This is particularly the case where the payer requests for an extension or declines a request. • Consequential loss occurring due to service failure could occur. An example of this would be customer incurring interest charges due to a missed or delayed payment arising from a failure of the Request to Pay service.	Yes. Similar to today, payers are liable to make a payment for service/goods received regardless of whether they have received a bill/invoice. In this case a Request to Pay from the payee. Payees and service providers are, however, expected to operate robust services. In addition, similar to today, frameworks should be in place to provide alternative communication channels.	The payer is still liable to make a payment regardless of whether they receive a Request to Pay or not. In addition to this, there is a responsibility on the Request to Pay service provider to ensure a minimum standard such as adequate speed and reliability of service. As an additional safeguard, it was suggested that user of Request to Pay should be notified of the delivery status of messages. This would allow users to take alternative action in the event of service failure. In the case of service failure, the 'Polluter Pays'[19] principle applies. The party at fault for a negative externality associated with their action should be liable.[20] An example of current providers is of Pingit which provides a Request to Pay service.[21]
Errors	There is a liability for losses/damage arising from errors being made by either the Payee, Request to Pay provider or Payer. For instance: • When a payment is initiated through Request to Pay, the relevant information such as the payment	Today, in the case of bills, billers are liable for losses borne due to error on the part of the biller. In addition, billers will typically provide channels through which payers can query errors in the bill.	All parties along the chain should put in place measures to reduce the likelihood of error and where it does occur, proper corrective measures are applied as soon as possible. The party responsible for the error would be liable for

[19] OECD definition: https://stats.oecd.org/glossary/detail.asp?ID=2074
[20] It is recognised that more work will need to be done by the NPSO in ensuring that this is validated both from a legal position, ensuring it captures any nuances that may not be recognised at present.
[21] See section 7 of the Pingit Terms and Conditions (Accessed 08/11/2017) https://www.barclays.co.uk/P1242604890843

	amount and account details are transferred into the payment. In case of error in this process, harm could result in one or several parties. Examples of this include wrong payment amount, misdirected payment etc. • There are also cases of error made on the part of the payer. For instance, if a payer pays an amount they do not mean to, how does the payer get the money back and who is liable if the money is not refunded? • In turn, the information on the request such as the payment amount, account details could be wrong resulting in harm.	In the case of misdirected payments due to payer error, the payer is liable. Additionally, in the case of a system error made when a message is being transferred to a payment instruction. The service provider is liable.	losses/damage resulting from the error. A dispute resolution process should be in place that aggrieved persons can utilise to resolve disputes arising between Request to Pay participants where current dispute resolution processes may not apply. This process would not be limited to just disputes arising from error.
Fin Crime / Data Protection			
Service abuse and fraud	There is a risk that spammers, fraudsters or other malicious actors will misuse the service resulting in harm to the end-users. In particular: • False payee accounts posing as legitimate billers sending spam requests to payers • Request to Pay being used for money laundering. • The service being used for malicious purposes other than monetary gain. For instance, using Confirmation of Payee (CoP) to identify and stalk individuals.	There are pre-existing legislation and regulation to mitigate against fraud and service abuse. Victims are able to take legal action against perpetrators. Regulations also exist that place responsibility on service providers to ensure that they put in place adequate measures to ensure the integrity of their systems and the safety of customer data.	In principle, the party responsible for actions leading to damages/loss should be liable – including fraudsters. Request to Pay service providers may be liable if they are unable to demonstrate a minimum standard of security. Request to Pay is a messaging service and separate from the payment type utilised to make the payment associated with the request. As a result, it is assumed that associated liabilities and protections associated with the particular payment method used remain the same.[22]

[22] We recommend that a more detailed analysis is done to validate this assumption focusing on each particular payment method. In particular Direct Debits and Credit/Debit cards where particular liability and consumer protection frameworks exist.

Breach of data privacy, protection and ownership	Some of the data utilised in the Request to Pay overlay services is personal data. This raises concern about data protection and privacy.	Yes, privacy impact assessments are required as part of GDPR. Service providers must be able to prove compliance with existing data protection regulations. In the event of a data breach, GDPR requires certain measures in such cases e.g. Notification of relevant authorities within 72 hours, giving full details of the breach and proposals for mitigating its effects.	Liability lies with data controller and in some cases the processor as well.

3.11 Dependencies

To successfully deliver the Request to Pay service described, several dependencies were identified. These are summarised in Table 11:

ID	Title	Description	Impact
001	Open Banking APIs data pass through	Transferring of Request information & Enhanced Data through to the payment service provider will likely be through the Open Banking APIs.	Request to Pay services are dependent on Open Banking APIs being in place, otherwise custom Request to Pay APIs may be required.
002	Cash payments	For payers to use cash, a physical point of service will be required, e.g. dependency on access to retail location or self-service kiosk.	Lack of organisations with physical branches or point of services may hinder Request to Pay cash acceptance.
003	Third party uptake	Request to Pay is meant to be competitive and as such is dependent on third parties to build consumer-facing solutions.	If Request to Pay is not convincing for third parties, payers and payees, adoption may be hindered.
004	Onboarding	Payer onboarding/KYC/validation will be left in the competitive space for PSPs/ Request to Pay service providers to manage – however a set of guiding principles will need to be developed.	Potentially overly strict or overly slack onboarding and identity verification requirements and processes.
005	Request to Pay Use Cases – Payer – Initiate Payment	Once a payment is initiated, the relevant data is added to the payment transaction. This additional data is expected to be via the Enhanced Data capability.	The impossibility of information (Enhanced Data; all information additional to payment details) cascading from Request to Pay message to the actual payment.

Table 11: Request to Pay Dependencies

4 Assurance Data

In our Strategy, we identified a need for assurance over key facts about a payment, e.g. the availability of funds to make a payment, the correct destination of the payment prior to paying, the status of the payment while 'en route' to the payee[23], and the delivery status. This increases end-users' confidence.

We proposed a suite of tools collectively called Assurance Data, which will consist of 3 main parts:

1. Provision of real-time balance information
2. Confirmation of Payee.
3. Payment status and tracking.

In combination, these 3 tools will provide assurance over the lifecycle of the payment: initiation, processing and receipt.

I. Real-time Balance

We also identified the lack of real-time balance information as a detriment affecting payers. A payer is prone to making a payment they cannot cover, due to lack of information on the funds available to them.

II. Confirmation of Payee

Confirmation of Payee (CoP) will provide a payer with information to give them assurance that the account to which they are making the payment belongs to the intended payee. This will help to address the detriment associated with misdirected payments.

As a special case, CoP will also include a Confirmation of Payer capability. Confirmation of Payer addresses the need for a payee setting up a payment mandate (direct debit) to verify that the account, from which they will be initiating the payment, belongs to the intended payer.

To understand how CoP attempts to solve associated detriments it is important to define misdirected payments, the various types and their causes.

A misdirected payment is a payment where the beneficiary is different from the payer's intended payee, as seen in Figure 12.

Figure 12: What is a Misdirected Payment?

Misdirected Payments are due to several causes which are summarised in Figure 13.

[23] The level and nature of status tracking varies across the payment methods.

Where a payer successfully pays their intended payee, but the goods or services the payment relates to fails to materialise (i.e. because the payee is a fraudster or scammer), this is not considered to be a misdirected payment. CoP will not solve this type of scam. This is, however, one of the detriments under consideration within the Forum's 'Improving Trust in Payments' work.

Figure 13 illustrates the types of misdirected payments addressed by CoP. It also provides a comparison to those not addressed.

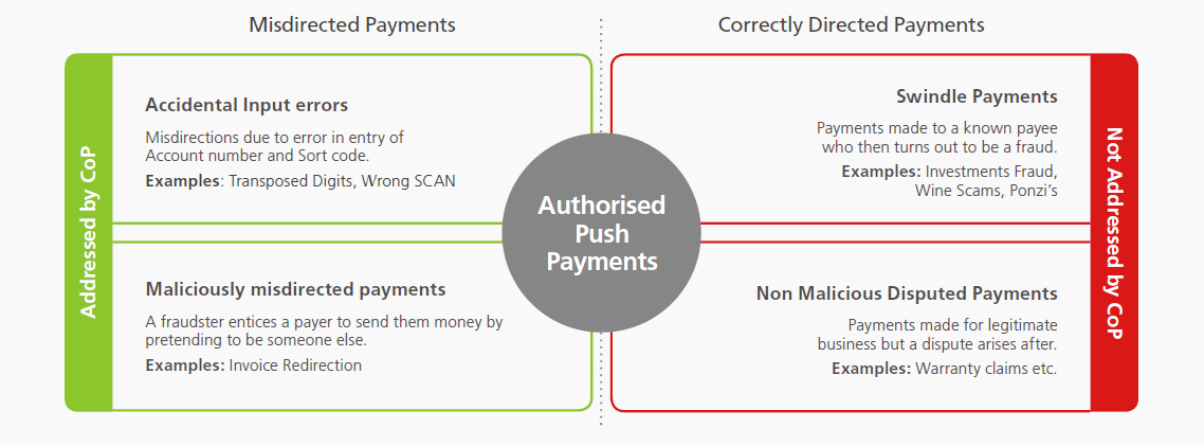

Figure 13: Types of Payment Misdirects Addressed by Confirmation of Payee

4.1 Detriments Addressed by Assurance Data

The key detriments addressed by the Assurance Data solution are listed in Table 12:

ID	Detriment Group	Detriment
2	Customer Control	Payers and payees need more mechanisms for payments that give greater control to the payer and more certain outcomes for the payee.
3,4, 5,6	Customer Assurance: Additional functionality for both payer and payee	Payers and payees require additional functionality in order to be able to: • confirm payee (validation of name or proxy regarding payment account details) • confirm adequate funds are available to cover payment • confirm the status of payment • confirm receipt of payment
12	Customer financial capability	Competition is not currently meeting user needs for transparency.
13	Customer financial capability	Competition is not currently meeting user needs for control.
25	Customer identity, authentication and knowledge	Customers have day to day concerns about the risk of identity theft and risk of fraudulent activity on an account.
26	Customer identity, authentication and knowledge	A payment is made to a wrong account.

ID	Detriment Group	Detriment
28	Customer identity, authentication and knowledge	Businesses pay into accounts not owned by their suppliers due to false invoices or false change of bank account notifications.
29	Customer identity, authentication and knowledge	The industry needs to better understand who the payment initiator (payer) is and the paying account.
30	Customer identity, authentication and knowledge	The industry needs to better understand who the payment recipient (payee) is and the beneficiary account.

Table 12: Assurance Data Detriments

4.2 Scope

4.2.1 In Scope

#	Item	Description
1	British Pound (£) accounts capable of making/receiving payments in the UK to Sort Code and Account Number addressable accounts (SCAN)	Payments made by/to British Pound accounts in the UK that have a sort code and account number are in scope.
2	Sort Code and Account Number addressable accounts (SCAN)	Accounts bearing a sort code and account number. They are the most common retail accounts in the UK, i.e. current accounts, head office collection accounts and some saving accounts.
3	2nd tier accounts	These are accounts that are not directly addressable using a sort code and account number. They may be indirectly addressable via SCAN accounts, if additional information is provided, i.e. roll no. accounts, credit card accounts, some savings accounts, mortgage accounts and investment.
4	Payment Schemes	• Faster Payments • Bacs Direct Credits • CHAPS

Table 13: Assurance Data In-Scope

4.2.2 Out of Scope

#	Item	Description
1	Cheques	Data that is not relevant to the payment is out of scope.
2	Card payments	Card transactions exist on a parallel infrastructure, external to the main payment infrastructure, operated by the card issuer. The Forum considers these out of the scope of its work.

Table 14: Assurance Data Out of Scope

4.3 High-Level Use Cases

The high-level functional overview of Assurance Data solution i.e. Confirmation of Payee/Payer and Payment Status from the payer's and payee's view are depicted in Use Case Diagrams Figures 14 and 15. They exhibit the functions identified as minimum 'core proposition' for customers to ensure consistent experience and 'competitive' functions that are open for innovation to offer more value to the users and promote healthy competition in the market.

Use cases are represented through UML diagrams followed by Tables 15 and 16 providing a short description for each of them.

4.3.1 Payer Use Cases Overview

The following diagram presents the Assurance data use cases from a Payer Perspective.

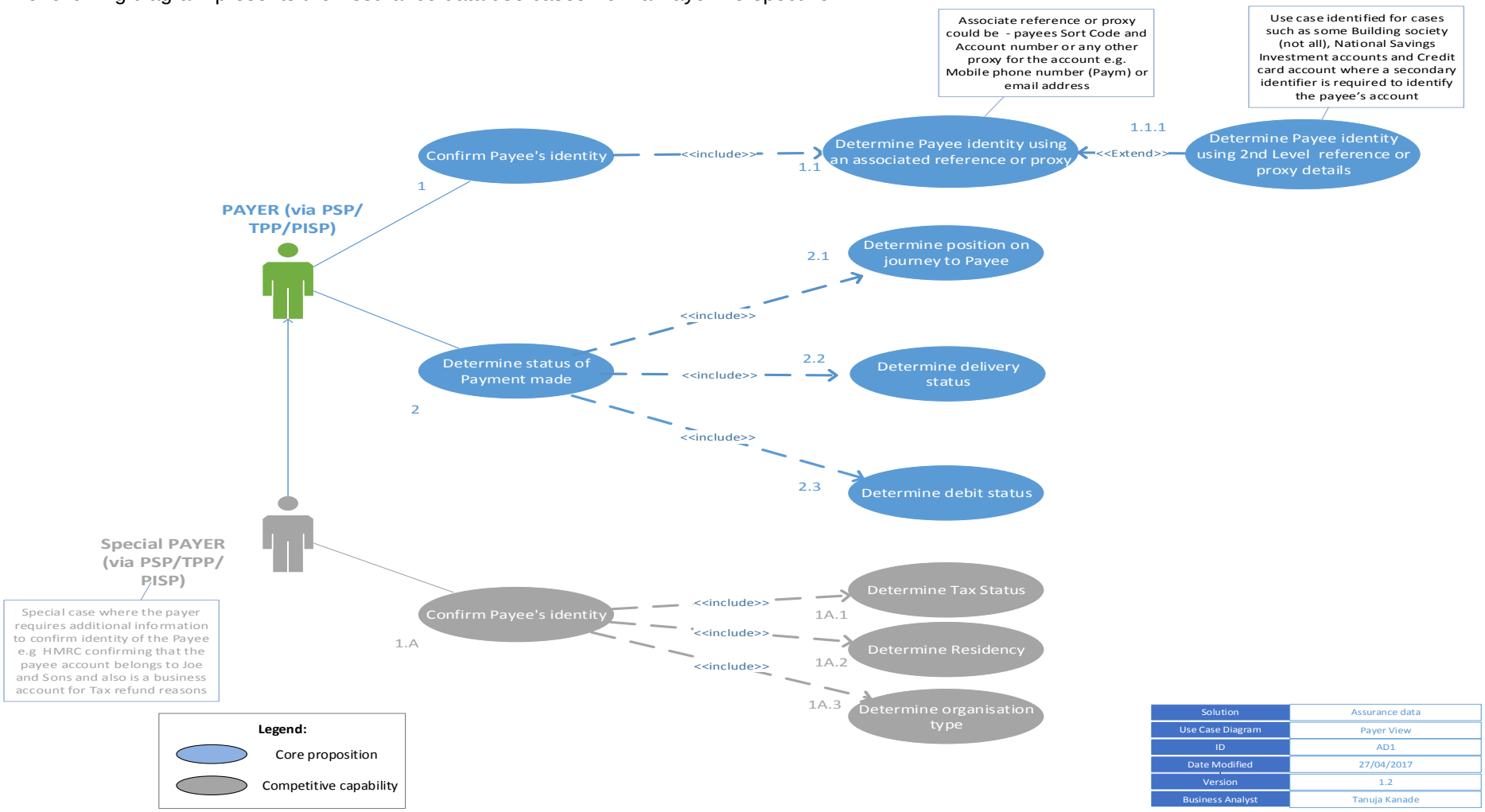

Figure 14: Assurance Data Payer Use Case

4.3.2 Payee Use Cases Overview

The following diagram presents the Assurance data use cases from a Payee's perspective.

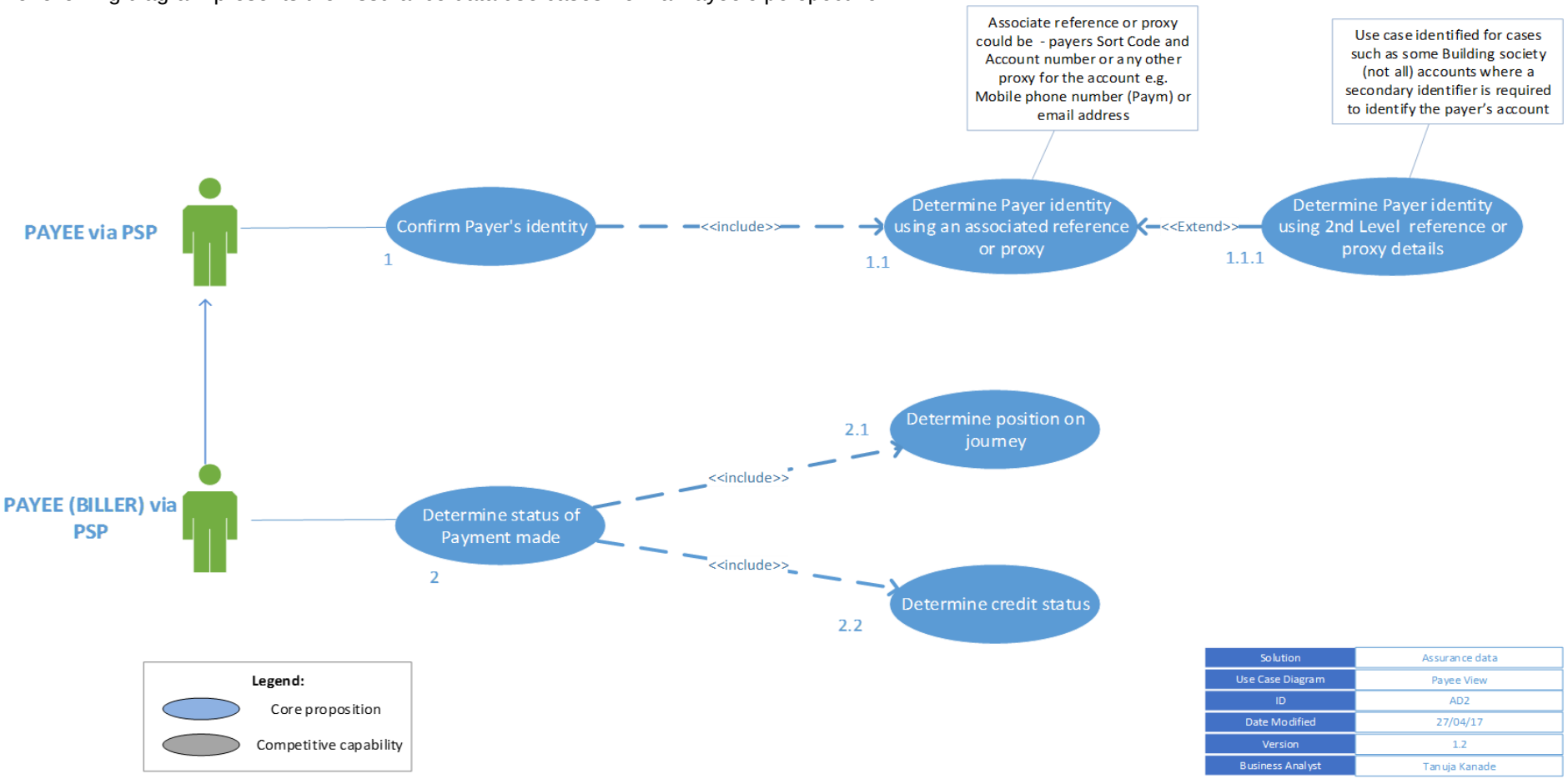

Figure 15: Assurance Data Payee Use Case

ID	Use Case	Description
1	Confirm payee's Identity	The payer wants to make a payment to a payee but before doing so wants certainty that the destination account is the payee's. For example, a personal customer 'A' making a payment to another personal customer 'B' wants confirmation that an account belongs to 'B' before making a payment.
1.1	Determine payee's identity using an associated account reference or proxy	To enable the payee's identity to be confirmed, the payer has to provide sufficient information for the destination account and payee to be identified. This could be the sort code and account number or some other reference or proxy that can be resolved back to the payee.
1.1.1	Determine payee's identity using an associated account reference/ proxy for 'indirectly addressable' accounts	The location of the destination payee account may require additional account reference beyond the primary sort code and account number. For example, making a payment to a credit card account, NS&I savings account or other accounts which require secondary reference data such as credit card number or roll/investment number account.
2	Determine status of payment made	After making a payment the payer wants confirmation that the payment has reached the payee's account. In the event that the payment does not reach the payees account in real time, either through design or error, the payer needs to be able to determine where the payment is in the process and, for conditions where the process has been halted and/or delayed, the reason for it not to reach its destination.
2.1	Determine delivery status	A payer needs confirmation that the amount paid to a payee has been received.
2.2	Determine position on journey to payee	A payer needs to determine that a payment has reached its destination and in the event that the process does not complete, be able to understand where the payment is in the process and whether there is a reason for it not to be complete.
2.3	Determine debit status	A payer needs confirmation that the payment has been debited from their account and subsequently credited to the destination account and value transferred - i.e. available balances are amended.
1A	Confirm payee's identity (special case)	In addition to confirming the payee's destination account, there are circumstances where a payer could potentially obtain additional information concerning the payee and destination account. For example, tax status, residency and type of organisation.
1A.1	Determine Tax status	As a special case, a payer is able to confirm the tax status of the account holder as recorded by the payee's PSP.
1A.2	Determine Residency	As a special case, a payer is able to determine the residency of the account holder as recorded by the payee's PSP.
1A.3	Determine organisation type	As a special case, a payer is able to determine the type of organisation as recorded by the payee's PSP.

Table 15: Assurance Data Payer Use Cases

ID	Use Case	Description
1	Confirm payer's identity	The payee wants to instruct the payer's PSP to make a payment to them (e.g. a Direct Debit or other regular pull payment) but before doing so, seek information on whether the payer's payment account details are correct and the account associated belongs to the payer. For example, a charity customer 'A' that wishes to accept recurring payments from a personal customer 'B' wants confirmation that 'B's account details i.e. a sort code/account number/or other proxy is associated with 'B' before setting up the payment instruction with B's PSP.
1.1	Determine payer's identity using an associated account reference or proxy	To enable the payer's identity to be confirmed, the payee has to provide sufficient information for the destination account to be identified. This could be the sort code and account number or some other reference or proxy that can be resolved back to the payer's account.
1.1.1	Determine payer's identity using an associated account reference or proxy for SCAN accounts.	The location of the payer's account may require additional information beyond the primary sort code and account number. For example, making a payment from a SCAN account may require secondary reference data such as a roll number.
2	Determine status of payment to be received	After payer has made a payment, the payee will want clarity on when a payment is received into their account and the resultant available balance.
2.1	Determine position on journey to payee	A payee needs to determine that a payment has reached their account and in the event that the payment has not been received, be able to understand where the payment is in the process and if not completed, the reason.
2.2	Determine credit status	A payee needs confirmation that the payment has been credited to their account and subsequently available balances are amended.

Table 16: Assurance Data Payee Use Cases

4.4 High-Level User stories and Rules

4.4.1 Payer User Stories and Rules

1. Confirm payee's identity

	As a payer, I want to be able to:
Confirming payee's identity	1. Determine that a payee's account information belongs to the intended payee so that I can correctly identify the payee before making payment. 2. Confirm a payee through any of the existing and future payment initiation channels such as online, mobile app, TPSP or Direct Access.

	3. Get a real-time (a few seconds) response when I enter the details to confirm a payee so that I can receive the information at that moment when I need it. 4. Have sufficient information from the response so that I can take a decision (to accept or reject) on the payee's identity before making a payment.
Rules	1. All banks must participate in CoP service. 2. CoP service must be used only with intent to make a payment. 3. A CoP request must return a response irrespective of success and failure. 4. If CoP request pertains to an account that has been switched under CASS the payer must be informed that the account has been transferred. 5. The CoP response must be returned to the payer in real time (<5 sec). 6. CoP service must be available to check personal (current/savings) accounts, joint accounts and trading (business) accounts. 7. There must be safeguards in place for CoP service participants, e.g. resolution process in case of errors or disputes. 8. The financial model for CoP service must be clearly defined to articulate any service charges and incentives for the CoP participants.
Protecting user's identity	As a user in exceptional circumstances… 1. I should be able to restrict access to my identity.
Rules	1. Under certain circumstances, an individual can on "grounds relating to his or her particular situation" be exempted from the CoP service. 2. There must be clear criteria in place to determine suitability to grant exemptions from the CoP service. 3. CoP providers should put in place a reasonable limit to the number of lookups that can be performed by a payer within a given time period. The value is dependent on the payer type and the individual's PSP.
Sending a request for Confirmation of Payee	As a payer's PSP / TPSP I want to be able to: 1. Know that CoP requests are being sent for legitimate purposes, i.e. for the purposes of making a payment, so that I can be sure that no one is obtaining customer details for the wrong purposes.
Rules	1. Providers of the CoP service must put in place demonstrable measures to minimise the chances of the service being used for any other business apart from confirming legitimate activities. 2. CoP data cannot be used for any other purposes apart from use of the CoP service.

1.1. Determine Payee identity using an associated account reference or proxy

	As a payer, I want to be able to:
Providing an associated reference or proxy against which to confirm payee's account	1. Determine the identity of a payee using associated account reference or proxy such as sort code, account number, mobile number and other so that I can have certainty I am paying the intended payee.
Rules	1. The combination of account references or proxy must be unique to a given individual or individuals (in the case of a joint account).

1.2. Determine Payee identity using an associated account reference or proxy for SCAN accounts

	As a payer, I want to be able to:
Providing an associated reference or proxy to confirm a payee SCAN account.	1. Determine the identity of a payee whose account is not directly addressable (e.g. some building society accounts, investment accounts or a credit card account), using associated account reference or proxy such as roll number, NS&I account number, credit card number or email address so that I can be sure that payment is made to the intended payee.
Rules	1. The combination of account references or proxy must be unique to a given individual or individuals (in the case of a joint account).

2. Determine status of a payment made

	As a payer, I want to be able to:
Confirming the status of a payment made	1. Determine the status of a payment I have made so that I can take appropriate action.

2.1. Determine delivery status

	As a payer, I want to be able to:
Obtaining delivery status of a payment made	1. Determine the delivery status of a payment so that I know the payment has been successfully delivered, failed or rejected. 2. Determine the destination account details when a payment is successful so that I know the payment was credited to the intended payee's account.
Rules	1. Confirmation of receipt must include time, date and delivery account number.

2.2. Determine position on journey to payee

	As a payer, I want to be able to:
Ability to track a payment	1. Know the payment's position on its journey to the payee's account so that I am aware of the payment's status throughout the journey.

	2. Track payment status in the event that a payment has failed to reach its intended payee so that I can take appropriate action.
Rules	1. In the event that a payment does not reach the payee's account in real time either through design or error, then a payer must be able to determine where the payment is in the process and the reason if it has been halted or delayed. 2. Any advice to a customer concerning the (non) processing of a payment should consider regulatory requirements including, for example, provisions around 'tipping off'.

2.3. Determine debit status

	As a payer, I want to be able to:
Receiving confirmation that payment has been debited from the payer's account	1. Receive the debit status of a payment I have made so that I can determine my account balance available to use.
Rules	1. The payer's PSP must provide the payer with information on debits made from their account and the resultant change in balance. 2. The payer must be provided with a debit status sufficient to determine whether the funds are conditionally or unconditionally debited. 3. The payer's debit status must be updated within a reasonable time frame from the point of the transaction being made (<10 minutes).

4.4.2 Payee User Stories and Rules

1. Confirm Payer's identity

	As a payee, I want to be able to:
Confirming payer's identity	1. Confirm that a payer's account belongs to the payer so that I can be sure that they own the account against which I am setting up a pull payment. 2. Get a real-time (a few seconds) response when I enter the details to confirm a payer so that I can receive the information at that moment when I need it. 3. Have sufficient information from the response so that I can take a decision to accept or reject the payer's identity before initiating a pull payment.
Rules	1. The response will be returned to the payee in near real time (< 5 sec). 2. The Payee must be presented with sufficient information to positively confirm the payer. 3. All payer PSPs must 'subscribe' to the service so that all payers are in scope.

	As a payee's ASPSP I want to be able to:
Receiving a request for Confirmation of Payer	1. Know that Confirmation of Payer requests are being used for legitimate purposes i.e. for the purposes of creating pull payments such as a Direct Debit.
Rules	1. Providers of the Confirmation of Payer service must put in place demonstrable measures to minimise the chances of the service being used for fraudulent activities.

1.1. Determine Payer's identity using an associated account reference or proxy

	As a payee, I want to be able to:
Providing an associated reference or proxy against which to confirm Payer account	1. Determine the identity of a payer using associated account reference or proxy such as sort code, account number, mobile number and other so that I can be sure that I am pulling the payment from the intended payer.
Rules	1. The combination of account references or proxy must be unique to a given individual or individuals (in the case of a joint account).

1.2. Determine Payer's identity using an associated account reference or proxy for SCAN accounts

	As a payee, I want to be able to:
Providing an associated reference or proxy to confirm a payer SCAN account	1. Confirm the identity of a payer whose account is not directly addressable (e.g. SCAN accounts), using associated reference or proxy such as roll number, NS&I account number or email address so that I can be sure that I am setting up a pull payment against the intended payer.
Rules	1. The combination of account references or proxy must be unique to a given individual or individuals.

2. Determine status of payment to be received

	As a payee, I want to be able to:
Confirming the status of a payment to be received	1. Determine the status of a payment I am expected to receive so that I can take appropriate action.

2.1. Determine position on journey to payee

	As a payee, I want to be able to:
Ability to track a payment	1. Know the payment's position on its journey to my/company's account so that I am aware of the payment's status throughout the journey. 2. Track payment status in the event when payment has failed to arrive so that I can take appropriate action.

Rules	1. In the event that a payment does not reach the payee's account in real time either through design or error, then a payee should be able to determine where the payment is in the process and the reason if it has been halted or delayed. 2. Any advice to a customer concerning the (non) processing of a payment should consider regulatory requirements including, for example, provisions around 'tipping off'.

2.2. Determine credit status

	As a payee, I want to be able to:
Receiving confirmation that payment has been credited to payee's account	1. Receive the credit status of a payment I have received so that I can determine my account balance available to use.
Rules	1. PSPs must make available to a payee credit status information sufficient to determine whether the funds are conditionally or unconditionally credited. 2. The payee's PSP must provide the payee with information on credits made to their account and the resulting change in balance.

4.5 Proposed End-to-End Journeys

4.5.1 Confirmation of Payee

The Confirmation of Payee end-to-end journey is illustrated in Figure 16.

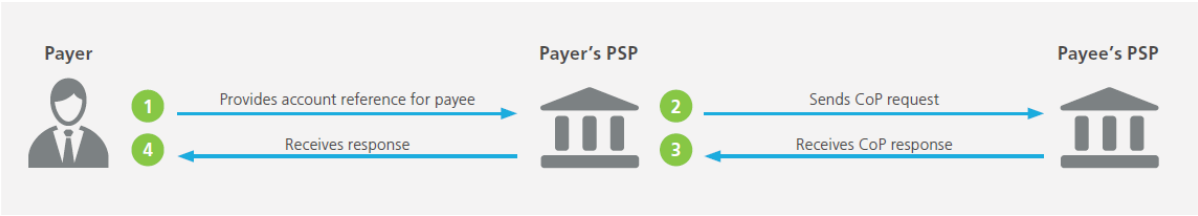

Figure 16: Confirmation of Payee End-to-End Journey

#	Step Name	Description
1	Provides account reference for payee	The payer provides the account reference details (e.g. sort code and account number) to their PSP.
2	Sends CoP Request	The payer's PSP sends CoP request to the payee's bank.
3	Receives CoP response	The payee's PSP sends a response back to the payer's PSP.
4	Receives response	The payer's PSP presents the response to the payer. The payer makes a decision based on the COP response.[24]

Table 17: Confirmation of Payee End-to-End Journey

[24] Payer is always in control.

I. Base standard Design

We considered several designs in our work. This was informed by an assessment of the two main approaches currently in the market. Following an analysis of these two approaches, including a public consultation we settled on a design that we have put forward as the base standard design for the CoP solution.[25] We combined the advantages and disadvantages of previous designs into an approach that provides assurance to payer while taking data privacy into consideration. Our proposed design is detailed in the section below.

In our consideration and design of the CoP base standard design we were guided by several main requirements:

1. The response presented to the end-user for a Confirmation of Payee request must be clear and unequivocal
2. The information presented to the end-user should increase their assurance that they are making a payment to the intended payee's account
3. The approach taken must take into account likely attempts to abuse the service by fraudsters and other bad actors and should by design reduce the likelihood of such activities succeeding
4. Data privacy considerations and regulations must be met[26]
5. The approach taken should allow for competitive delivery of CoP on multiple payment channels and methods. Online, telephone, Faster Payments, BACs and Chaps.

The proposed approach is illustrated in Figure 17.

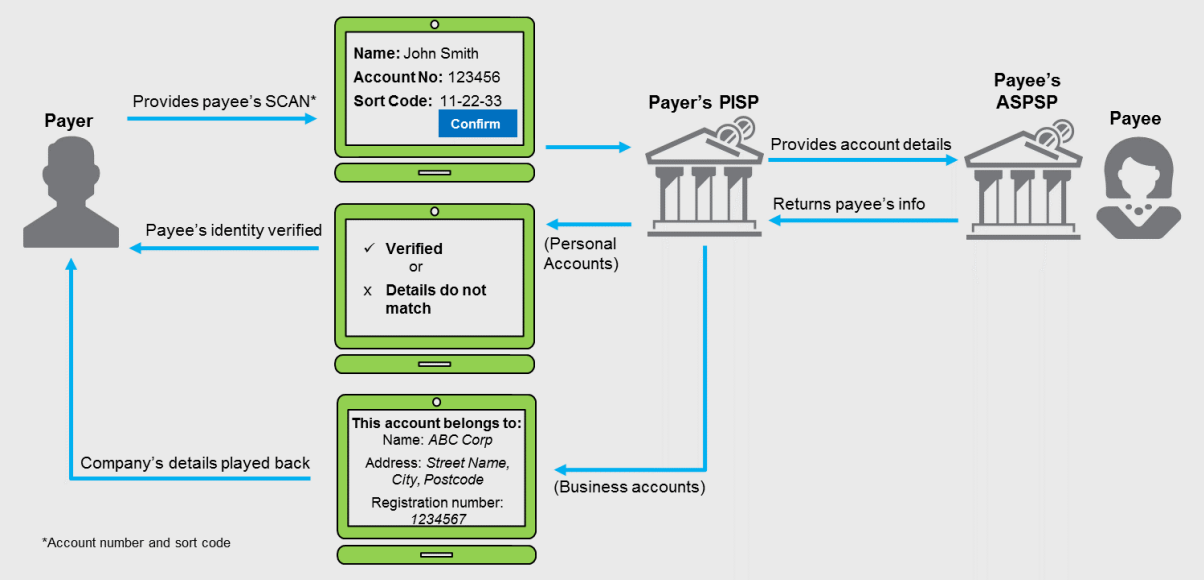

Figure 17: Confirmation of Payee base standard design approach

The approach involves the following main actors:

I. **Payer:** The payer initiates the CoP request[27]. They are tasked with providing the information required to carry out a confirmation of payee check. They would also at the tail end of the process receive the CoP response and based on this make a decision on whether the account belongs to the intended payee.

[25] Detailed analysis of the two main CoP response designs in the market is presented in Appendix 4.

[26] See separate Privacy Impact Assessment in Appendix 6.

[27] In theory, the payer can conduct a confirmation of payee, at the point of setting up a payee or making the payment. Based on our analysis and input from various industry parties, we recommend that the payer conduct the confirmation of payee when setting up the payee for the first transaction. Once this has been done, there would be no need to carry out the check for every payment unless the payee's account details change or a significant length of time has gone by since the last check.

The payer provides the following information:

a. **Beneficiary (Payee) account name:** The payee's beneficiary account name as recorded on their account.[28] [29]
b. **Beneficiary's account number:** The beneficiary's account number
c. **Beneficiary's sort code:** The beneficiary's sort code.

II. **Payee:** The payee has the responsibility of providing the payer with all the information required that is also sufficiently correct to carry out a confirmation of payee check. For purposes of Confirmation of Payee, payee's fall into two categories as determined by their **account type**:

a. **Personal account holders:** Non-corporate entities operating personal accounts as single individuals or jointly. Such entities include individuals and sole traders[30]
b. **Business account holders:** Company entities operating business accounts. Such entities include: Public limited company (PLC), Private company limited by shares (LTD), Company limited by guarantee, Unlimited company (Unltd), Limited liability partnership (LLP), Community interest company, Industrial and Provident Society (IPS), Royal Charter (RC)

III. **Payer's PSP:** The payer's PSP provides the payer with the confirmation of payee service as part of payment initiation. The payer's PSP will:

a. Collect the information required from the payer
b. Identify the payee's account provider and pass it on to account provider as a confirmation of payee request as well as receive resulting response from the payee's account provider
c. Process the response provided factoring in the information provided by the payer to determine whether the account belongs to the payer's intended payee
d. Provide a clear and unequivocal response[31] to the payer on the result of the confirmation of payee check. The information provided in the response type to the payer is dependent on the payee's account type.

For personal accounts, the payer's bank returns an affirmative or negative response[32] [33]

For business accounts, the payer's bank returns the **payee's business name, registered address,** as well as a **third party identifier** that the payer can verify with a third party such as the **company registration number** which the payer on their own volition can verify with companies house.[34] [35]

---

[28] We recognise that the manner in which account names are generated and captured is non-standard across the various PSPs in the UK. This provides a likely challenges for use cases such as Confirmation of Payee where the payee's account name may differ from their account name. While this regime persists, we make several considerations to reduce the challenges resulting as a result. See considerations section.

[29] We recommend that PSPs in the design of their customer channel provide clear and easy ways to capture the beneficiary account name.

[30] It is technically possible for a sole trader to utilise their personal account for business purposes. However, our research from speaking to most of the PSPs represented on the Forum and larger community we established that practice is frowned up and in most cases disallowed in the personal account terms and conditions. As a result most sole traders tend to use business accounts for business transactions.

[31] We leave it to individual PSPs to design the most suitable way to display the confirmation of payee responses to the payer. We are however keen that as a standard the response should be clear and unequivocal. In particular we discount response approaches where the payer is presented with a probability or scale based on which they are then required to make a decision. Our research shows that this approach does not provide payer's with increased assurance.

[32] In our consultations with the payments community and various stakeholders such a consumer groups and the data commissioner's office, a recurring concern was around the risk arising from payee personal data being shared outside the frameworks set out in the data regulations. In particular GDPR.

[33] Personal data in this case would only apply to the names of individuals holding personal accounts as Business names and associated information is classified as public information.

[34] From repeated stakeholder input, we established that to provide the required payer assurance, a confirmation of payee service should provide additional information for corporate payees in comparison to personal accounts. In addition, evidence gathered from Which? and the PSR as part of the Which? Super complaint on APP scams evidenced the propensity for fraudsters to utilise accounts bearing names very similar mainstream companies.

[35] We recognise that there is a minority of corporates with UK accounts that are not registered with company's house for example foreign companies. We recommend that in the next phase of design and implementation more detailed analysis is done to identify these exception cases and appropriate alternatives provided.

e. As at the time of this document being published the PSR is in the process of consulting on a contingent reimbursement model for losses arising due to APP scams. Should this come into effect as detailed, the payer's bank may bear liability in applicable circumstances. See PSR consultation paper for more information. https://www.psr.org.uk/psr-publications/consultations/APP-scams-report-and-consultation-Nov-2017

IV. Payee's PSP: The Payee's PSP holds the payee's account. They are tasked with:

a. Receiving confirmation of payee requests from the payer's PSP
b. Based on the information provided, responding appropriately to the payer's PSP with the payee's account details required for the given account type.

For **all accounts,** the payee's PSP returns the **account name** and **account type**
For **business accounts,** in addition to the account name and type**,** the payee's PSP provides the business's registered address and company registration.

II. Architecture

To support the above design, Confirmation of Payee service can be provided as a centralised service by one entity or as a distributed service provided by multiple entities competitively. Upon analysis based on existing models and input from multiple stakeholders we propose, an API based implementation enabled by a standard API connectivity. This would allow for competition in the market for the provision of CoP services which should ideally result in better services to end users.

The model is illustrated in Figure 18 below.

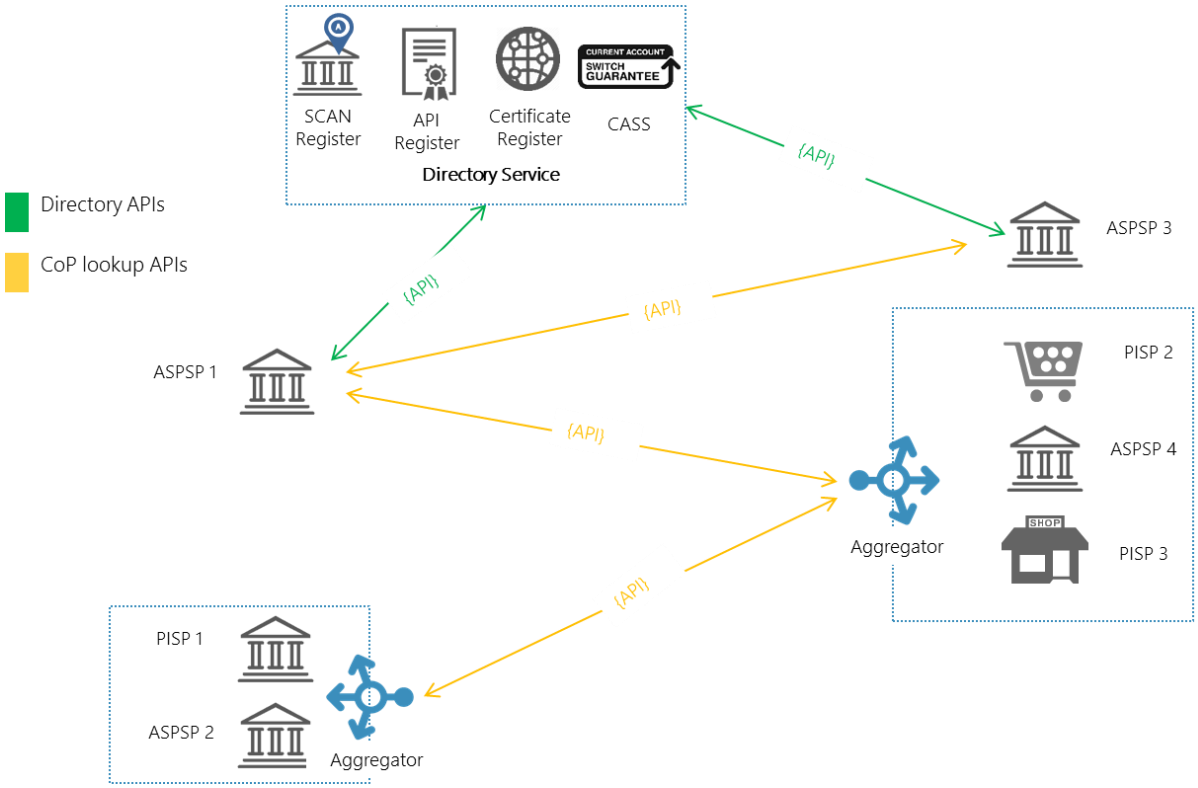

Figure 18: CoP Architecture

The CoP architecture includes 4 main components:

1. **APIs:** The backbone of the service is an API layer allowing CoP requests to be made directly or indirectly between the payer's and payee's account servicing PSP.

2. **CoP End-users:**
   i. ASPSP for payers and payees
   ii. PISP for payers
   iii. NPSO as a regulator
3. **Directory Service:**
   i. Maintains and updates certified participants register and API requirements
   ii. Allows payer's PSP to determine payee's PSP and vice versa
   iii. Provides the API details for the respective payee's PSP
   iv. Facilitates authorised participant access to the system (certificates)
4. **Aggregators:** PSPs not able or wishing to implement APIs would utilise 3rd party providers to indirectly participate in the CoP service.

The detailed design of the APIs and components parts will be carried out by the NPSO in a subsequent phase of implementation.

4.5.2 Payment Status and Tracking

The Payment Status and Tracking end-to-end journey is illustrated in Figure 19.

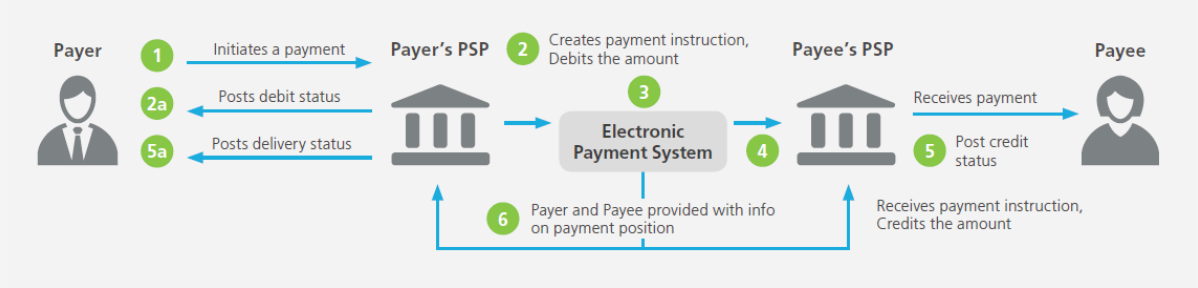

Figure 19: Payments Status and Tracking End-to-End Journey

#	Step Name	Description
1	Initiates payment	Payer initiates a payment by providing PSP with payment details and instructions.
2	Creates payment instruction. Debits the amount	Payer's PSP creates payment instruction and initiates it. The payer is provided with information on the debit status of the payment (2a).
3	Payment Initiation	Payment passed on to the payment systems.
4	PSP receives payment instructions	Payee's PSP receives payment instruction and credits payment to payee's account.
5	Credit Status provided	Information on credit status provided to the payee. The payer is provided with information on the payment being credited to the payee (5a).
6	Payment status provided	Throughout the journey, the payer and payee are provided with information on the payment's position.

Table 18: Payments Status Tracking End-to-End Journey

4.6 Assumptions

#	Title	Description
001	Governance	It is mandatory that PSPs respond to Confirmation of Payee queries.
002	Functional	The CoP service is offered 24x7 to all the customers.
003	Functional	The CoP service is payment scheme/method agnostic.
003	Functional	The Confirmation of Payee service will be used only with an intention to make a payment.
004	Functional	The CoP response is as accurate as the data gathered during the KYC process.
005	Functional	The CoP service does not validate data gathered or replace the KYC process.
006	Regulatory/ Governance	Safeguards will be required for all the actors of the CoP service.
007	Governance	A commercial pricing (billing) model will be required for the CoP service.
008	Functional	The CoP service will work on the New Payments Architecture.

Table 19: Assurance Data Assumptions

4.7 Key Risks and Considerations for Assurance Data

While developing the requirements and rules for Assurance Data, we identified key risks and considerations that must be made. For each of these risks, we have identified mitigations. The identified risks are summarised in Table 20.

ID	Risk	Description	Mitigation
001	Phishing and fraud	There is a risk that end-users details obtained through CoP are used in a fraudulent manner.	Service providers must ensure that the design of the service minimises the possibility of fraud and phishing.
002	Data privacy, protection and ownership	As CoP could require sharing sensitive information and data between end-users, there is the risk of data protection being breached harming end-users.	Service providers must be registered and accredited. Governance should be in place that requires all CoP service providers to demonstrate a minimum standard of information security.
003	Proceeds of Crime Act and ‘Tipping off’ clause	Proceeds of Crime Act 2002 make it an offence for any PSP to 'tip-off' (i.e. inform) a payer if they are under investigation for any offences covered by this act. This is a risk in the provision of information on a payment’s status and tracking. PSPs must comply with this regulation	Service providers must ensure that the design is compliant with this regulation.

ID	Risk	Description	Mitigation
		whilst they provide Payment status and tracking capability to payers.	
004	Non-participation	We have provided the ability to opt out of the CoP service where mitigating circumstances exist. This presents the risk, however, that fraudsters may opt-out from the service in order to disguise their identity.	Service providers of CoP must have in place strict criteria and rules under which a user can opt-out of the service.
005	Service failure	There is a risk that Confirmation of Payee service could be temporarily unavailable due to a payer's PSP, payee's PSP or underlying systems (including potentially CASS) being unavailable.	All CoP service providers should have service failure backup plans.

Table 20: Assurance Data Potential Risks

In addition, the following must be considered:

1. **The accuracy of data utilised:** Assurance Data is dependent on the accuracy of the underlying data. In particular:

    - CoP utilises the information held by the payee's PSP to determine whether the account belongs to the payee. This information is gathered as part of the KYC process carried out by the PSP. It is imperative that the KYC process is adequate and the information is kept up-to-date and accurate.
    - Payment Status and Tracking is dependent on the NPA providing the right messages in a timely manner to the payer and payee PSPs. In turn, the PSPs need to present this information to the payer and payee in a manner that clearly communicates the status of the payment.
2. **Periodic re-confirmation of payee:** Payers should periodically reconfirm payees they may have confirmed previously and saved in their payee lists. This guards against instances where the payee has transferred the account or where the saved account number has been reassigned to a new payee.[36]

3. **End-user interface design and experience:** CoP and Payment Status Tracking service providers will be tasked with determining the best way to present the various functionality and capability to the end-user. In doing so, consideration must be made to ensure that these interfaces allow the end-user to interact with and utilise the services in the most effective manner.

4. **End-user awareness and education:** To aid the successful adoption, payers will need to be made aware of the existence of the CoP and Payments Status Tracking services as well as education on how best to safely engage.

5. **Alignment with industry initiatives and upcoming regulations:** Access and operation of the CoP and Payments Status Tracking services will be compliant with the secure customer authentication and communications requirements of PSD2 and the regulatory requirements of GDPR and 4MLD and other regulations as appropriate. This includes alignment with any liability models developed for the operation of PSD2.

[36] PSPs may choose to recycle account numbers once a payee closes an account. We have only identified two PSPs who recycle accounts.

6. **Name convention for CoP:** The format in which names are captured and returned for CoP is important. A lack of a standard would present interoperability challenges. An example of a convention would be: A name is composed of a first name and last name.

7. **Cost of CoP:** CoP users should not be charged for using the service.

8. **CoP sign-up:** Payers will not be required to sign up for the CoP service. Assuming their bank offers the service, they will have the option to utilise CoP by default. However, a payer does not have to conduct a CoP check to make a payment. They could ignore and proceed to make a payment without performing the check in line with the principle that the payer is always in control.

9. **The position of CoP along payments journey:** CoP can be performed for every payment transaction or once when setting up a payee. We leave the positioning of CoP along the customer journey at the discretion of the PSPs

10. **CoP channels:** Confirmation of Payee can be offered on all channels apart from paper-based payment instructions such as a cheque.
    a. CoP channels can include internet, phone call, text message, etc.
    b. Banks are not compelled to offer CoP on all channels. This is a competitive decision. The decision on what channels to offer the service may be influenced by the need to balance the PSP's liability responsibilities resulting from the 'Contingent reimbursement model' for push payments proposed by the PSR (currently under consultation) and their TCF responsibilities.

11. **Use of CoP data:** It is important that CoP data is only used for purposes of CoP only and not for other uses for example marketing, credit references etc.

4.7.1 Data Protection Impact Assessment

Privacy and Data Protection legislation and in particular the introduction of the General Data Protection Regulation (GDPR) in May 2018, are critical elements that will shape overlay services such as Confirmation of Payee. The document in Appendix 6 is the Data Protection Impact Assessment (DPIA) assessing the data protection consideration surrounding the implementation of this Service and identifying corresponding mitigating measures. As part of this process, the assessment has:

- Considered the benefits that Confirmation of Payee could deliver to data subjects;
- Identified what personal data is required to deliver these benefits, now and in the future;
- Considered the potential data protection risks and issues; and
- Identified safeguards to mitigate these data protection concerns.

To operate successfully, Confirmation of Payee (the "Service", "CoP") will involve the collection and processing of personal data including of name, account number and sort code. In addition, there is a possibility that personal data captured by Confirmation of Payee will be disclosed to third parties or organisations who have not previously had routine access to such information. The Service would introduce a new capability – beneficiary identification – to enable the person entering the payment details to verify that the bank details they have provided belong to the person or organisation they wish to pay before the payment is processed.

To minimise security and adverse data protection impact, the information of the payee provided in the beneficiary identification process (e.g. sort codes, account numbers) would be expected to be kept to a minimum and their access restricted.

Personal data will be processed on the basis of legitimate interest under GDPR. While the volume of personal data and data subjects in scope is not pre-determined, Confirmation of Payee will be offered to the UK market.

I. Summary of Risks Considerations and Mitigations

While developing Confirmation of Payee, potential data protection risks and related mitigating safeguarding measures have been considered. The key findings are as follows:

Key Risks	Proposed Mitigations
Data Security and Service Failure There is a risk of technical failure of the Service or the exposure to external cyber threats or personal data being inadvertently shared with a third party outside the permissions given. This will result in personal data breaches	Personal Data should be encrypted while in transit to mitigate the risk raised by security breaches. Governance requirements from the NPSO is expected to be in place to ensure Confirmation of Payee service providers demonstrate a minimum standard of information security for the Service (e.g. service failure back-up plan).
Service Fraud and Phishing There is a risk that personal data is misused by spammers, fraudsters (incl. phishing) or other malicious actors wrongfully accessing the Service resulting in harm to individuals.	Service providers will be required to register/be accredited with the NPSO to ensure the service is trustworthy and reduce the risk of fraudulent use. The CoP service will only be utilised for the purposes of making a payment. Service providers will be expected to ensure the design of the service minimises the exposure to phishing, fraud etc. CoP queries from customers will be recorded to identify cases of misuse and provide an audit trail.

Table 21: Summary of CoP Data Risks, Considerations and Mitigations

CoP service providers will be tasked with determining the various functionality and capability of the Service to the end-user including establishing enhanced mechanisms for data protection.

Confirmation of Payee will be supported by a service provider and the NPSO as governing body. The NPSO will provide a thin layer of governance on which service providers will be expected to build technical provisions and additional functionalities. These will ensure the objectives of the Service and compliance with the GDPR accountability and privacy by designs requirements are met. The NPSO will also be responsible for registration and certification of Confirmation of Payee service providers.

II. Consultation Process and Next Steps

Development of the NPA requirements and rules was achieved collaboratively through public consultations, workshops and interviews with various representatives of the main end-user groups: governments, charities, consumer groups, retailers, housing associations, Payment Service Providers (PSPs), and NPSOs. This has enabled the PSF to achieve an industry-wide position on data protection implications that affect each of the solutions. In addition, planned consultation with the Data Protection Supervisory Authority may result in conducting further work yet to be defined. The output of these will be incorporated in the Data Protection Impact Assessment.

4.8 Dependencies

To successfully deliver an Assurance Data solution as described, several dependencies need to be considered. These are:

#	Title	Description
001	Regulatory	CoP service design approach is dependent on the data protection rules set by the GDPR.
002	Regulatory	The legislation changes may be needed to CoP service. The specifics of this are yet to be determined.
003	Industry participation	The ubiquity of the CoP service is dependent on the majority of the industry participation including PSPs and consumers.

Table 22: Assurance Data Dependencies

5 Enhanced Data

In the Strategy, we identified several detriments relating to data affecting end-users:

- Lack of sufficient data
- Lack of structure in the existing data
- Lack of a common standard format

For example, Bacs is limited to 18 characters of reference information which is freeform in nature, whilst Faster Payments is limited to 140 characters. Consequently, end-users are forced to send the payment instruction and associated remittance information separately (for example by post or email). Ideally, with sufficient capacity and structure, the two would be sent and processed together.

Sufficient capacity and structure of data will allow straight-through processing of payments and eliminate the need to carry out manual reconciliation. We, therefore, recommended the delivery of an Enhanced Data capability as one of the three EUN Solutions.

An electronic payment is broadly composed of two parts; a payment instruction and remittance information. The payment instruction initiates transfer of money between the payer and payee. The remittance information provides context on the underlying commercial transaction. Enhanced Data 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[37] and standard.

Reconciliation is required to link a payment transaction to its reference information. Reconciliation occurs at two levels:

- Reconciling the payment instruction to the remittance information
- Reconciling the remittance information to the associated transaction

The associations between the monetary payment and the underlying transaction can vary in complexity from relatively straightforward (for example, a single payment for a single unique transaction) to very complex (for example, multiple payments relating to a chain of multiple transactions). In an ideal situation, the payment system has sufficient capacity to allow the payment instruction and sufficient remittance information to travel together,[38] a unique linkage exists between the payment instruction and remittance advice, and the remittance information is structured such that is it easy to identify the underlying transaction.

ISO 20022 and Open Banking APIs

Payments systems are a complex combination of PSPs, payments service operators and end-users (individual consumers, businesses and government) all acting in concert to allow transmission of a payment from a payer to a payee. To enable ubiquity of the solution a standard is required across the various parties that specifies the input, format, carriage, access to enhanced data.

ISO 20022 is an ISO standard for electronic data exchange between financial organisations. It provides an open framework offering a common vocabulary and set of message definitions. Open Banking enables end-users to share their bank data securely with other banks and with third parties. The Open Banking Initiative in the UK is defining and developing the required APIs, security and messaging standards that underpin Open Banking.

The NPA will utilise ISO 20022 as the common messaging standard and, by extension, Enhanced Data will utilise this as the common message standard. To facilitate a common standard for input and access across the industry we recommend the use of the Open Banking APIs.

[37] Structured data is data that is highly organised, and strictly defined in its form and nature. Structured data has the advantage of being easier to enter, store, query and analyse using a computer.

[38] The payment instruction and all the remittance information do not strictly have to travel together. An alternative interpretation of this can be the use of a link that travels with the payment instruction and links to the complete reference information which is carried out of band.

5.1 Detriments Addressed by Enhanced Data

Enhanced Data aims to solve the following detriments:

ID	Detriment Group	Detriment
7	Customer Assurance: Additional functionality for both payer and payee	Payers and payees require additional functionality in order to be able to include additional reference data in the payment (to ease reconciliation).
8	Customer Assurance: Additional functionality for both payer and payee	Payers and payees require additional functionality in order to be able to include additional data for third parties (e.g. accounting; taxation and age verification).
22	Corporate Customers	Reconciliation costs and treasury management for businesses; also government reporting costs.
23	Corporate Customers	The distance between physical and financial supply chain affects e-invoicing.
34	Data sharing, reference data, and analytics	Insufficient reference data and a lack of knowledge sharing amongst users resulting in gaps in preventing financial crime; fraud, money laundering, terrorist financing, bribery and corruption.

Table 23: Enhanced Data Detriments

5.2 Scope

5.2.1 In Scope

ID	Detriment Group	Detriment
1	All electronic payments excluding Card Initiated payments	Any payment that is electronic in nature. For payments that are not entirely electronic throughout their lifecycle, only the electronic phases will be in scope.

Table 24: Enhanced Data In-Scope

5.2.2 Out of Scope

ID	Detriment Group	Detriment
1	Data not relevant to the payment	Data that is not relevant to the payment is out of scope.
2	Cash (physical notes and coins) transactions that are entirely external to the electronic payment systems	Cash payments that do not Ingress or Egress into the electronic payment systems during their life cycle.
3	Card payments	Card transactions exist on a parallel infrastructure operated by the card issuers, external of the main payment infrastructure. The Forum considers these out of the scope of its work.

Table 25: Enhanced Data Out of Scope

5.3 High-Level Use Cases

The high-level functional overview of Enhanced Data use cases from the payer's and payee's view are depicted in Use Case Diagrams Figures 20 and 21. They are classified into use cases identified as minimum 'core proposition' for customers to ensure consistent experience and 'competitive' use cases that are open for innovation to offer more value to the users and promote healthy competition in the market. The Forum will not be defining requirements and rules for the competitive cases.

Use cases are represented as UML diagrams accompanied by Tables 26 and 27 providing a short description for each use case.

5.3.1 Payer Use Cases Overview

The following diagram represents the case where the payer uses enhanced data for reconciliation purposes of both himself and the payee.

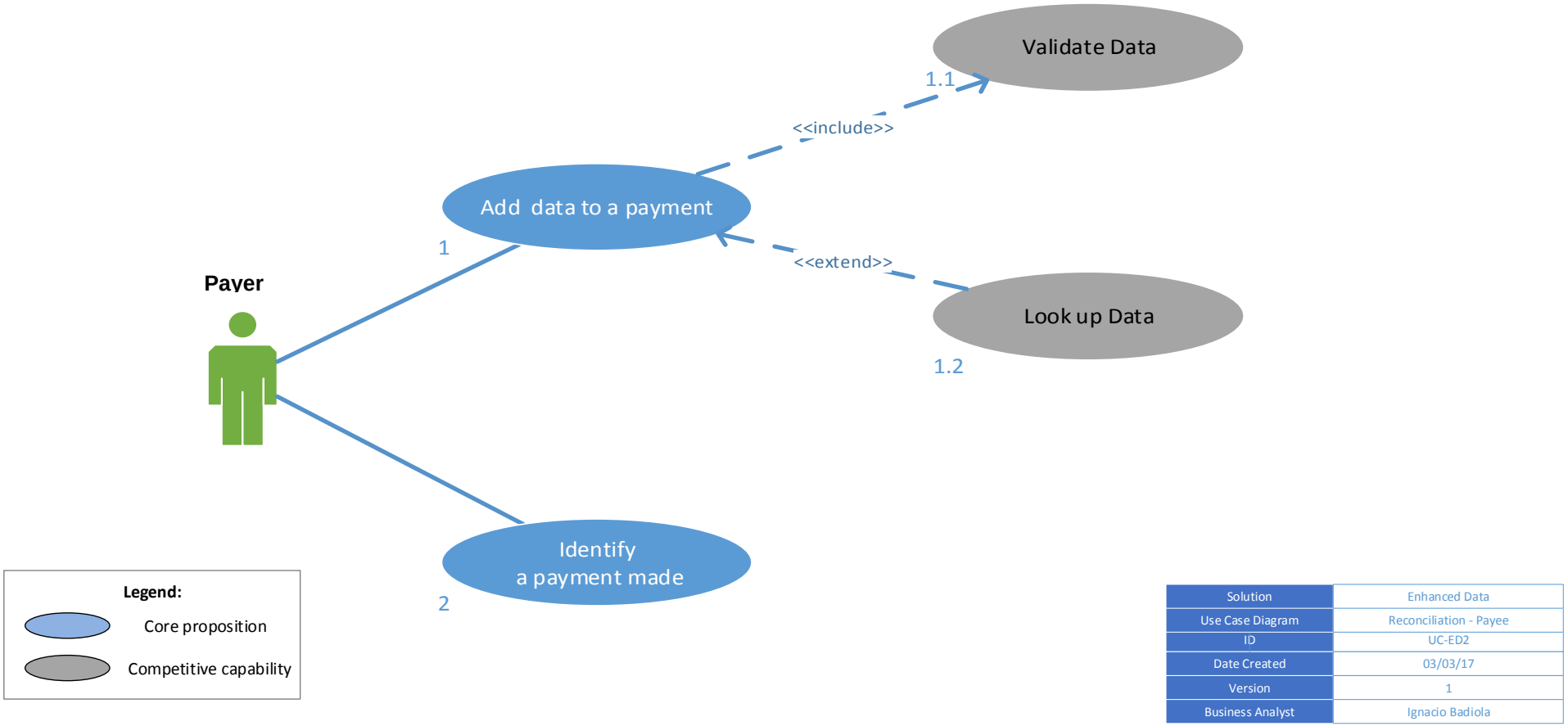

Figure 20: Enhanced Data Payer Use Case

5.3.2 Payee Use Cases Overview

The following diagram represents the case where the payee makes use of the enhanced data in a received payment for reconciliation purposes.

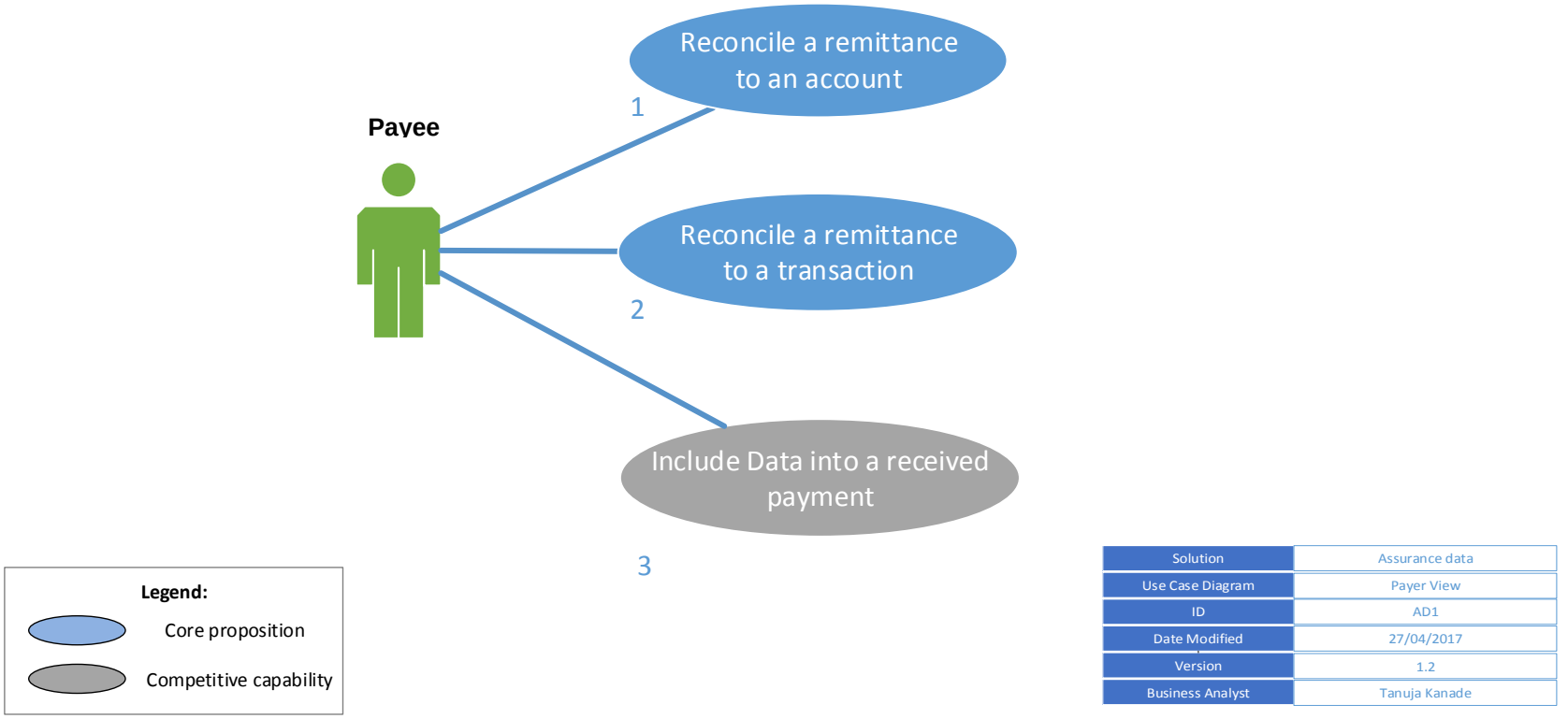

Figure 21: Enhanced Data Payee Use Case

ID	Use Case	Description
1	Add data to a payment	The payer is able to add information to a payment.
2	Identify a payment made	A payer requires additional data in payments to be able to recognise and identify a payment made. This data needs to be visible and accessible by the payer. Also, it needs to travel with the payment throughout its whole journey and keep its integrity so that the same data that was added by a payer is received by the payee.

Table 26: Enhanced Data Payer Use Cases

ID	Use Case	Description
1	Reconcile a remittance to an account	When a payee receives a payment, the payee should be able to receive along with the remittance some information/data which provides necessary details of the payment to reconcile it against the appropriate customer's account. For example, the payment carries with it a reference number which allows the payee to identify to which customer's account/bill a payment received relates.
2	Reconcile a remittance to a transaction	When a payee receives a payment, the payee must be able to receive along with the remittance some information/data which provides necessary details to be able to trace back the remittance to the correct transaction. For example, when the payee receives a payment and wants to know to what exact payment transaction the remittance belongs.

Table 27: Enhanced Data Payee Use Cases

5.4 High-Level User Stories and Rules

The primary end-users of Enhanced Data will be the payer and the payee. However, with the rollout of PSD2 and the Open Banking initiative, we foresee the rise of a third end-user type in the form of Account Information Service Providers (AISPs).
The Enhanced Data requirements of each end-user are dependent on the role they are playing:

a. Making a payment: A payer making a payment could add Enhanced Data to the payment.
b. Receiving a payment: A payee receiving a payment will utilise the Enhanced Data when provided by a payer to identify a payment received.
c. Accessing payment information: Payers, payees and AISPs will access the information for other purposes other than making or receiving a payment, subject to appropriate permissions for processing data.

In the Strategy, we focussed on the most pressing need that Enhanced Data will address; helping end-users, typically a business or a third party such as government department, to auto-reconcile a payment to their internal systems accurately and efficiently. We are however conscious that this is not the only use case for Enhanced Data. In our work with the various end-users, we have identified numerous additional use cases, e.g. business intelligence through data analytics and processing, customer marketing and loyalty programs, machine learning and fraud detection.
With this in mind, we have specified a core set of requirements that address the key detriments highlighted in the original Strategy. At the same time, they will provide a broad framework that allows extension of the solution to cover the breadth of potential use cases.

The minimum requirements are shown in the following sub-section.

5.4.1 Payee User Stories and Rules

1. Reconcile a remittance to a payer

	As a payee, I want to be able to:
Reconcile a remittance to an account	1. Receive sufficient data with the payment so that I can identify the payment and reconcile it to the correct customer account. 2. Receive the data in a form I can consume so that I can process it and reconcile the payment with the correct customer account.
Rules	1. Payee must receive all data exactly as included by payer.

2. Reconcile a remittance to a transaction

	As a payee, I want to be able to:
Reconcile a remittance to a transaction	1. Receive sufficient data with the payment so that I can identify the payment and reconcile it to the correct transaction with which it is associated. 2. View the data received alongside a payment so that I can reconcile the payment with the correct transaction.
Rules	1. Payee must receive all data exactly as included by payer.

5.4.2 Payer User Stories and Rules

1. Add additional data to a payment

	As a payer, I want to be able to:
Input data into a payment	1. Add additional data to a payment so that the payment carries more contextual information. 2. Add the additional data in a form that is structured and standard so that any other involved parties (e.g. payee) are able to read it.
Rules	1. Where applicable, all additional data[39] must be formatted suitably, compliant with NPA message standards at either end. 2. The payer must be able to see the details of their payment regardless of whether the payment has actually been settled[40]. 3. All legal and regulatory requirements must be complied with at all times by all data processors and data stores[41].

[39] Any data added to a payment's message. E.g. Link, photograph, PDF, message, etc.

[40] In cases of failed payments or non-instant payments (Bacs) the payer must be able to always access the payments Enhanced Data.

[41] The Data Protection Act 1998, GDPR Data Storage Regulations, the Privacy and Electronic Communications Regulations

2. Identify a payment made

	As a payer, I want to be able to:
Identify a payment made	1. Access a description of the payment so that I can identify what, why and to whom the payment was made. 2. Determine any information included in a payment such as a bill, a receipt, invoice, warranty or other so that I can identify the reason of the payment.
Rules	1. Where applicable, all additional data must be formatted suitably, compliant with NPA message standards at either end. 2. The payer must be able to see the detail of their payment and the data attached independent of whether the payment has actually been settled. 3. All additional data included in payments must be accessible through any channel through which I am able to see the payment. This may not be possible through analogue channels.

5.5 Proposed End-to-End Journey

The end to end journey for Enhanced Data lifecycle will be broadly similar regardless of the types of actors involved. For example, a peer-to-peer payment, between individuals, will typically follow the same flow as a business-to-consumer journey.

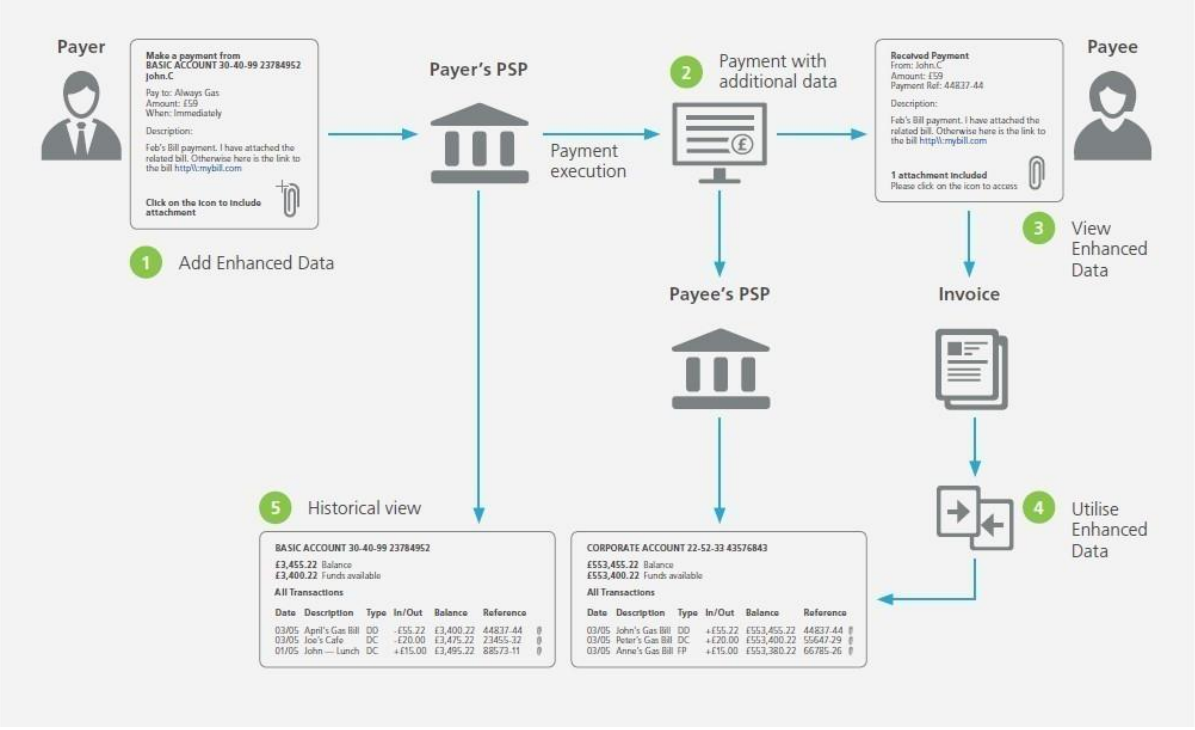

Figure 22: Enhanced Data End-to-End Journey

#	Step Name	Description
1	Add Enhanced Data	The payer adds Enhanced Data to a payment. E.g. gas bill or hyperlink.
2	Payment with additional data	Payment travels to the payee's PSP with Enhanced Data included by the payer.
3	View Enhanced Data	The payee accesses the Enhanced Data provided through APIs or PSP interfaces.
4	Utilise Enhanced Data	Payee utilises Enhanced Data to reconcile the payment to the customer's account.
5	Historical View	Both payer and payee are able to access Enhanced Data added to historic payments made or received through APIs or PSP interfaces.

Table 28: Enhanced Data End-to-End Journey

5.6 Assumptions

#	Title	Description
001	Technical	The NPA will adopt ISO 20022 as its messaging standard including for Enhanced Data.

Table 29: Enhanced Data Assumptions

5.7 Key Risks and Considerations for Enhanced Data

While developing the requirements and rules for Enhanced Data, we identified key risks and considerations that must be made. For each of these risks, we have identified mitigations. The identified risks are summarised in Table 30.

ID	Risk	Description	Mitigation
001	Data privacy	There is a risk of a data privacy breach or data inadvertently being shared with a third party outside the permissions given. This would breach existing data protection regulations.	Data carriers must comply with all data privacy existing and upcoming regulations, including but not limited to AML4 and GDPR.
002	Data ownership	There is a risk of data being misused or mishandled if no data ownership and responsibility is well defined throughout the whole journey.	Data carriers must comply with all data ownership existing and upcoming regulations, including but not limited to AML4 and GDPR.
003	Data structure	There is the risk that if the data structure is not met the receiver of the data will not be able to access it or the data itself might be altered or corrupted.	Data carriers must comply with all existing and upcoming data structure regulations, including but not limited to PSD2 regulations and AML4. It's important to be aware that existing regulations might not completely cover data structure risk mitigation in its entirety.

ID	Risk	Description	Mitigation
004	Data storage	There is a risk that storing data for a short period of time might impact regulatory bodies needing to audit participant's data. Also, storing data for too long can be detrimental to both the provider and for customers.	Data carriers must comply with all existing and upcoming data storage regulations, including but not limited to AML4 and GDPR. It's important to be aware that existing regulations might not completely cover data storage risk mitigation in its entirety.

Table 30: Enhanced Data Potential Risks

To successfully deliver on the Enhanced Data solution as described, several considerations need to be made. These are:

1. **Technical, operational or system failure:** Providers will guard against or mitigate for harm due to:
    a. A system, data management or process failure which impedes the capture, movement or access to Enhanced Data.
    b. Data passed being insufficiently clear, complete or standardised in structure or size for the purpose it is being used for.

    The risks described above could originate from different parties within the Enhanced Data end-to-end journey, including any parallel system holding data, and could encompass the ability to link data with payments.

    Alignment with industry initiatives and upcoming regulations: Access and operation of Enhanced Data will be compliant with the secure customer authentication and communications requirements of PSD2 and the regulatory requirements of GDPR and 4MLD and other regulations as appropriate. This includes alignment with any liability models developed for the operation of PSD2 and requirements from Fraud and Financial Crime to carry certain payments details in the actual payment message (as opposed to in the Enhanced Data) – i.e. Name, Address or beneficiary and remitter, to comply with AML regulations and also to allow payer and payee to know who they're paying and who they are receiving a payment from.

5.8 Dependencies

To successfully deliver an Enhanced Data solution as described, a dependency needs to be considered. This is:

#	Title	Description
001	Implementation	For the delivery of Enhanced Data in the NPA, it will need to adopt the ISO 20022 messaging standard. This will inherently provide the capability to carry more data as well as the framework to ensure data added is structured.

Table 31: Enhanced Data Dependencies

6 Critical Success Factors and Go-to-Market Strategy

A key risk identified with the three End User Needs solutions was a lack of adoption. Instances of this can be seen elsewhere in the market, where comparable solutions have been launched, but due to a lack of a critical mass, they have not been able to achieve ubiquity. Examples include Paym, Monzo.me at Monzo and Receive on Pingit. The reasons for lack of adoption range from a lack of common standards and interoperability to inconsistent branding. As such, if solutions do not get adopted the associated benefits cannot be realised - be it individual consumer benefits or a reduction in financial crime within the industry. Understanding the risks of adoption by differing groups within the payments ecosystem such as PSPs, individuals and businesses is crucial in mitigating these risks and to consequently promote solution ubiquity.

Against this backdrop, the Go-to-Market strategy framework was created with the intention of assessing what the key components of a successful strategy would entail and how this would lead to the high adoption of the solutions. The framework sought to combine all of the various segments that are key in achieving high adoption ranging from technical infrastructure to branding and awareness as well as adoption approaches which are laid out in detail in the subsequent sections.

Lastly, in addition to establishing the framework, it is also important to ascertain what a good/successful rollout would, in fact, look like in relation to each solution. The final section intends to review this and the metrics used to measure this.

It should also be noted that in developing the strategy and adoption approaches, the focus was given to Request to Pay and Confirmation of Payee since they are the most distinct of the EUN solutions. Enhanced data and Payment Status Tracking are to be built into the NPA infrastructure as intrinsic features of the infrastructure, hence are not subject to the same adoption pressures as Request to Pay and Confirmation of Payee.

6.1 Go-to-Market Framework

The framework below contains the components of a successful Go-to-Market strategy with high adoption as the subsequent end goal. The framework is split into two main parts: ‘Enablers’ and ‘Drivers’. The ‘Enablers’ component, provides the basis to which the EUNs can function and be interoperable which is then further split into two main sub-categories of technical infrastructure and governance. The ‘Drivers’ refer to the aspects of the solution that attract end-users to adopt the solution offering. These include the presence of end-user advantage as set out in end-user proposition, awareness and access to the solutions to the target groups. This section will focus in on the key aspects of these two main elements.

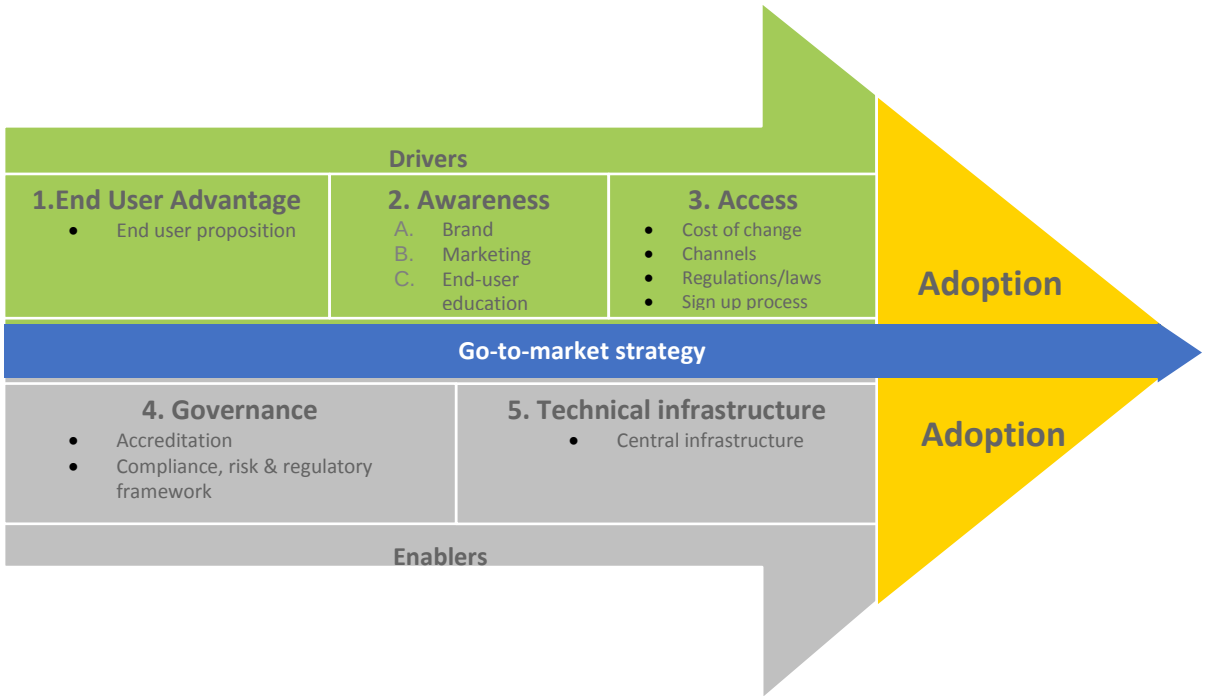

Figure 23: Go-to-Market Framework

6.1.1 Drivers

The following section will focus in on the main aspects of the 'Drivers' element of the framework. These are split into three main areas: End-user advantage, Awareness and Access.

I. End User Advantage

The presence and clear articulation of benefits to end users from using the EUNs solutions is a key factor in enticing end users to adopt these solutions. The End-user Proposition sets out this advantage for each solution. This includes firstly identifying the target end-users of each solution, their needs (which are the customer detriments initially outlined by the PSR), the advantages of adoption to the end-user and the relative competitive advantage - which relates to solution-wide features that if utilised can ensure wide adoption and ensure the needs of the identified end-users are met.

End-user Proposition

	End-user identification	End-user needs	End-user advantage
Request to Pay	• Individuals and SME's with variable incomes/cash-flows • Users who are excluded from current payment systems or financial products	• Greater control • Options available to those suffering from financial exclusion • Choice and competition	• Request to Pay aims to provide Control, Flexibility, and Transparency. This is through the introduction of a messaging system as part of the payment process allowing improved communication between payee and payer on the specifics of the payment, ability of the payer to control how much, how and when they want to make the payment.

	End-user identification	End-user needs	End-user advantage
Assurance Data	• End-users making push- • payments	• Knowledge that sufficient funds are available to make a payment • Assurance that payers are making the payment to the intended payee's account Status of the payment once t the payment is made	• Assurance data aims to provide payers and payees with adequate information throughout the payment lifecycle to assure them that they have sufficient funds to make the payment; are making the payment to the right payee as well as visibility in the position of the payment in its journey to the payee
Enhanced Data	• Individual and corporate end-users requiring more data to be included alongside a payment message	• Individual end-user needs include: provision of additional and sufficient supporting data when making and receiving payments • Corporate or government billers needs include; using data to enable a better payments reconciliation process	• The Enhanced Data solution proposes an increase in the amount of data that can be added to a payment in a standard structure that is uniform across the payment industry. This has benefits including; enhanced payments reconciliation, especially for businesses. In addition, the ability to carry more data will spur new opportunities in areas such as data analytics and data intelligence that are currently inhibited by the limited nature of current systems

Table 32: End-User Proposition

II. Awareness

A key driver of adoption is awareness of the solutions by the target end-user groups. Differing target groups will have different educational and marketing requirements and thus the channels by which this is communicated will be different. Consequently, the responsibility for the promotion of the solutions to each target group will potentially fall to different actors within the payments ecosystem. The table below illustrates a proposed structure outlining what the marketing and awareness aims and objectives should entail.

Target end-user groups	Awareness and marketing objective	Marketing channel	Potential Responsibility
SME's	Education of the EUNs solution service offerings and their relative advantage specifically in relation to SME's. For instance, the additional information provided in Enhanced Data can aid in the payment reconciliation process. Additionally, Request to Pay can enable flexibility and control which can assist in cash flow management.	Marketing campaigns	PSPs Service providers

Target end-user groups	Awareness and marketing objective	Marketing channel	Potential Responsibility
Financially excluded	Specific education on EUN solution advantages in relation to greater flexibility and control achieved when making payments.	Variation in marketing channels. Examples include: Advertisements Corporate websites	NPSO Government Corporates
Digitally-enabled end-users	To spread awareness of Request to Pay and how it fits into the digitally-enabled user's lifestyle enabling them to leverage existing technology which they currently use. For example, making peer-to-peer payments more effectively via their smartphones.	Social-media	PSPs Service providers

Table 33: Awareness and Marketing Objectives

Brand Elements

The brand of any individual product or service offering is made up of various elements. These are presented below alongside the various considerations and recommendations that need to be taken into account.

Element	Consideration	Recommendation
Brand Name	• The name should be memorable and easy to recognise • Ideally, it should also hint at what the solution does • Should not be easily confused with another product/solution	• We recommend keeping the existing solution names (i.e. Request to Pay, Confirmation of Payee and Payment Status Tracking). This is on account of the solution names having already been socialised extensively through the PSF strategy and blueprint
Logos, Symbols and Slogans	• The NPSO will need to design and define associated logos, symbols and slogans including specifics such as their colour, typeface, positioning and usage	• We believe the NPSO is better placed to design and define the logos, symbols and slogans
Visual design	• This encompasses the design of the customer-facing components of the solutions e.g. customer interfaces, button shapes, colours etc.	• We recommend that the NPSO allows providers to determine the most suitable design for their customer's interfaces. This should not prejudice specific brand constraints such as standard logos and brand name

Element	Consideration	Recommendation
Minimum Customer proposition	• The minimum requirements and rules as defined by the PSF constitute part of the base brand of the solution • The solutions feature various terminologies that are specific to them e.g. payment extension, Confirmation of Payee, payment period	• As a minimum, every implementation of the EUN solution should possess the minimum functionality as defined by the PSF • We recommend that terminology as defined is standardised
Terms and Conditions	• In some cases, terms and conditions specific to the solutions will be required	• We recommend that the NPSO provides guidance terms and conditions that providers of the EUN solutions can appropriate into their product T&C's as appropriate
Customer Communication	• Standardised customer communication mediums including letter templates, application forms etc. • Notifications	• We recommend that each service provider is allowed to draft their own customer communications • Service providers are free to determine the nature of and trigger for notifications with the exception of notifications mandated in the rules

Table 34: Brand Elements

Brand Ownership and Control

Achieving a favourable balance of control and ownership of brand elements between service providers and the NPSO is vital to ensure the individual solutions have a clear recognisable brand and customer proposition, whilst at the same time allowing for competition and variety to be offered among providers to enable favourable end-user outcomes. The framework below intends to illustrate the key advantages and disadvantages of a low, medium and high brand control and ownership between the NPSO and service providers. Overall we recommend that the NPSO adopts a Medium level of ownership and control over the EUN solutions' brands.

Service Providers / NPSO	Low	Medium	High
Description	• Service providers own and control all aspects of the brand • In a competitive regime, each solution offering would have a completely different brand from the other	• Solution providers own certain aspects of the brand, with the rest owned by the NPSO • Across the various solutions, certain aspects of the brand would be common	• NPSO owns and controls all aspects of the brand • All solutions would have a uniform brand. In a competitive regime, it would be very difficult to differentiate one provider from the other
Pros	• Each service provider is free to define their solutions brand and is subject to competitive forces	• Adequate level of brand ownership and control by the NPSO resulting in reduced brand fragmentation and reduced customer confusion • A minimum standard is assured for end-users while leaving room for various providers compete and differentiate themselves	• NPSO owns and control all aspects often brand and can tailor it to suit the end-user
Cons	• Likelihood of fragmented brands for the same solution, which is likely to result in consumer confusion • Lack of a minimum reference experience for customers resulting in an overall dilution of the solution offering	• Increased effort is required from the NPSO	• Different providers have minimal room to differentiate themselves resulting in minimal to no competitive advantage • Huge overhead on the NPSO and the service providers to comply with the brand requirements

Figure 24: Levels of Brand Ownership and Control

III. Access

Access refers to the relative difficulty end users face when seeking to adopt EUNs solutions. A high number of barriers to entry can severely block the adoption process, due to this, the following framework aims to outline the various barriers that exist and the corresponding considerations and recommendations needed to offset them.

Barrier	Considerations	Recommendation
Opportunity cost of change	• The cost of implementing and running the solutions has a direct impact on the ability of end-users to adopt the solutions. This is especially true for small businesses and consumers • The cost of carrying out the required technical and operational changes, as well as the cost of running the solutions	• Technical solutions need to be simple, with minimal expertise needed to implement them • Effort should be made to minimise operating costs • Reuse of common standards such as ISO20022 should be maximised
Multi-channels	• Different segments of the market may prefer to use different channels to access the EUN solutions. Diversity in the channels available to end-users can lower barriers to access	• In line with the requirements and rules defined, the providers of the solutions should provide various channels for end users to access. Both digital and analogue
Sign up Process and onboarding	• An extensive and complex signup process can inhibit the adoption process both service providers as well as end-users • Sign up processes include user registration and service provider accreditation	• Sign up process should be as simple as possible • A balance should be struck between meeting the objectives of the signup processes and their potential to be a barrier to entry • The proposed accreditation process for each of the 3 EUN solutions is detailed in the accreditation section
Regulation/Laws	• The legal and regulatory environment, through the existence or lack of, appropriate laws may impact the adoption of EUN solutions	• Changing regulation is the preserve of legislative authorities. • Should a need arise, appropriate negotiations should be initiated with the relevant bodies

Table 35: Barriers to Entry and Related Recommendations

6.1.2 Enablers

This section will seek to highlight the key 'Enablers' of the adoption which are categorized into governance and technical standards. The first category of governance seeks to outline the compliance, risk and regulatory framework governing the EUNs solutions as well as the accreditation of the solutions and the process by which this is done. The technical infrastructure aspect illustrates the system architecture of the solutions.

I. Governance

Governance relates to the mechanism by which common standards, accreditation and compliance are enforced within the NPSO. A balance is needed between enforcing the necessary governance and control systems whilst also fostering high competition and innovation.

Compliance, Risk and Regulatory framework

The solutions must be compliant with all existing and future applicable regulations including, but not limited to, AML4, GDPR and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). There are several entities who are responsible for governance, including but not limited to, regulation, authorisation, registration and accreditation of the participants including the following:

1. Payment Systems Regulator (PSR) is an economic regulator for the payment system. It has the role of promoting competition and innovation in payment systems and ensuring that they work in the interests of payment service users.

2. The Bank of England (BoE) provides the Real-time Gross Settlement System (RTGS) service used for settlement in central bank money and is the prudential supervisor of some types of PSPs as well as payment systems, with an objective of protecting and enhancing financial stability.

3. The Financial Conduct Authority (FCA) regulates the financial services industry in the UK. Within the context of the NPA and its participants, the FCA will be responsible for authorising and registering applicable PSPs and TPSPs.

4. The New Payment System Operator (NPSO) will be the key vehicle for the delivery and governance of the NPA. It will be responsible for the procurement and contract management of the NPA. It will also run some NPA components, in particular, those related to clearing and settlement, and the required integration with the Bank of England RTGS. It will be the central body that governs the NPA, including the setting of standards and rules, such as for overlay services and for technical considerations such as security. In addition, the NPSO will be responsible for the accreditation and certification of certain participants, for example, Request to Pay, Confirmation of Payee and Enhanced Data service providers.

Accreditation

In order to ensure the integrity of the solutions, key standards and requirements of solutions will need to be meet in order for providers of the services to operate. Accreditation provides the means by which key players in Request to Pay or Confirmation of Payee service provision can be approved to operate.

What is accredited?	Service providers will need to meet a minimum standard in the provision of the EUN services. This includes: a) Technical requirements relating to: • APIs • Common messaging standards • Security and fraud companies' measures b) Functional requirements and associated rules: • Functional requirements as defined for each solution • Associated rules c) Branding: • The NPSO will own and control certain aspects of the brand. Compliance with this will be part of the accreditation d) Other requirements: • In some cases, service providers will also have to meet other requirements that may have an indirect bearing on the provision of the EUN solutions such as Registration as a TPP by the FCA, Technical capability, security certificates and more.

What body is accrediting?	• NPSO is the primary accrediting body. They will own the requirements, rules and standards as well as carry out the accreditation process Secondary accrediting bodies: • To be accredited, there may be a requirement that you are also accredited/registered/authorized by another body such as the FCA. The entity will compliment NPSO.
Who is being accredited?	The parties subject to accreditation will be the service providers.

Table 36: Accreditation

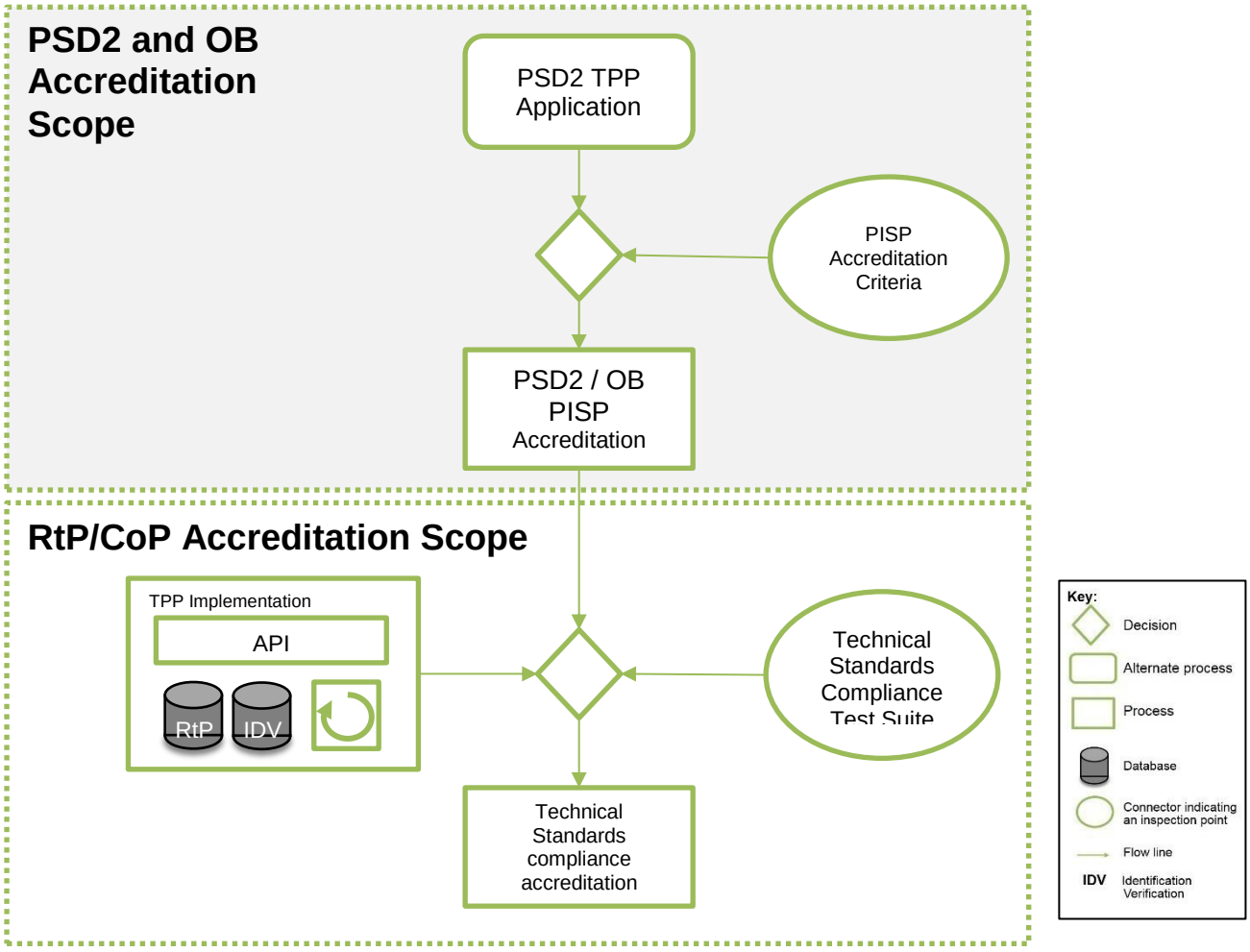

Figure 25: Request to Pay Accreditation Framework

II. Technical Infrastructure

The Request to Pay technical infrastructure is laid out in depth in the "Request to Pay Technical Solution Blueprint"[42]. Please see section 6 'Functional description' from page 15 onwards.

For more information on the infrastructure for CoP specifically and the API infrastructure then please see **Error! Reference source not found.** in section 4.5.1

[42] "Request to Pay Technical Solution Blueprint" is a companion document published alongside this document.

6.2 Adoption

As outlined above, the purpose of the Go-to-Market Strategy is to factor in key features that lead to high adoption as the projected outcome. When assessing this, it is important to define what adoption is, including the theoretical underpinnings. This section also suggests favoured approaches to adoption, based on analysis and key considerations of current adoption trends within the payments industry.

I. Adoption theory

Adoption is a measure of the number of end-users (or equivalent proxy) using a particular solution at a particular time. The rate and extent to which a solution is adopted is dependent on the on potential end-users becoming aware of the solution and thereafter adopting it.

In an ideal case, a plot of the number of adopters of a new technology or idea over time assumes a sigmoid shape driven by the technology/idea being initially adopted by a small number of vanguards and slowly to the masses and lastly to the remaining holdouts. As more and more end-users adopt a technology, its market share among potential end-users increases and eventually reaches saturation and ubiquity.

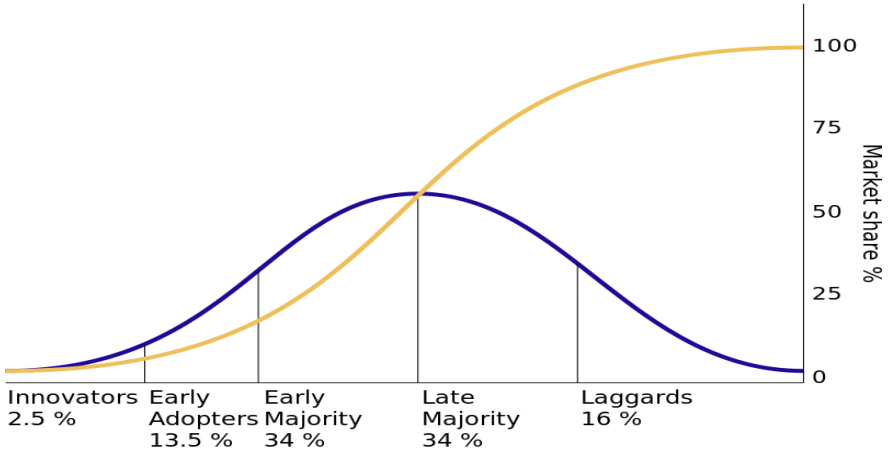

Figure 26: Illustration of an Ideal Plot of Number of Adopters of a Technology over Time[43]

What is the expected adoption rate for the EUN solutions?
The NPA cost-benefit analysis provides an indicative adoption rate for the EUN solutions. This is conservative view based on previous payment solutions of a similar nature such as Paym, CASS and real-time payments.

The table below shows the level of adoption assumptions for the 3 solutions by the end-users. The percentages show estimates of the proportion of the large and medium scale business population (on a per transaction basis) that adopt the solutions over time.

Services	Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9
Request to Pay	3.1%	3.8%	4.6%	5.6%	6.8%	8.3%	10.1%	12.3%	15.0%
Assurance Data	3.1%	3.8%	4.6%	5.6%	6.8%	8.3%	10.1%	12.3%	15.0%
Enhanced Data	5.0%	6.1%	7.4%	9.0%	11.0%	13.4%	16.3%	19.9%	24.2%

Table 37: Level of Adoption Assumptions by End-Users for EUN solutions

[43] Rogers Everett - Based on Rogers, E. (1962) Diffusion of innovations. Free Press, London, NY, USA.

II. Adoption approaches for Request to Pay and Confirmation of Payee

Confirmation of Payee

A unified rollout approach of the CoP service, across the industry, is required to achieve ubiquity. After examining the cases of Paym, Contactless Payments and CASS, common themes were found which would contribute to the successful roll-out of CoP:

1. **Promotion and adoption of the new service roll-out needs to be done synchronously by all payment market participants**
2. **Commitment and collaboration among industry participants is vital**
3. **Recourse to further action is needed if there are limited adoption and promotion**

Account providing PSPs represent the single and most important channel for carrying CoP from development, through adoption and promotion to end-users. In this single channel model of delivery several considerations should be made:

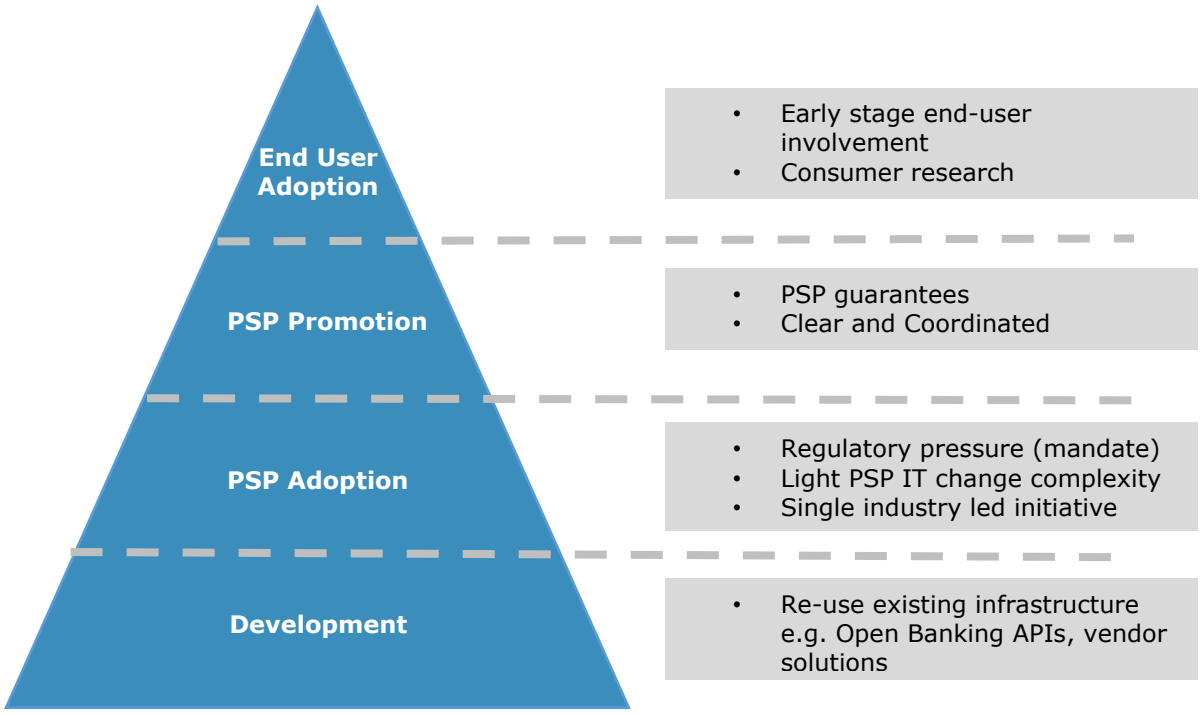

Figure 27: Adoption Diagram

Request to Pay

The successful rollout of Request to Pay is dependent on concurrent adoption by both the payer and payee. Unlike CoP, for Request to Pay PSPs and market participants are mutually dependent upon each for the success of the solution. The solution cannot be scaled to a critical mass without the adoption and promotion by both.

In this case, several challenges are apparent that require consideration:

1. **Lack of a business case:** There is the risk that market participants, who are driven by competitive pressures amongst market participants, may not adopt solutions if there is no feasible business case. In order to address these challenges, pressure from PSPs can be used to drive adoption and promotion, whilst sound business cases can be presented to market participants to compel participation.

2. **Mutual dependency:** PSPs and market participants moreover, face a related challenge of mutual dependency between PSPs and market participants. This presents a demand and supply side risk in that both are relying upon the other to adopt and promote the offering, which may obstruct adoption. Collaborative promotion agreements could be used to mitigate this.

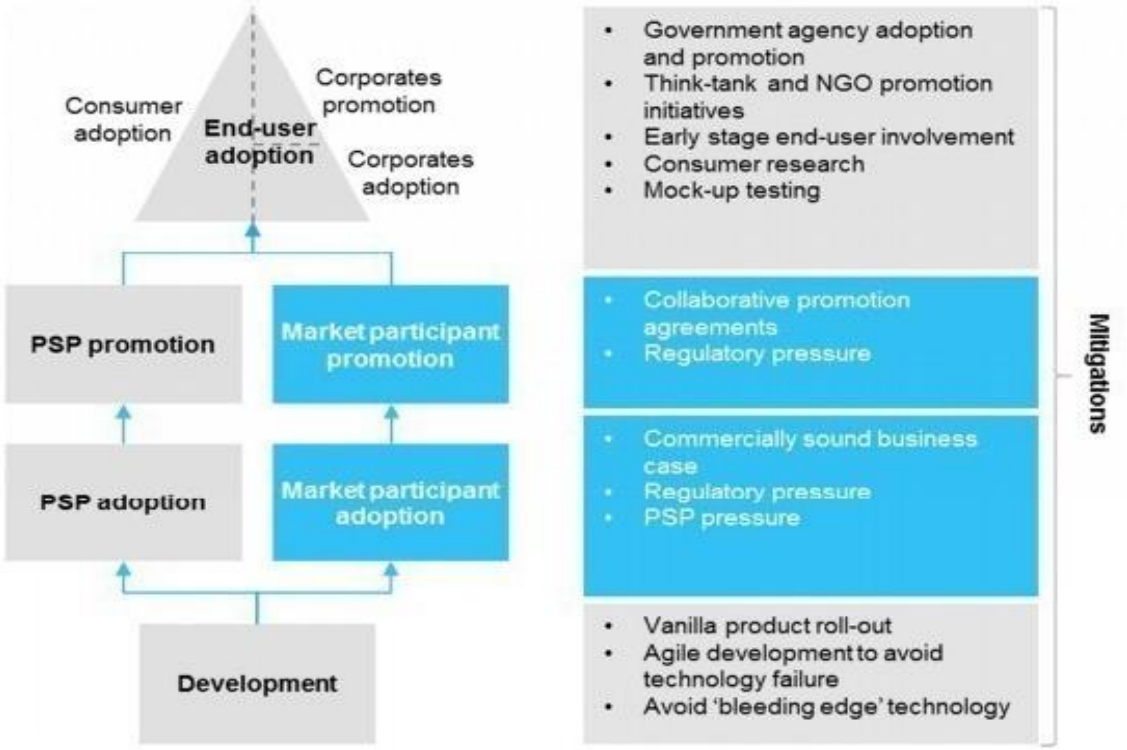

Figure 28: Coordinated Adoption Approach Diagram

III. EUNs Solutions Competition characteristics

All the EUNs solutions will generally be provided through competition in the market. As a result, it is important that the NPSO puts in place the necessary frameworks and engages the market early on to ensure that it encourages widespread adoption.

There are components of each of the EUN solutions that are however exempt from this. These are defined below by solution.

Request to Pay

Within the Request to Pay infrastructure, the User Frontends and Repositories will be provided in the competitive market the only centralised infrastructure will be the Index which exists for the market. This seeks to promote innovation and greater end-user choice in the market. Figure 29 below shows the elements included in the infrastructure of the Request to Pay service.

In regard to the provision of the Request to Pay service, end-users will not be mandated to use or provide the service.

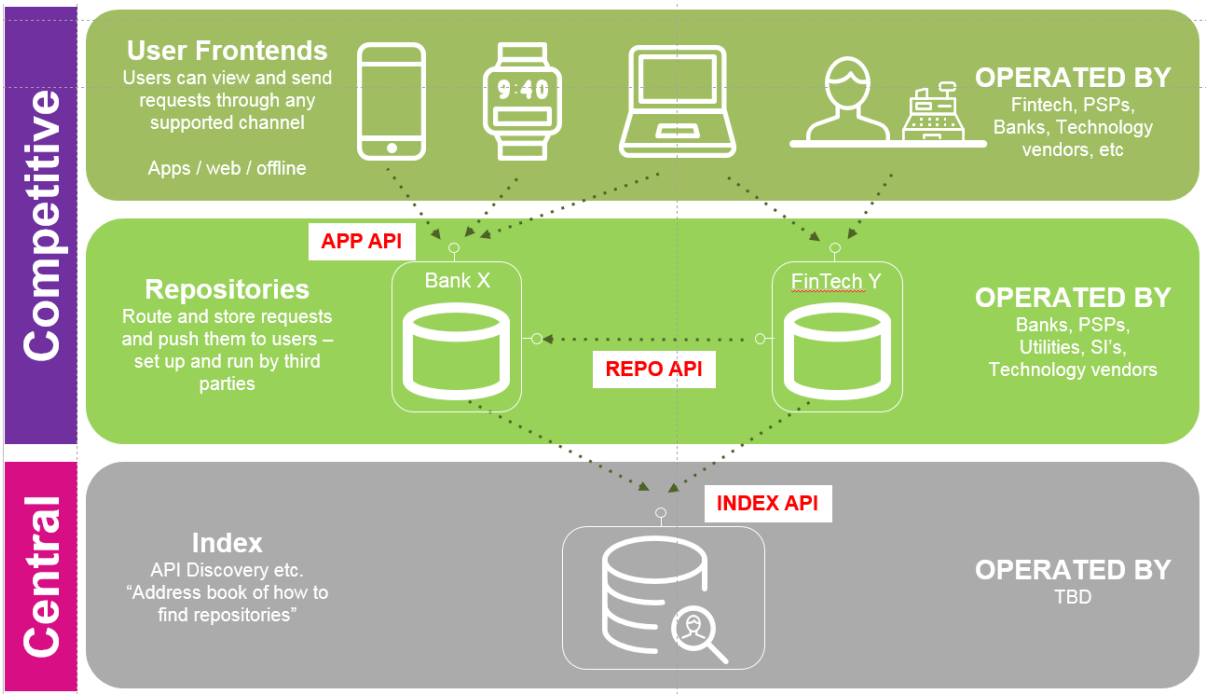

Figure 29: Competitive view of Request to Pay service provision

Confirmation of Payee

The Confirmation of Payee solution exists within the competitive space entirely. For a Payer's PSP to offer Confirmation of Payee it is imperative that the payee's PSP responds to their request for confirmation. We recommend that all ASPSPs should, as a pre-requisite to participating in push payments respond to requests for Confirmation of Payee. The NPSO should encourage ASPSPs, in addition to responding to requests, to offer CoP to payers before making push payments through a coordinated initiative across the industry.

Overall, driving adoption and achieving greater assurance in the payments industry is dependent on end-users having access to Confirmation of Payee and their relevant PSP's offering the service. The PSR has the powers and could mandate Confirmation of Payee should it deem it appropriate and necessary.

6.3 EUN Success Criteria

To assess whether the adoption has been successful it is first important to understand what is defined as success and what the Key Performance Indicators (KPIs) would be in measuring this for both the Request to Pay and Confirmation of Payee solutions. This section is segmented based on different aspects of what success means for both solutions.

I. Request to Pay success criteria

	Critical Success Factor	KPI
Adoption	• High adoption among payers and payees • High usage by service providers	• Number of payers, payees and service providers
Social & economic impact	• Societal economic benefit achieved from the use of Request to Pay which reduces the poverty premium associated with payments • Reduced debt due to increased flexibility and control introduced by Request to Pay • Economic benefit to the UK economy due to reduced debt, lower costs etc. • Increased financial inclusion due to Request to Pay • Increased control and flexibility for all end-users	• A qualitative study to assess the impacts of Request to Pay at a personal level • % reduction in debt directly attributable to Request to Pay • % reduction in cost of processing payments
Awareness	• High awareness among end-users, PSPs and other market participants on what Request to Pay is, its functionality, the channels it's offered through and its associated benefits	• Surveying a population sample size to see the proportion of respondents who have heard of Request to Pay • Mapping the awareness to different end-user categories to identify to what extent our target groups are being made aware
Service performance	• High availability and resilience of service	• Service uptime
Confidence, trust & security	• Knowledge of how to engage safely • Confidence among payees and payers that requests and associated messages and payments will be actioned • Minimal Fraud	• Low % of fraudulent and spam requests and a 100% effective remediation process of those that are fraudulent • Measurement of complaints, errors and disputes as % of total requests • End-user survey to gauge confidence and trust

Table 38: Request to Pay Critical Success Factors

II. Confirmation of Payee success criteria

	Critical Success Factor	KPI
Adoption	• Adoption among all PSP's for qualifying accounts by a particular date • All new PSPs to offer CoP from day one	• No. of account servicing PSPs able to respond to a CoP request • No. of PSPs offering CoP as part of a payment or the number of payee set-up within CoP services • Minimising the no. of accounts excluded from CoP [44]
Confidence, trust & market integrity	• Increase end-user assurance due to use of CoP • Minimal misdirected payments • Data protection of customer personal information during electronic payments	• No. of payments either due to fraud or operator error • Surveys to identify levels of end-user trust and confidence in CoP • Measurement of no. of data breaches
Service performance	The CoP service must be available: • to all payers making an applicable payment • At the point of making the payment, independent of the payment channel e.g. mobile, online, telephone etc. • Real-time and Available 24/7	• Tracking of service performance across different payment systems and channels • Tracking performance of real-time service functionality and availability

Table 39: Confirmation of Payee Critical Success Factors

[44] However, in some instances this may be permitted i.e. individuals needing to withhold their identity due to security reasons. Although this should be minimised as much as possible.

7 Appendices

7.1 Appendix 1 – Data Protection Impact Assessment: Request to Pay

SECTION I - INTRODUCTION

Request to Pay is a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment. The product may require individuals to provide personal data about themselves including first name, surname, email/phone number and date of birth. The processing of this information presents some privacy concerns, hence the need for this DPIA. In addition, there is a possibility that information about individuals captured by Request to Pay will be disclosed to third party or organisations who have not previously had routine access to the information.

SECTION II - PRELIMINARY SCREENING QUESTIONS

These questions are intended to help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

1. **Does Request to Pay involve processing of personal data about individuals?**
   a. **Yes - proceed to the next question.**
   b. **No - no Privacy Impact Assessment required.**

Yes. Request to Pay involves the collection and processing of personal data about individuals registered to the service.

2. **Describe the nature of the personal data to be processed?**

Request to Pay will require individuals to provide personal data about themselves through the interface of the service including: their first name, surname, date of birth, email/phone number and possibly address, account number and sort code. This information is expected to be collected at the registration stage, and used for the purposes of making requests for payments and receiving payments associated with a Request to Pay.

3. **Does the personal data processed include new information not previously held about the individual?**

Yes. The Request to Pay service provider ("the provider") will be registering new users of Request to Pay. As a consequence, it will be collecting and processing new personal data about such individuals.

4. **Indicate the Purposes for which the personal data will be processed. Is the personal data intended to be processed for a new purpose? If so, specify.**

Request to Pay is a new overlay service developed as part of the End User services accompanying the New Payments Architecture (NPA) proposed in our Strategy and Consultation, to be offered by Payment Services Providers ("PSP") and third parties. The service is a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment. Through Request to Pay, a payee will be able to notify a payer of a payment that requires their attention and in return, the payer will be able to respond to the payee.

5. **Will the processing involve sharing of personal data with entities which previously did not have access to the personal data? If yes, please provide details.**

Possibly. The provider will be collecting personal data about individuals upon registering

through the Request to Pay interface. They may, however choose to outsource the identity verification activities to an external third party and share personal data about their Request to Pay users to such third party as part of the KYC process.

6. **Will new technology/organisational solutions be used to process the personal data? If yes, please provide details.**

Yes, Request to Pay is a new End User Needs Solution which architecture consists of a layered model.

7. **Will the processing involve sensitive personal data, personal data concerning vulnerable individuals or information particularly likely to raise a privacy concern?**

Request to Pay will not be accessible to individuals categorised as vulnerable under the GDPR or other equivalent data privacy regulations. The personal data processed under Request to Pay will be limited to the information listed in Question 2 and is not expected to include any sensitive personal data.

SECTION III - IMPACT ASSESSMENT

Scope of the DPIA

1. **What objective is the processing expecting to achieve?**

Request to Pay is a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment.

Through Request to Pay, a payee will be able to notify a payer of a payment that requires their attention and in return, the payer will be able to respond to the payee. For example, the payer will be able to accept the request and make full or partial payments; decline it; request an extension of the time period in which they can make the payment; or request more information. When a payer accepts the request, they will be able to pay using a choice of available methods, and the acceptance will automatically trigger the payment being made.

End-users (individuals, SMEs, corporates and government) could benefit from Request to Pay. Payees will be provided with an additional communication mechanism to improve visibility on what the payer's intention is with regards to a bill payment.

Currently, once a payee sends out a bill, they have limited visibility on whether the payer will make a payment or not and when they will pay. Increased visibility has a positive impact on cash flow management, payment reconciliation, debt management and overall customer relationship management. Cash flow management is especially important to SMEs who tend to have limited cash reserves making them vulnerable to cash flow challenges.

Request to Pay provides visibility to the payer on outgoing payments; it opens a communication channel to the payee; and it provides a tool through which a payer can flex how they make their payments - when, how, and how much. This helps users manage their financial position more effectively.

We provide further information on Request to Pay in the July 2017 Consultation and WS1 supporting document.
Blueprint for the future of UK Payments

Information Flows Description

2. Describe the collection and use of personal data throughout the Request to Pay process.

The information flows are summarised in the table and diagram below:

	Step Description	What Data?	Data Type	Parties Involved	Ownership	Processing	Storage	Controller	Processor
1	**Registration for TPP's**	• Organisation name • Organisation registration number • Organisation address • Telephone • Technical contact • Organisation admin contact	Non-personal	• TPP • NPSO	TPP	Submission & verification by NPSO	NPSO storage	NPSO	NPSO
1	**Registration for End-users**	Can include: • Title • First Name, Middle, Surname • Date of birth • Address • Post code • Account number • Sort code • Email • Mobile number	Personal	• Payee • Payer • PSP/TPP • NPSO	Payee or payer (depending on who is registering)	Submission & verification (App provider does basic verification checks e.g. correct number of characters etc., whereas repository provider does verification)	Index - User ID Repository - rest of data	NPSO	Repository
2	**Create RtP**	• Name • Email • Mobile Number • User ID • Payment period • Payment description • Payment Amount • Payment options • Reference ID (Generated at either creation or sending phase) **Optional attachment file**	Name – personal Other data - non-personal Dependent on what is in optional attachment	• Payee • Repository	• Payee • Payer owning name	N/A	Local front end medium e.g. Local storage App/cloud or paper	Request to Pay provider	Local front end medium e.g. Local storage App/cloud or paper
3	**Send Request**	• Name • Email • Mobile No • User ID • Payment period • Payment description • Payment Amount • Payment options • Reference ID (Generated at either creation or sending phase **Optional attachment file**	Name - personal Other data - non-personal	• Payee • Payee's repository	• Payee • Payer owning name	Transmission of the request from the payee's repository to the payer's repository. Front end update for both payer and payee	Payee's repository	Request to Pay provider	Messaging processor (infrastructure, specifically repositories)
4	**Request Received**	• Name/ • Email/ • Mobile No/ • User ID • Payment period • Payment description • Payment Amount • Payment options • Reference ID (Generated at either creation or sending phase **Optional attachment file**	Name - personal Other data - non-personal	• Payer • Payer's repository	• Payee • Payer owning name	To be determined by front end e.g. batch payments for large billers, pre-processing depending on contracts	Payer's repository, front end medium e.g. Local storage App/cloud or paper	Request to Pay provider	Front end interface

5	**Create Response, Send Response (options below)**	• Response: Pay all, Partial pay, Decline, Block, Extension or Contact • Response to period & amount • Choice of payment preference e.g. cash, card	Non-personal	Payer's PSP	Payer		• Payer's repository • Payee • PSP	Payer's PSP	
5.1	**Pay all/partial payment -- second loop**	• Payment method • Payment details - depends on method e.g. bank account, card, PayPal	Personal	• Payer • Payer's PSP	Payer	Request to pay interface contacts bank's back office, which processes the payment. When confirmed, the status of the payment is updated in both payer and payee's repository. Payer and payee's front end is then updated.	• Payee's and payer's repository • Payer's and payee's PSP • Front end	• Request to Pay provider • Payer's PSP	• Payer's front end • Payer's PSP • Payer's repository • Payee's repository • Payee's app/front end
5.2	**Extension request**	• Date • Reason - optional	Non-personal	• Payer • Payer's and payee's Repository	Payer	Request to pay interface updates the payer's repository. When confirmed, the status of the payment is updated in both payer and payee's repository. Payer and payee's front end is then updated.	• Payer's and payee's Repository • Front end	Request to Pay provider	• Front end • Repositories
5.3	**Contact (chat message or email address or call up depends on app and channel)**	Data (e.g. email, phone number) or attachment	Dependent on type of data attached	• Payer • Payee	Payer or payee depending on front end and payee requirement	Message transmission - Interaction at the front end level	Front end	Request to Pay provider	Front end
5.4	**Block**	Blocked User IDs	Non-personal	Payer	Payer	Repository will check user IDs and if they are in the blocked list, for that specific user, then they will not be delivered	Payer's repository	Request to Pay provider	• Repository` • Block set up via front end
5.5	**Decline**	Decline or optional message and data/attachment	Dependent on type of data attached	• Payer • Payer's and payee's Repository	Payer or payee depending on attachment	Transmission of the request from the payer's repository to the payee's repository. Front end update for both payer and payee	• Payer's and payee's Repository • Front end	Request to Pay provider	• Front end • Repositories

Table 40: Request to Pay Detailed Information Flows

The information flows are summarised in the diagram below:

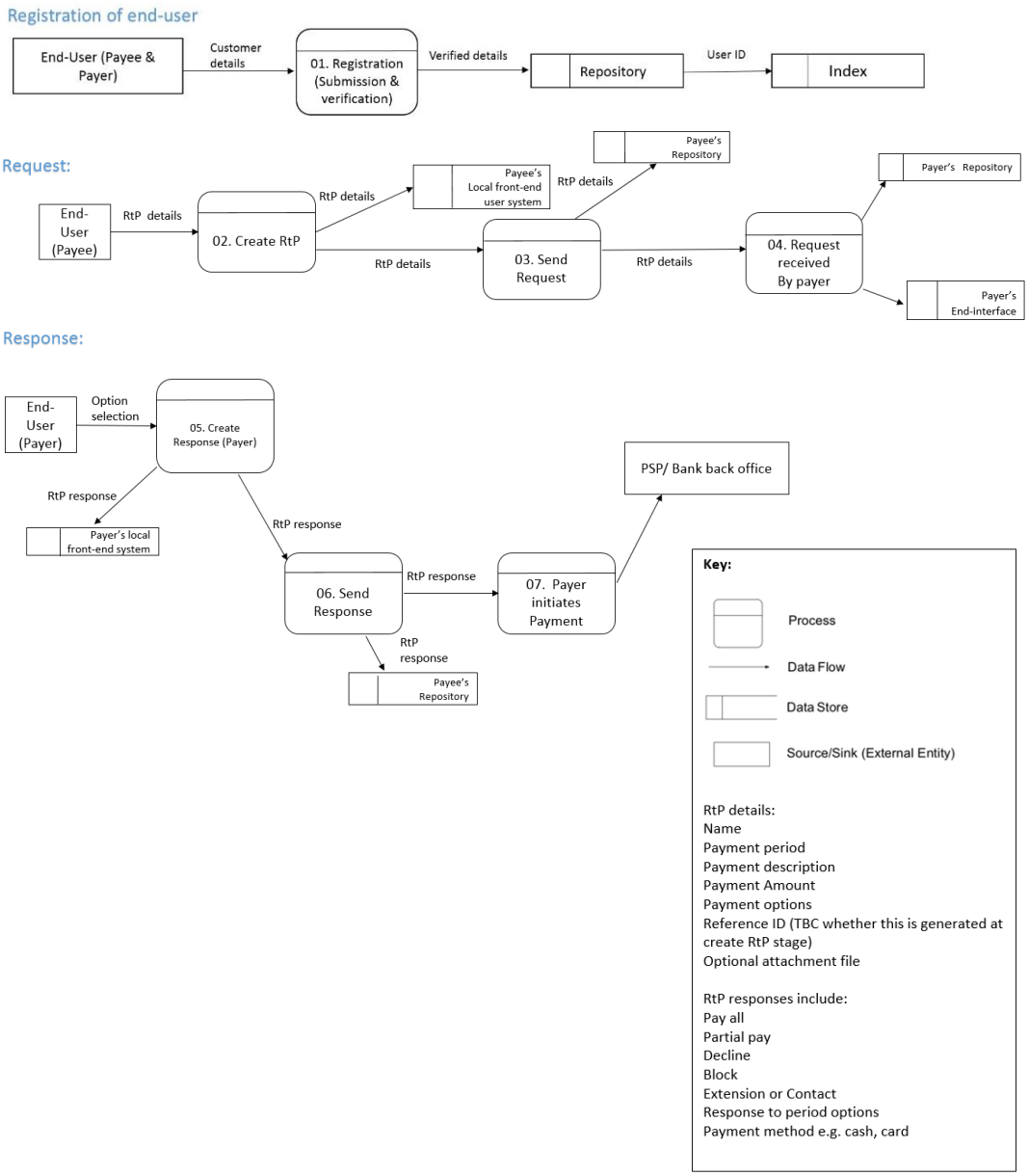

Figure 30: Request to Pay Information Flows

Privacy Risk Evaluation

3. What is the volume of data to be processed and the number of individuals concerned?

The volume of personal data and data subject is not pre-determined. Request to Pay will be offered to the public across the UK payments market.

4. Does the processing involve the transfer of personal data to countries or territories outside the European Union? If so, specify

The intended scope of Request to Pay is limited to payments occurring within the UK.

5. What is the expected duration of the processing?

The processing will be dependent on the usage of the service by the providers and is not subject to a prescribed duration.

6. Will the processing involve profiling or systematic monitoring? If yes, please provide details.

No. These activities are not expected to be within the scope of the service.

7. Will the processing involve matching or combining personal data? If yes, please provide details.

No. These activities are not expected to be within the scope of the service.

8. Have you identified other sources of risk to individuals' privacy?

Data Protection Issue	Risk to individuals	Compliance risk	Risk to Associated organisation / corporate
Data Security breaches during storage of personal data or transit and service failure	There is a risk of technical failure of the service, exposure to external cyber threats or personal data being inadvertently shared with a third party outside the permissions given. This will result in personal data breaches exposing the individuals to fraudulent actions	Risk of non-compliance with GDPR	Request to Pay service providers, PSPs or third parties, may be exposed to reputational damages, fines, penalties and loss of their customers' patronage.
Service abuse and fraud	There is a risk that spammers, fraudsters or other malicious actors wrongfully access the service resulting in misuse of personal data and harm to individuals (i.e. identity theft, fraud).	Risk of non-compliance with GDPR	Request to Pay service providers, PSPs or third parties, may be exposed to reputational damages, fines, penalties and loss of their customers' patronage

Table 41: Request to Pay Data Protection Issues

Proposed Risk Mitigations

9. Please provide a description of the measures envisaged to address the privacy risks identified.

Risk Title	Mitigation(s) Description	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project (Yes/No)?
Service abuse and fraud	Providers of the Request to Pay service should be registered / accredited to ensure that the service is trustworthy and reduce the risk of fraudulent use. Implementation of the Confirmation of Payee service	The risk is reduced	Yes
Data security breaches and service failure	Personal Data should be encrypted while in transit to mitigate the risk raised by security breaches. Governance requirements from the NPSO is expected to be in place to ensure Request to Pay service providers establish a minimum standard of information security for the Request to Pay components (e.g. service failure back-up plan).	The risk is reduced	Yes

Table 42: Request to Pay Risk Mitigations

10. Has the lawful basis of processing been established? If yes, please specify.

Personal data will be processed on the basis of consent.

11. Describe how information about the processing will be provided to individuals. Do you need to amend your privacy notices?

The Request to Pay service provider will ensure that its Terms and Conditions include the information about the processing prescribed by the GDPR.

12. If consent is the lawful basis of processing, how and when will the consent of individuals be obtained and recorded? Will measures be established to address withdrawal of such consent?

Consent will be obtained at the registration stage through the user consenting to the terms and conditions of the Request to Pay provider. Appropriate measures will be established by the providers to receive and address any withdrawal of such consent by the data subject.

13. If relying on consent or necessity for contract as a lawful justification, has a data portability solution been designed?

Request to Pay is currently expected to meet the requirements of Data Portability under GDPR.

14. Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act?

No. Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society". Request to Pay will not compromise the users' right to privacy and respect for family life.

15. Have you identified the social need and aims of Request to Pay? Are your actions a proportionate response to these needs?

Yes. There was an acknowledgement that a growing number of end-users' needs are not fully met by the current payment systems. A predominant theme include the need for end-users to have:

- More control over their payments.
- More flexibility over how much, when, and how they pay.
- Increased transparency in their interactions with payments.

In response, Request to Pay intends to meet these needs by providing a messaging service that encourages financial inclusion, transparency and control.

16. Does your Request to Pay plan cover all of the purposes for processing personal data?

Yes. The data map provides a detailed illustration of the data journey and processing of the collected personal data (See Section B, Question 2).

17. Have you identified potential new purposes as the scope of Request to Pay expands?

At this stage of the project, the primary purpose of Request to Pay has been set and confirmed under the agreed solution. This does not prevent other providers from expanding the scope of the service in the future.

18. Is all the personal data necessary and relevant to achieve the objectives of the processing?

Yes, the personal data in scope is necessary and relevant to ensure Request to Pay achieves its objectives of allowing payees to notify the appropriate payers of a payment request.

19. Could the objective of the processing be achieved without the use of data identifying individuals (e.g. by using anonymised data)?

For Request to Pay to perform as intended, individuals will be expected to consent to the provision of personal data allowing their identification.

20. How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Personal data will be provided by individuals. Personal data will subsequently be verified by the provider as part of its KYC process or through the identity verification performed by a third party vendor.

21. If you are procuring new systems do they allow you to amend personal data when necessary?

Yes. All individuals will be offered the option to amend their personal data when necessary through the user application interface of the Request to Pay provider.

22. What is the envisaged retention period for the personal data? What safeguards will be put in place to ensure the secure deletion/destruction of the personal data within the prescribed retention period?

The personal data is intended to be retained for as long as the service is used by the individuals (i.e. payer/payee) subject to the retention procedures of the related regulatory requirements.

23. What measures are envisaged to comply with the rights of individuals to access, rectification, erasure, objection to and restriction of processing?

The provider or third parties will be responsible for establishing measures ensuring these rights are respected.

24. Would Request to Pay providers use the personal data available for marketing purposes?

Possibly. Users of Request to Pay may be subject to marketing such as advertising under the application interface of the Request to Pay provider.

25. What would be the potential impact on individuals in case of illegitimate access, undesired modification and disappearance of personal data?

Individuals may be exposed to negative or unwanted effects which may cause financial loss and moral damage (for example identity theft and fraud) See Section C, Question 8 for further information).

26. Do any new systems provide protection against the security risks identified?

Yes. Both providers and third parties will be required to demonstrate a minimum standard of information security. This will be overseen by the New Payment System Operator. The participants will be expected to take measures to maintain the integrity of the processed personal data and minimise the possibility of fraud or phishing.

27. What training and instructions are proposed to ensure that staff know how to operate Request to Pay securely?

This is to be determined at a later stage by the Request to Pay service providers.

28. If personal data transfers in countries or territories outside of the European Union are envisaged, how will you ensure that the personal data is adequately protected?

N/A as no transfers outside the EU are planned at the moment.

SECTION IV - GOVERNANCE & VALIDATION

29. Have a consultation with representatives of individuals whose personal data will be processed been conducted? If yes, please provide details. If no, please Explain why not. Who else will be consulted internally and externally as part of this process? How will you carry out the consultation?

The development of the service was achieved collaboratively through numerous workshops and interviews with a range of stakeholders including various representatives of the main end-user groups: government, charities, consumer groups, retailers, housing associations, PSPs, and Payment System Operators (PSOs). In addition, we incorporated further research by various organisations already working on these solutions both within and outside the UK.

In July 2017, we published a Consultation Paper opened to comments from the public including representatives of Data Subjects. Responses were received by key associations and taken into consideration as part of the further development of the Solution.

The ICO will be consulted as part of this Data Protection Impact Assessment process.

7.2 Appendix 2 – Request to Pay FAQ

1. What is Request to Pay?

Request to Pay is a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment and in turn the payer can respond to the payee . The service provides the end-user payment options that include: Pay all, Pay Partial, Decline and Request for extension where payment is to be made available through a range of channels e.g. paper, telephone and via apps. All of which seek to give greater transparency, flexibility and control to the end-user.

2. Does Request to Pay replace Direct Debit?

No, Request to Pay is not intended to be a replacement for Direct Debit. Request to Pay is a messaging service completely distinct from the underlying payment mechanism. For many organisations and individuals Direct Debit fulfils their needs, however, for others this is not the most suitable form of payment. For instance, users or SME's with irregular cash inflows who need more control and flexibility of when and how they pay. This category of persons and businesses would benefit from the flexibility, control and transparency accorded by Request to Pay.

3. How does Request to Pay provide flexibility?

Request to Pay provides flexibility by allowing end-users to decide how much (through the pay all or pay partial options); when (through the ability to pay now or request a payment extension) and how they pay (provided through the payer's ability to choose a suitable payment mechanism).

4. What if my business model does not support offering all the Request to Pay options?

The full range of options should be supported by all Request to Pay providers as defined in the common standard. However, it is appreciated that not all payees are able to offer all of the options as dictated by their business model. The common standard provides leeway for payees in such cases to determine which Request to pay options to offer to the payer. If a payee is unable to offer a particular option they should notify the end-user appropriately.

5. As a payer, when can I block a payee from sending me Request to Pay?

The payer can block a payment which they believe to be fraudulent; likely to pose a security risk or erroneous.

6. I don't have access to electronic mediums, can I use Request to Pay through analogue channels?

Yes, Request to Pay can be offered through various channels and mediums. This includes mobiles apps, web channels, paper, telephone and physical premises e.g. Kiosks.

7. If I decline a request, does this cancel the contract/existing relationship with the payee?

No, declining a request does not automatically cancel a contract. Request to Pay is a messaging service and as such has no bearing on the contractual relationship between the payee and payer.

8. What additional information can be added to Request to Pay?

In addition to the base information required as part of every Request (Payee name, Bill Description, Amount, Payment period and Request reference), payees can add additional data about the transaction. For example, invoices, detailed bills, pictures etc.

9. I do not want to authorise each individual payment leaving my account especially recurring payments. Can I authorise a recurring payment?

At present, support for authorisation of recurring payments is not part of the minimum standard. However, this does not prevent Request to Pay providers offering this functionality.

10. Why do we need a minimum standard?

The standard would ensure that all solutions built addressed the end-user detriments and ensure interoperability across the industry. These standards will present the base standard, and we expect that the competitive market will provide additional features over and above this. The NPSO will have ownership of the standard and conduct accreditation of Request to Pay providers.

11. As a payee, will the added flexibility reduce my assurance in payers paying me?

No. Appropriate safeguards have been designed into Request to Pay to ensure it that it does not change the current risk profile associated with payers not making payments. These safeguards include: requiring appropriate notifications to payers on when payments are due and the consequence of not paying; notifying payees on the delivery status of the request to guard against instances where the payer did not receive the request.

In addition, the payee is legally covered by the existing contractual relationship between the payer and themselves. The contract should define the payment terms and consequences of the payers falling into arrears.

12. As a Request to Pay provider, what should I consider when offering this to vulnerable users?

Similar to other payment methods in use today, payees will continue to have a duty of care to ensure that they are conscious of payers who may be or at risk of falling into financial difficulty. Payees should refer to the appropriate best practices on this. Request to Pay provides increased dialogue between the payer and the payee and this will be helpful in identifying and working with vulnerable users.

13. As a payer will my credit score be impacted if I request an extension or decline?

A request or receipt of a payment extension should not result in detriment to the end user's credit score or be construed to imply the user is in financial difficulty. More work will be carried out as part of the Request to Pay implementation, in collaboration with payments community and The Steering Committee on Reciprocity (SCOR), to put in place the required standards.

14. What happens when the end date elapses whilst I am still waiting for a decision on a payment extension?

Payees will need to have parameters in place specifying the minimum and maximum time available for payees to respond to requests for payment extensions that provide a sufficient window to mitigate this risk.

15. What happens if for technical reasons I don't receive a request?

In cases where the payee does not receive the request, they are still liable to pay for services or goods consumed as defined in the commercial/contractual relationship. However, we have put in technical requirements to ensure that service providers meet adequate levels of resilience and reliability. In addition, payees should be able to determine the delivery status of a request sent and in cases of non-delivery make alternative arrangements.

16. Is Request to Pay safe from spam and fraudsters?

There are various measures in place to reduce the occurrence of spam and fraud in the Request to Pay service. These include:

Measures	Details
Service Provider accreditation	Providers of the Request to Pay service should be registered/accredited as part of ensuring that the service is trustworthy and reduce the risk of fraudulent use. Also, the NPSO will put in place governance to ensure Request to Pay providers demonstrate a minimum standard of information security.
Confirmation of Payee	Applicable payments initiated via Request to Pay should provide the payer with the ability to confirm that the payee details provided (Account number and Sort Code) are correct and belong to the intended payee. This solution is called 'Confirmation of Payee' and is intended to prevent cases of misdirected payments due to fraudulent activity.
Payee Verification for Business users (Payees)	Business payees sending out Request to Pay should be verified as part of the KYC onboarding process which should be visible to payers. This would provide payers with added assurance that the business payee from whom they have received the Request to Pay is a genuine actor.
Data encryption and security	Data throughout the system will be encrypted-at rest and in motion. In addition, adequate controls will be put in place to ensure end-user data is secure. For instance, service providers must be compliant with data protection regulations such as General Data Protection Regulation (GDPR) as well as all other applicable regulation such as Anti-Money Laundering directive 4 (AML4) and The Privacy and Electronic Communications Regulations (PECR).

Table 43: Measures against Fraud and Scams

7.3 Appendix 3 – Request to Pay Plan

Below is an indicative Request to Pay implementation plan:

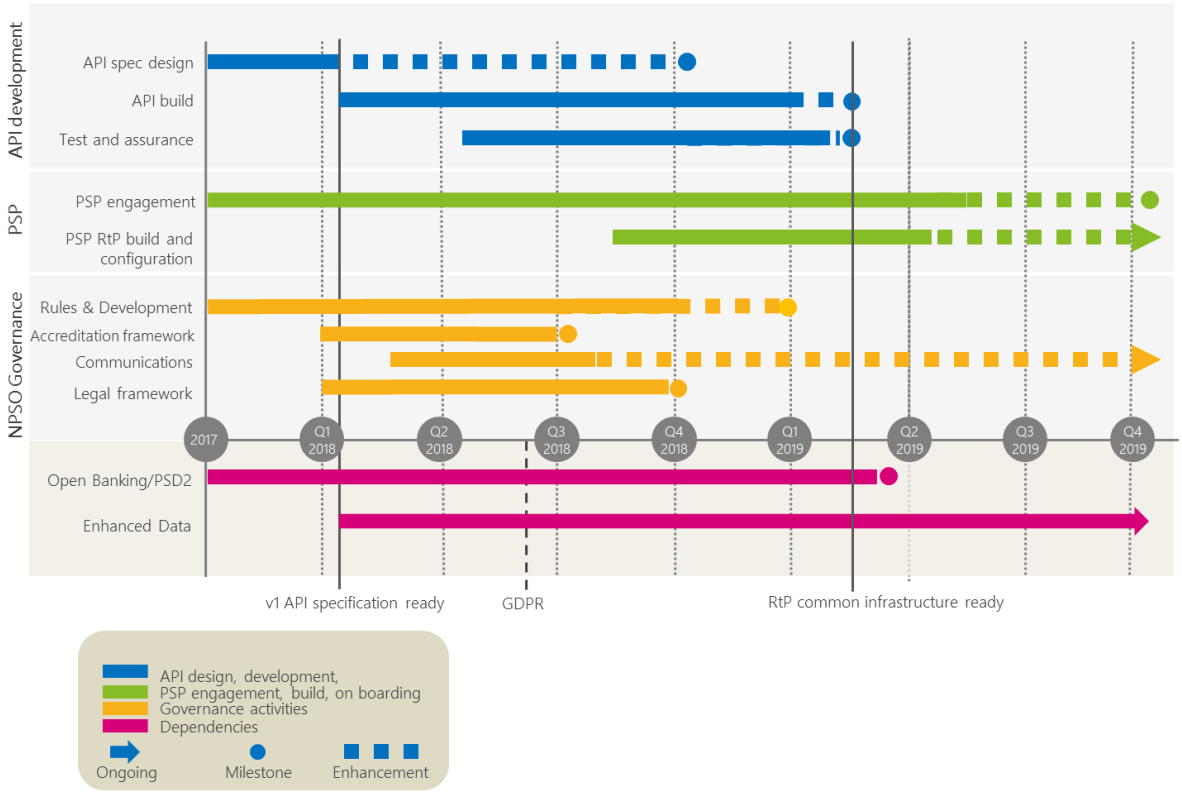

Figure 31: Request to Pay Implementation Plan

Notes:

- The NPSO will define the API specification based upon which PSPs will build Request to Pay repositories and end-user applications
- Request to Pay will be delivered on existing payment infrastructure with the capability to transition to the NPA
- The NPA will deliver the Enhanced data capability required to attach data to payments initiated via Request to Pay

7.4 Appendix 4 – CoP Response Approaches Analysis

Approach 1:

The payer is provided with an affirmative or negative confirmation on whether the account belongs to the intended payee.

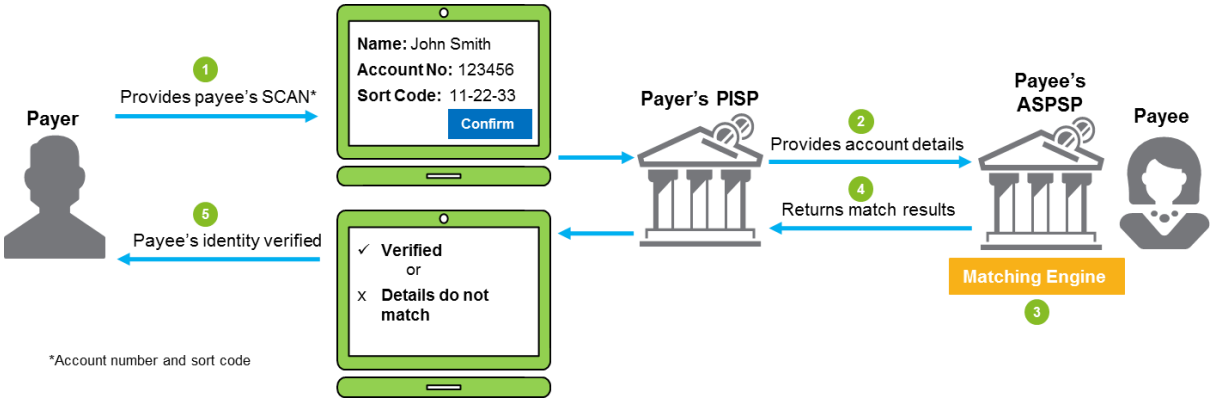

Figure 32: CoP Approach 1 End-to-End Journey

#	Step Name	Description
1	Provide Payee's SCAN	The payer inputs the payee's name, account number and sort code. The details provided by the payer are fed to their PSP.
2	Provide account details	The payer's PSP forwards the details provided to the payee's PSP.
3	Match the payee's name	The payee's PSP matches the payee's details with their records.
4	Return match results	The payee's PSP returns the match results to the Payer's PSP.
5	Payee's identity verified	The payer is provided with an affirmative or negative confirmation on whether the account belongs to the intended payee.

Table 44: CoP Approach 1 End-to-End Journey

Approach 2:

The payer is played back information on the payee: In this approach, the payer is provided with associated account information related to the sort code and account number. The payer uses this information to determine whether that account belongs to the intended payee.

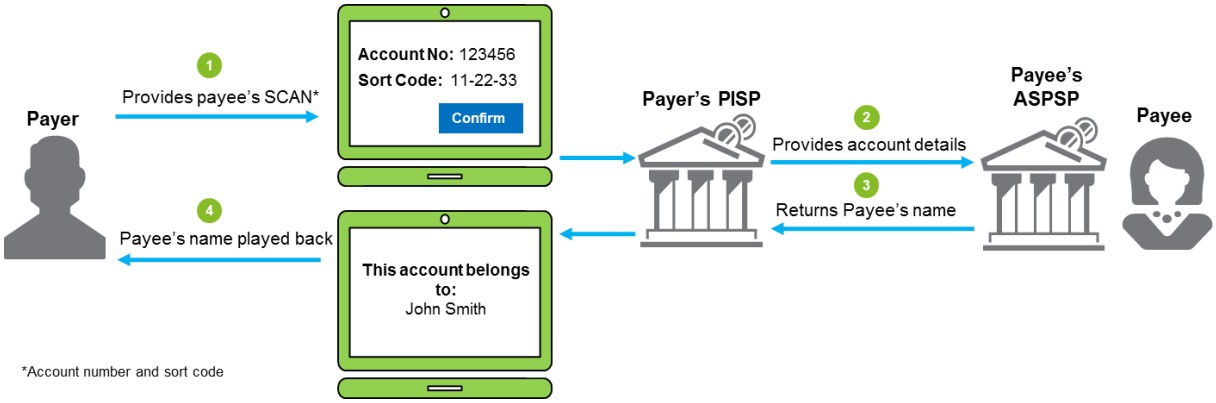

Figure 33: CoP Approach2 End-to-End Journey

#	Step Name	Description
1	Provide Payee's SCAN	The payer provides the payee's sort code and account number.
2	Provide account details	The payer's PSP passes this information to the payee's PSP.
3	Return payee's name	The payee's PSP returns the associated account name for the SCAN combination provided.
4	Payee's name played back	The name is passed by the payer's PSP to the payer. The payer then determines whether that is the intended payee.

Table 45: CoP Approach 2 End-to-End Journey

We posed a consultation question, to elicit responses on the preferred approach, considerations etc. 59 organisations have responded to the consultation. 11 responses were not analysed because they are unstructured. Of those analysed, 29 responded to the question on the CoP approaches. The results are presented below:

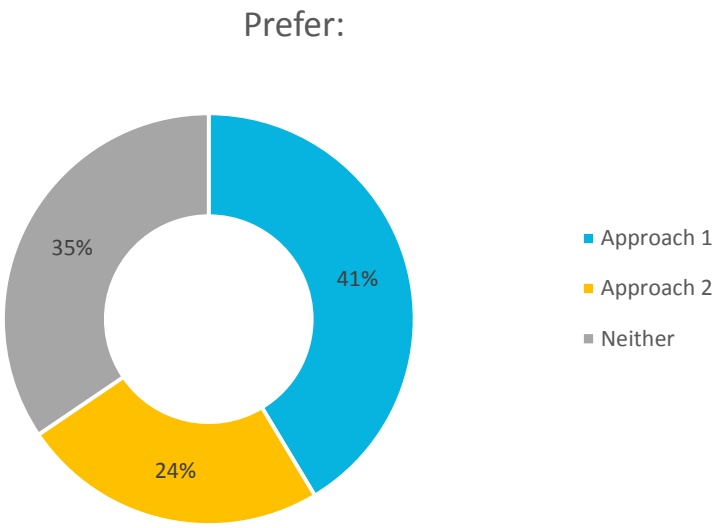

Figure 34: CoP Responses to Approaches 1 and 2

Among respondents, **41%** preferred Approach 1 while **24%** preferred Approach 2. A total of **10** organisations did not prefer either approach.
In their responses, respondents outlined the advantages and disadvantages of each of the approaches presented.

	Approach 1	Approach 2
Advantages	• Avoids sharing of personal data with payer • Simplicity which would ease integration with business rules and systems*	• Most useful to end-user • Easier to develop than Approach 1 • Increased transparency
Disadvantages	• Accurate match may prove difficult to obtain • Minimal value add to end-user in comparison to Approach 2 • Complexity of fuzzy logic and the liability associated to it on the payee's PSP	• Data protection and privacy is a major concern • Could expose accounts to other potential fraudulent activity and abuse • Would need to operate through a central database model to work* • Confusion where the account name fed back is different to the recognised name the payer was expecting.

Table 46: Advantages and Disadvantages of Approaches 1 and 2

7.5 Appendix 5 – CoP Architecture Comparison: Centralised vs Distributed

The 2 main approaches for delivering CoP are :

1. **Centralised Aprroach:**

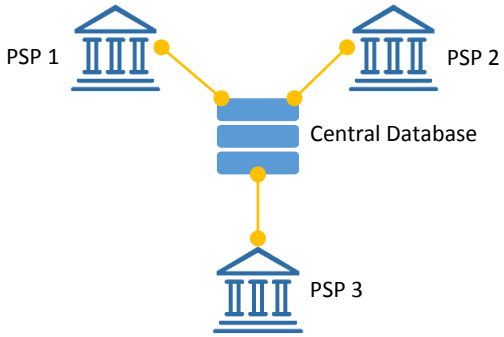

Figure 35: CoP Architecture - Centralised Approach

This approach utilises a single shared database to which all PSPs upload account information. The database is then queried for CoP requests.
In addition to the technical infrastructure, there is a centralised scheme to maintain integrity of the service and security of the data.

Pros

- ✓ **Existing solutions:** There are several centralised providers in the market. E.g. Paym, Vocalink (Accura), Experian etc. This tentatively reduces the timeframes required to adapt them to meet the PSF requirements
- ✓ **Multilateral Data agreements:** A common data sharing agreement can be utilised. In addition associated processes such as audits can be centralised.

Cons

- x **Security:** Due to the sensitivity of the information, a very high standard of security would be required guard against cyber-attacks etc.

2. **Distributed Approach:**

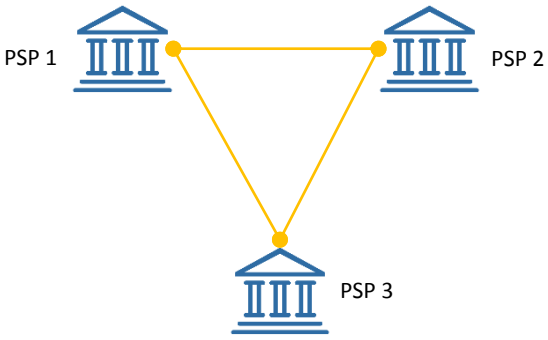

Figure 36: CoP Architecture - Distributed Approach

This approach utilises point to point APIs. The Payer's PSP directly queries the Payee's PSP to verify the account belongs to the intended payee. This aligns with the CMA open banking programme approach.
A central function may be required (but not mandatory) to facilitate routing and security.

Pros

- **Future proof:** The strategic industry direction is moving towards an API driven architecture. The CMA's Open Banking initiative is the best example
- **Competition**: Supports competition in the market
- **Distributed Security:** Each PSP takes care of its own data and removes the danger of a central database being compromised

Cons

- **Smaller PSPs may not have the technological capability:** Smaller PSPs especially most building societies and credit unions may not be able to build the required API infrastructure
- **Bilateral Data agreements:** Data sharing agreements required for each bilateral connection, and audit processes to ensure data isn't misused. May disadvantage smaller PSPs with less legal/audit resource

7.6 Appendix 6 – Data Protection Impact Assessment: Confirmation of Payee

SECTION I – INTRODUCTION

Confirmation of Payee ("CoP") will provide a payer with information to give them assurance that the account to which they are making the payment belongs to the intended payee. This will help to address the detriment associated with misdirected payments. As a special case, CoP will also include a Confirmation of Payer capability. Confirmation of Payer addresses the need for a payee setting up a payment mandate (direct debit) to verify that the account, from which they will be initiating the payment, belongs to the intended payer. The process for Confirmation of Payer is similar to CoP, especially regarding data processing. Where applicable, areas of difference are highlighted throughout the document.

In the approach assessed under this DPIA, the payer provides the account name, account number and sort code of the payee. This is passed on to the payee bank who respond with the payee's details. The payer bank returns an affirmative/negative response depending on whether the name provided by the payer matches the details returned by the payee bank for cases where the payee account is a personal account and in the case of non-personal accounts plays back the payee's details provided. In this case the account name, registered address and the company registration or equivalent. [45]

An individual's name is personal data and it will be utilised in CoP, hence a DPIA is required. A DPIA is also needed because this approach to Confirmation of Payee processes individuals' personal data for a new purpose.

SECTION II - PRELIMINARY SCREENING QUESTIONS

These questions are intended to help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

- **Does Confirmation of Payee involve processing of personal data about individuals?**

a. Yes - proceed to the next question.
b. No –

Yes, Confirmation of Payee involves the collection and processing of personal data about individuals.

- **Describe the nature of the personal data to be processed.**

Confirmation of Payee will involve as a minimum the processing of the following information: individual's first name, last name, account number and sort code.

- **Does the personal data processed include information not previously held about the individual?**

Confirmation of Payee will involve a provider, either a Payment Service Provider ("PSP") or a third party, receiving payee's personal data that they might not currently hold.

- **Indicate the Purposes for which the personal data will be processed. Is the personal data intended to be processed for a new purposes? If so, specify**

Yes. Confirmation of Payee is a new overlay service created as part of the End User solutions that form part of the New Payments Architecture (NPA) proposed in the PSF's

[45] See addendum for further explanation of how Confirmation of Payee will work

Strategy in Nov 2016 and further elaborated in the draft blue print published for consultation in July 2017. The Service provides payers making a payment with information that gives them assurance that the account to which they are making payments belongs to the intended payee. CoP is designed to help address the detriment associated with fraudulent and misdirected payments.

- **Will the processing involve sharing of personal data with entities which previously did not have access to such personal data? If yes, please provide details.**

Yes. Personal data about individuals (combination of name, account number and sort code) will be shared among PSPs and might be shared with third party organisations offering the Confirmation of Payee service.

- **Will new innovative technology and/or organisational solutions be used to process the personal data? If yes, please provide details.**

Yes. Confirmation of Payee will rely on a newly designed architecture based on Open API.

- **Will the processing involve sensitive personal data, personal data concerning vulnerable individuals or information particularly likely to raise a privacy concern?**

Possibly. Confirmation of Payee may be used to process the personal data of individuals categorised as Children under the GDPR or other equivalent data privacy regulations. Personal data processed under the service will be limited to the information listed in Question 2 and is not expected to include any further sensitive personal data.

SECTION III - IMPACT ASSESSMENT

Scope of the DPIA

30. What objective is the processing expecting to achieve?

Confirmation of Payee will provide a payer with information to give them assurance that the account to which they are making the payment belongs to the intended payee. This will help address the detriment associated with misdirected payments.

We have proposed that the CoP response provided to the payer will be clear and unequivocal. In our consultation, we identified two main forms that a CoP response could take: approach 1 (Matching approach) and approach 2 (Playback approach)[46]. We posed a consultation question to elicit responses on the preferred approach, considerations etc. Respondents highlighted flaws in both approaches. Based on the feedback provided we have designed an alternative approach that leverages on the advantages of both approach 1 and 2 and addresses the cons highlighted.

This PIA was only prepared for the alternative approach. Under this approach, the payer's PSP provides the payer's account name, account number and sort code; The payee's PSP returns the payee's account name (plus address and company registration number for companies) to the payee's PSP. In turn, the payer's PSP returns an affirmative/negative response (for personal accounts) or plays back the name, address and registration no (for corporates). This approach was agreed by the members of the Forum and will need to be tested and verified once implemented.

We provide further information on Confirmation of Payee in the July 2017 Consultation and WS1 supporting document.
Blueprint for the future of UK Payments

[46] See consultation document pp.34 and Appendix 7.4.

Information Flows Description

31. Describe the collection and use of personal data throughout the Confirmation of Payee process.

Data roles are summarised in the table below:

	Payee	Payee's PSP	Payer's PSP	CoP provider repository
Data Recipient			✓	
Data Subject	✓[47]			
Data Controller		✓		
Data Processor			✓	✓

Table 47: Confirmation of Payee Data Roles

The information flows are summarised in the diagram below:

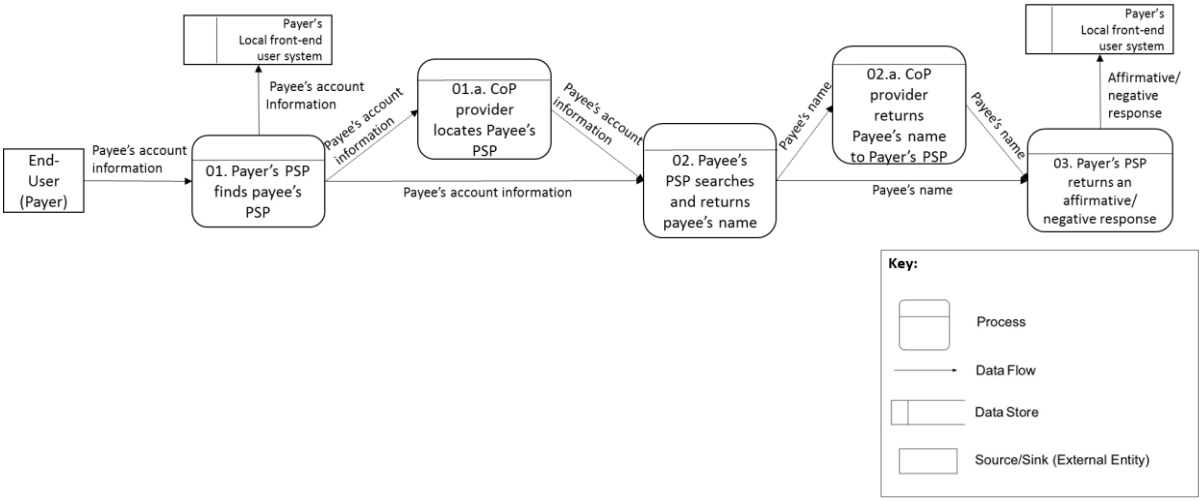

Figure 37: Confirmation of Payee Information Flow

Privacy Risk Evaluation

32. What is the volume of personal data to be processed and the number of individuals concerned?

The volume of personal data and individuals is not pre-determined. Confirmation of Payee or Payer is a service to be offered by PSPs for push and pull payments. It will be utilised through multiple channels: web, mobile, telephone, face to face, etc.

33. Does the project involve the transfer of personal data to countries or territories outside the European Union? If so, specify

The intended scope of the service is limited to payments occurring within the UK.

34. What is the expected duration of the processing?

The processing will be dependent on the usage of the Service by the Confirmation of Payee service provider ("the service provider") and is not subject to a prescribed duration.

[47] In the case of Confirmation of Payer, the data subject would be the payer.

35. Will the processing involve profiling or systematic monitoring? If yes, please provide details.

No. These activities are not expected to be within the scope of Confirmation of Payee's purpose. Logs of CoP queries, however kept, are not intended to be used for targeted monitoring.

36. Will the processing involve matching or combining data sets? If yes, please provide details.

No. These activities are not expected to be within the scope of Confirmation of Payee's purpose.

37. Have you identified other sources of risk to individuals' privacy?

Data Protection issue	Risk to individuals	Compliance risk	Risk to Associated organisation / corporate
Data security breaches and service failure Data security breach during storage of personal data or transit and service failure	There is a risk of technical failure of the service, or the exposure to external cyber threats or personal data being inadvertently shared with a third party outside the permissions given. This will result in personal data breaches	Risk of non-compliance with GDPR	Confirmation of Payee providers, PSPs or third parties, may be exposed to reputational damages, fines, penalties and loss of their customers' patronage.
Service fraud and phishing	There is a risk that personal data are misused by spammers, fraudsters (incl. phishing) or other malicious actors wrongfully accessing the service resulting in harm to individuals.	Risk of non-compliance with GDPR	Confirmation of Payee providers, PSPs or third parties, may be exposed to reputational damages, fines, penalties and loss of their customer's patronage.

Table 48: Confirmation of Payee Data Protection Issues

Proposed Risk Mitigations

38. Please provide a description of the measures envisaged to address the privacy risks identified.

Risk Title	Mitigation(s) Description	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project (Yes/No)?
Data security breach and service failure	Personal Data should be encrypted while in transit to mitigate the risk raised by security breaches. Governance requirements from the NPSO is expected to be in place to ensure Confirmation of Payee service providers demonstrate a minimum standard of information security for the service (e.g. service failure back-up plan).	The risk is reduced.	Yes
Service fraud and phishing	Service providers will be required to register / be accredited with the NPSO to ensure the service is trustworthy and reduce the risk of fraudulent use. CoP queries from customers should be logged to avoid phishing and identify cases of misuse as well as an audit trail. The CoP service will only be utilised for the purposes of making a payment. Service providers will be expected to ensure the design of the service minimise the exposure to phishing, fraud etc.	The risk is reduced.	Yes

Table 49: Confirmation of Payee Risk Mitigations

39. Has the lawful basis of processing been established? If yes, please specify

Processing relies on legitimate interest relating to the prevention of fraud and misdirected payments.

40. Describe how information about the processing will be provided to individuals. Do you need to amend your privacy notices?

Service providers will be expected to update their terms and conditions and privacy notices to cover the processing of their customers' personal data through Confirmation of Payee.

41. **If consent is the lawful basis of processing, how and when will the consent of individuals be obtained and recorded? Will measures be established to address withdrawal of such consent?**

Not applicable as Confirmation of Payee does not rely on consent. See question 10.

42. If relying on consent or necessity for contract as a lawful justification, has a data portability solution been designed?

Not applicable as Confirmation of Payee does not rely on consent. See question 10.

43. Is the processing of individual's personal data likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act?

No. Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society". Confirmation of Payee will not compromise the users' right to privacy and respect for family life.

44. Have you identified the social need and aims of Confirmation of Payee? Are your actions a proportionate response to these needs?

Yes. Confirmation of Payee provides payers with the assurance that the account to which they are making a payment belongs to the intended payee. The service addresses the identified need for assurance within the payment process and attempts to remediate detriments associated with accidental or maliciously misdirected payments. In addition, CoP will help address the issue raised by Which? around authorised push payments (APP) scams, hence reducing fraud. It therefore enhances end-users' confidence and reduces the financial and social impact related to misdirected payments.

45. Does your Confirmation of Payee plan cover all of the purposes for processing personal data?

Yes. The data plan provides a detailed illustration of the data journey and processing reflecting Confirmation of Payment's purpose. (See Section B, Question 2).

46. Have you identified potential new purposes as the scope of Confirmation of Payee expands?

At this stage of the project, the primary purpose of Confirmation of Payee has been set and confirmed under the agreed solution. This does not prevent other service providers from expanding the scope of the service in the future.

47. Is all the personal Data necessary and relevant to achieve the objectives of the processing?

Yes, the personal data in scope is necessary and relevant to ensure Confirmation of Payee achieves its objective. This relates to the processing of personal data required to appropriately determine that the account to which a payer is making a payment belongs to the intended payee.

48. Could the objective of the processing be achieved without use of data identifying individuals (e.g. by using anonymised data)?

The processing of data identifying individuals is necessary to ensure the service performs as intended. As such, the processed data is required to enable payers to confirm the identities of their intended payees and ensure their payments are appropriately directed.

49. How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Confirmation of Payment utilises the information held by the payee's PSP to determine whether the account intended to be paid belongs to the appropriate payee. This information is gathered as part of the KYC process carried out by the PSP. The PSP will, therefore, be responsible for ensuring that its KYC process is adequate and the information is kept up-to-date and accurate.

50. If you are procuring new systems does they allow you to amend personal data when necessary?

Yes. All users will have the option to amend their personal data when necessary through the PSP's existing customer's channels and processes.

51. What is the envisaged retention period for the personal data? What safeguards will be put in place to ensure the secure deletion/destruction of the personal data within the prescribed retention period?

Confirmation of Payee will be provided through a distributed API Architecture which does not include any personal data repository features. The personal data processed by the service will be retained at the PSP level and subject to the retention procedures of the PSP as well as the related regulatory requirements. In addition, payers may maintain a list of payees they may have confirmed previously through Confirmation of Payee.

52. What measures are envisaged to comply with the rights of individuals to access, rectification, erasure, objection to and restriction of processing?

PSPs will be responsible for establishing measures ensuring these Rights are respected as part of their GDPR Compliance framework.

53. Would Confirmation of Payee service providers use the personal data available for marketing purposes?

N/A. This does not apply to Confirmation of Payee.

54. What would be the potential impact on individuals in case of illegitimate access, undesired modification and disappearance of personal data?

Individuals may be exposed to negative or unwanted effects which may cause financial loss and moral damage (for example identity theft and fraud). See Section C, Question 8 for further information.

55. Do any new systems provide protection against the security risks identified?

Yes. Confirmation of Payee service providers will be required to demonstrate a minimum standard of information security. This will be overseen by the New Payment System Operator. The participants will be expected to take measures to maintain the integrity of the processed personal data, safeguard individuals from the risks identified and minimise the possibility of fraud or phishing. These measures are detailed in Question 9.

56. What training and instructions are proposed to ensure that staff know how to operate Confirmation of Payee securely?

This is to be determined at a later stage by the CoP service providers.

57. If personal data transfers in countries or territories outside of the European Union is envisaged, how will you ensure that the personal data is adequately protected?

N/A as no transfers outside the EU are planned at the moment.

SECTION IV - GOVERNANCE & VALIDATION

58. Have a consultation with representatives of individuals whose personal data will be processed been conducted? If yes, please provide details. If no, please explain why not. Who else will be consulted internally and externally as part of this processs? How will you carry out the consultation?

The development of the service was achieved collaboratively through numerous workshops and interviews with a range of stakeholders including various representatives of the main end-user groups: government, charities, consumer groups, retailers, housing associations, PSPs, and Payment System Operators (PSOs). In addition, we incorporated further research by various organisations already working on these solutions both within and outside the UK.

In July 2017, we published a Consultation Paper opened to comments from the public including representatives of data subjects. Responses were received by key associations and taken into consideration as part of the further development of the Solution.

The ICO will be consulted as part of this Data Protection Impact Assessment process.

7.7 Appendix 7 – CoP Implementation Plan

Below is an indicative Confirmation of Payee implementation plan:

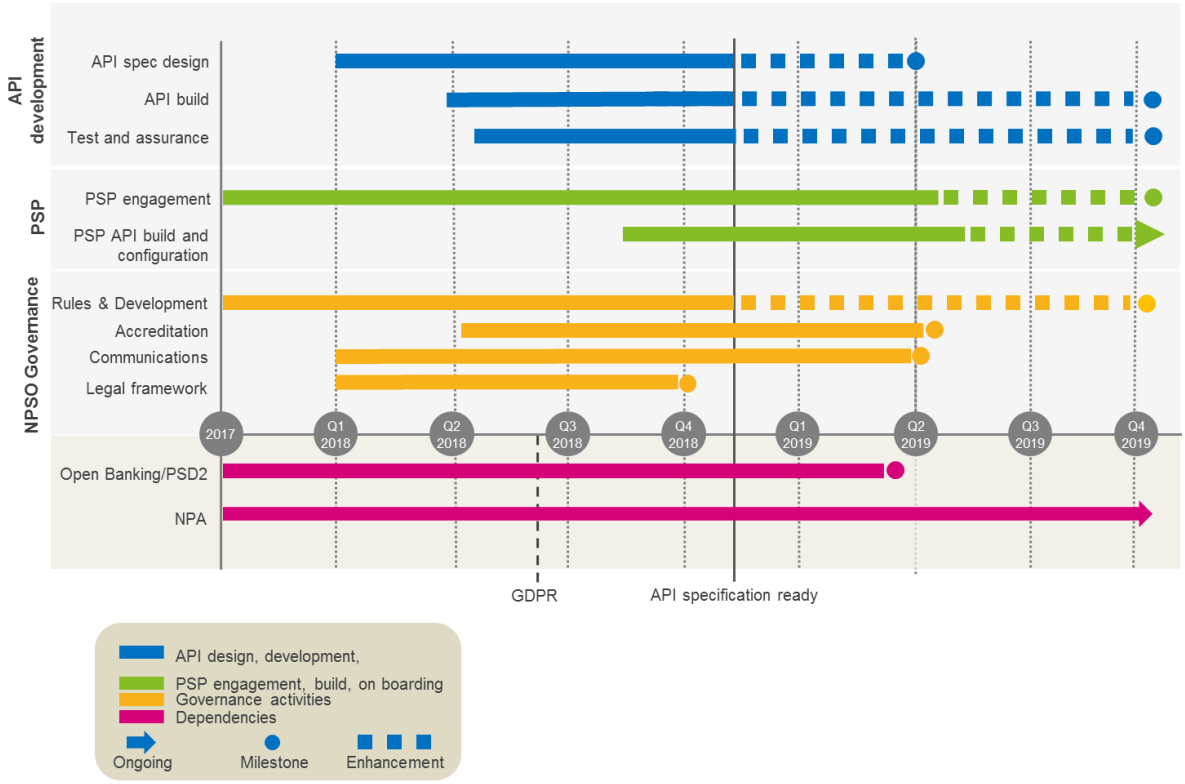

Figure 38: CoP Implementation Plan

Notes:

1. The NPSO will define the API specification based upon which PSPs and vendors will build the APIs
2. In addition to the API framework, CoP is dependent on PSPs configuring their customer channels e.g. online banking portals.
3. There is a dependency on the Open Banking API framework and the NPA to provide some common infrastructure e.g. API directory.

7.8 Appendix 8 - Payment Solutions Delivered by the Industry

Purpose of this paper

- To examine recent payment solutions that have been rolled out by the industry of a similar or comparable scale to overlay elements of the New Payments Architecture.
- To consider what worked well from these initiatives and what was less successful.

Examples of Industry Rollout of Payment Solutions

- Examples of payment solutions co-ordinated at industry level include chip and PIN implementation for card payments, Current Account Switch Service (CASS) and the Paym mobile payment service.
- Chip and PIN cards were introduced in 2004. The CASS Service began in 2013, while Paym launched in 2014.

Why is Industry Direction and Support Needed?

- Industry collaboration in payments is needed to create the minimum level of customer experience for an initiative to be successful.
- Innovation and competition can occur over and above this minimum level.
- In payments there is always a flow of funds between the initiator of the payment and the recipient. In card payments this is principally between the cardholder and retailer, while in other payments it involves the payer and payee.
- This means to be successful both the proposition for sender and receiver has to be compelling. Getting this balance right, stimulating investment by those working with each side of the market and doing this simultaneously is the key challenge for all new payments initiatives.

What happens if Industry is Not Involved?

- If the industry is not involved the risk of failure for a new payment initiative increases significantly.
- A striking example of this were the delays in widespread uptake of contactless card payments. For approximately 5 years the technology was available but take up was negligible. Despite efforts to co-ordinate at industry level the international card schemes pursued their own offerings and approaches. Initiatives to encourage retailers to accept contactless cards were inconsistent and each acquirer had differing attitudes to adoption.
- For card issuers the lack of a consistent acceptance proposition and short term business case limited rollout.
- In the end customers demanded the technology, as once used consumers adopted it strongly. This was driven on by the demand for contactless payments on mobile devices and subsequently supported by appropriate financial incentives to both sides of the market and finally mandates by the card schemes.
- It is not hard to see that a more co-ordinated approach to rollout and adoption could potentially have reduced the time to market for contactless cards by several years.
- In contrast in card payments the move to chip and PIN technology, a major infrastructure change for the industry, was delivered in a highly collaborative way, engaging all stakeholders and proved remarkably successful in modernising and securing card payments.

What Approaches Have Been Successful?

- CASS is a good example of where industry co-ordination supported by professional and skilled programme management delivered a new service across the whole payments industry.
- The driver of a regulatory demand to deliver a service brought the industry together but there were a range of factors that contributed to the success of the programme.
- This can be summarised in to 5 key success criteria, which became key pillars of the programme:

1. A clear mandate adopted by the industry setting out the requirement.
2. Adequate funding and structure for the programme agreed at an early stage.
3. Clear vision for the programme repeated regularly to stakeholders.
4. Having a clear and consistent plan.
5. Active management of stakeholders, which was the biggest single challenge.

- Other key learnings from the programme include:
- Recognising that consensus is the right approach rather than chasing the perfect answer that not all can get behind.
- Resolve critical issues where views differed at an early stage in the programme.
- Setting adherence principles at Board level 18 months prior to launch driving stakeholders to comply.
- Developing a Service Definition document used throughout programme delivery, which was developed and consistently updated. This allowed all parties to see what they had to do to be ready to go live at any given time.
- Having an effective commercial operator of the service following completion of the programme.
- Clear and consistent branding

What Approaches Have Been Less Successful?

- Paym was delivered to the market in 2014 in a secure and operationally efficient way, following an industry programme over the previous two years. It offers an innovative real time person to person mobile payment service.
- Take up of the service has been limited despite its ability to reach over 95% of UK accounts and lags markedly behind similar services developed subsequently in other countries, some of which have captured a greater proportion of the payments market e.g. Swish (Sweden), MobilePay (Denmark), Jiffy (Italy), Paymit (Switzerland).
- Despite the innovative and slick proposition the industry failed to address key issues including:
- Failure to force all participating banks to adopt Paym branding with key players using different names to support their own internal propositions.
- Operating alongside existing solutions with sizable market share.
- Participants were not forced to commit to deliver scale to the proposition.
- Under investment both in scheme marketing and by individual banks.
- Tackling low levels of registrations effectively.

Other Key Learnings

- Individual commercial offerings claiming to offer payments across the whole industry face significant challenges when compared to effective industry collaboration.
- It can be argued that Pingit has been highly successful for the owning bank but has constrained opportunities for a ubiquitous person to person payment service for all.
- Zapp (now renamed as Pay by Bank) has struggled to get adoption in the market. This is a good example of a payments service not only needing adoption by providers but acceptors of payments. Without take up by both of these parties then neither can be successful. This also reflects the fact that there was no regulatory or industry driver to push adoption forward.

Conclusions

- To deliver new payments solutions both the initiator and receiver of the payment and all parties in between need to be clear on what the service offering is and what they must do to participate in it.
- Having an industry or regulatory driver is more likely to deliver success as long as the vision is clear, realistic and unambiguous.
- Effective and efficient programme management is needed to manage stakeholders and ensure key decisions are taken early around a well-structured Service Definition.
- Creating the right collaborative approach to deliver the network effect needed for major change in payments to be successful will remain an important role for the industry.

7.9 Appendix 9 – Complete Set of Detriments

Detriment Group	#	Detriment
Customer Control	1	Payers and payees need more flexible mechanisms for collecting and making recurrent and ad hoc payments.
	2	Payers and payees need more mechanisms for payments that give greater control to the payer and more certain outcomes for the payee.
Customer Assurance: Additional functionality for both payer and payee	3	Payers and Payees require additional functionality in order to be able to: • confirm payee (validation of name or proxy regarding payment account details).
	4	• confirm adequate funds are available to cover payment.
	5	• confirm the status of payment.
	6	• confirm receipt of payment.
	7	• include additional reference data in the payment (to ease reconciliation).
	8	• include additional data for third parties (e.g. accounting; taxation and age verification).
Customer financial capability	9	Some financial products are overly complex and lack transparency, leading to avoidance by unconfident users.
	10	Access to cash remains important for many users (due to either low or unpredictable incomes or mistrust of electronic payments due to lack of transparency) - and will continue to do so while non-cash products do not meet their needs for control and transparency.
	11	Competition is not currently meeting user needs for simplicity.
	12	Competition is not currently meeting user needs for transparency.
	13	Competition is not currently meeting user needs for control.
	14	Competition is not currently meeting the needs of low income / low use users who need simple payment mechanisms and prefer cash.

Detriment Group	#	Detriment
Corporate customers	15	There is lack of realistic alternative payment options other than cards available to merchants / retailers.
	16	Online payments – there is a lack of access for business users for alternative rails (i.e. need more availability of credit transfer payment online).
	17	Card scheme fines (for which there is no appeals process) are mandated onto merchants.
	18	There is a lack of user say in changes mandated from card scheme level - merchants bear costs with no representation at governance level.
	19	International payments for Retail and Corporate users are sometimes hard to execute as UK Payment Systems not perfectly connected to international equivalents.
	20	Corporate service users would like to know where payments are at all times if it is not real-time.
	21	There is a need for greater transparency of users for services in corporate space.
	22	Reconciliation costs and treasury management for businesses; also government reporting costs.
	23	The distance between physical and financial supply chain affects e-invoicing.
Customer identity, authentication and knowledge	24	A customer's identity is used successfully by a criminal (third party).
	25	Customers have day to day concerns about risk of identity theft and risk of fraudulent activity on an account.
	26	A payment is made to a wrong account.
	27	There is friction in the payment service. For example: • Online payment verification checks, e.g. a '3D Secure' retailer. • Point-of-Sale card payment declined by PSPs fraud systems as a 'false positive'. • Opening a bank account, application is declined due to ID checks.
	28	Businesses pay into accounts not owned by their suppliers due to false invoices or false change of bank account notifications.
	29	The industry need to better understand who the payment initiator (payer) is and paying account.
	30	The industry need to better understand who the payment recipient (payee) is and the beneficiary account.
	31	Current ID solution may not be sufficient for proof of identity in criminal cases.
	32	The industry need to know who their vulnerable consumers are.
	33	At account opening, where customers are seeking access to payment instruments, the industry need to understand who the applying customer is.

Detriment Group	#	Detriment
Data sharing, reference data, and analytics	34	Insufficient reference data and a lack of knowledge sharing amongst users results in gaps in preventing financial crime; fraud, money laundering, terrorist financing, bribery and corruption.
	35	Real-time payment risk is limited, reducing the ability of customers and PSPs to act against fraudulent payments. For example, business customers and government departments are constrained in identifying fraud by the lack of information available on the payee / beneficiary account, and the payer / remitter account.
	36	Switching to a new bank means re-doing checks for Know your customer (KYC), anti-money laundering (AML) and anti-terrorist financing.
	37	When a customer actually realises payment is a fraud, banks cannot work quickly together to target mule accounts and to prevent funds being paid away.
	38	Banks cannot make fully reliable risk decisions on third parties because they cannot be 100% sure of identity and information about them.
	39	A beneficiary bank has limited information about a remitter, the reason for payment and the network of accounts the beneficiary account transacts with - impacting its ability to identify accounts used to receive proceeds of fraud.
	40	Banks cannot comply easily with KYC, AML or anti-terrorist financing requirements on their own customers or on third parties.
	41	Unnecessary bank secrecy prevents effective control of money laundering.
International payments and account activity	42	There is a lack of clarity regarding the speed, costs and risks of international payments.
	43	Bank account access - opening or maintaining account facilities - regulatory burden is different, and variable, in different territories.
	44	The perceived risk of fraud is higher for international payments e.g. businesses pay into accounts not owned by their suppliers due to insufficient ability to confirm payee identity and beneficiary account.
	45	The customer identity and data sharing approach for international payments is less robust than that for UK-UK payments.
	46	There is a lack of understanding of the ultimate beneficiary owner (UBO) and robustness of KYC.
	47	There are issues around the emergence and growth of alternate PSPs and methods where regulation is less robust, and banks have limited control, e.g. blockchain, cross-border payments being made under the disguise of domestic payments (Hawala-type payments), giving rise to consumer safety issues and money laundering opportunities.
	48	Using the name of legal entities or individuals is not sufficient to uniquely identify them across jurisdictions.

Detriment Group	#	Detriment
Payment scheme issues/ weaknesses	49	There is insufficient merchant education and understanding on fraud levels and best practice for engaging with Payment Schemes.
Customer education and awareness	50	There is a lack of customer awareness about mule accounts for avoiding 'non-complicit' involvement and criminal implications of complicit involvement.
	51	There is a lack of customer awareness of widespread methods used for fraud - such as duped customer payments (e.g. caller requesting remote access to PC, romance scams, pension liberation, invoice diversion, ghost payroll, etc.).
Choice and competition	52	There are only a small number of sponsor / commercial solutions for indirect PSPs.
	53	Consumers have little choice if they require a PSP with real-time Faster Payments (FPS). There are 10 members of FPS and only these banks offer real-time FPS to their customers. If customers want real-time payments, they need to bank with one of the 10 members.
	54	Existing sponsor banks can limit competition as there are only a few that offer indirect access; indirect PSPs are reliant on the Sponsor Bank solution and innovation.
	55	It's difficult for PSPs to switch indirect access providers as Sponsor Banks' solutions may make it difficult to switch to another provider.
	56	New types of PSPs may encounter difficulties in finding direct PSPs to sponsor them and get access to a payment system, due to having new models where current sponsor bank risk appetite will not support such entities.
	57	There is a lack of competition between schemes.
	58	There is a lack of interoperability and common standards in the payments infrastructure which reduces the ability for PSPs to innovate and businesses to benefit from new payment options.
	59	There is no level playing field for PSPs that are not a credit institution due to difficulty in obtaining a BoE settlement account as a new direct participant.
Common standards and rules	60	Too many standards and too much complexity reduce front end simplicity and stifle innovation, unlike the EU where the Single Euro Payments Area (SEPA) has aligned rules for DC / DD.
	61	Different rules and standards within EU to the UK; SEPA has largely aligned EU standards / rules for DC / DD and should do for instant (real-time) payments. Still in-country variances.
	62	The range of standards could limit infrastructure competition. If operators set the rules, there could be multiple infrastructure providers, provided they are all aligned to an ISO standard.
	63	There is no real substitutability between payment systems in the event of system failure.

Detriment Group	#	Detriment
Schemes for rules and governance	64	Indirect PSPs don't own the schemes so change and governance of schemes is driven by big banks. There is no effective voice for indirect participants' views to be taken into consideration by the schemes.
	65	There is no clear / transparent on-boarding process or requirements for PSPs to join a scheme and the process can be lengthy and costly for participants to join. Scheme rules are too complex, therefore expensive to join and / or comply with.
	66	There are expense implications for card issuers / acquirers to be direct members of card schemes.
	67	Multiple payment schemes are expensive, complex and time consuming to join for PSPs and confusing for end-users. Cheque imaging is an added scheme, which risks this reinforcing the multiple operator model.
	68	Card scheme governance does not adequately represent merchants and can be inflexible when translating USA-based rules into rules for EU firms.
Third party	69	Third party users (end user PSPs) can't initiate real-time payments and access data as they have difficulty gaining access.
Switching	70	Consumer and corporate users are reluctant to switch bank accounts which increases costs of banking to end users.
	71	The need to change sort code and account numbers when switching bank accounts creates difficulties for customers making payments / companies receiving and causes loss of competitiveness in banking provision.
Innovation and Competition	72	Banks are not good at innovating – the external market should innovate.
	73	There is no long term strategy for blockchain.
	74	New technologies –there is a lack of products not running on old 'rails' (i.e. 4-party-scheme model). Need to make it easier for new entrants to get established in the market.
	75	There is a lack of competition between schemes.
	76	Mobile payments – lots of closed applications for payments that are not interoperable higher up the chain making life complex for consumers.
DD Guarantee	77	Unlimited Direct Debit (DD) guarantee makes it difficult to provision for risks or acts as a barrier for non-direct PSPs and end-users to offer the service.
Data theft	78	Consumer data is exposed to theft at multiple points along the value chain, leading to increased fraud.
Fraud	79	Merchants have little information on fraud levels and no appeals process for card scheme fines.
Localisation	80	Card scheme rules need to be localised.
Execution Risk	81	Execution risk – the more change we add into the system, the greater execution risk in the climate of cybercrime.
Choice and competition	82	New third party providers can't initiate payments and access data to initiate payments.
Localisation	83	The USA centric model doesn't translate to EU regulatory framework – e-money is missing, for example.

Table 50: Complete Set of Detriments

7.10 Appendix 10 – Stakeholders Log

Table 51 shows the meetings that were held by Workstream 1 with different industry stakeholders to review the EUN solutions.

Stakeholder's name	Stakeholder Type	Date of session	Location	Subject	Solution Reviewed	Representative
Payments UK	Scheme	15/02/2017	Payments UK (2 TMS)	Collateral Review - Overview of existing solution work	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Nick Rucker
Vocalink	Solution Vendor	22/02/2017	EY (25 CP)	Solution Presentation	2. Assurance Data	1. Michael Kitt 2.Marc Corbalan 3.Richard Luff
Faster Payments (FPS)	Scheme	23/02/2017	Faster Payments (2 TMS)	Collateral Review - Introduction to Request for Payment	1. Request to Pay	Mike Banyard
Payments UK	SME	02/03/2017	EY (25 CP)	Collateral Review - World Class Payments walkthrough	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Nick Rucker
Paym	Scheme	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	John Maynard
Faster Payments	Scheme	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Simon Brooks
BACs	Scheme	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Anne Pieckielon
Toynbee Hall	Charity	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Sian Williams
Housing Association	Housing Provider	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Philip Exley
NS&I	Government	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Christine Mose
DVLA	Government	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Natalie Morgan 2. Kathy Merchant
HMRC	Government	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Karen Rhodes-German 2. Diane Heights
DWP	Government	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Nick Davies
British Gas	Utility	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Clare Buck
Money Advise	Advisor	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Carl Pheasey
Nationwide	Financial Institution	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Ruth Bookham
HSBC	Financial Institution	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Glyn Warren
Signia Money (QuidCyle)	Fintech	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Shahini Vallipuran
Individual User	End User	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Carl Packman
Small Business Federation	SME	07/04/2017	EY (25 CP)	EUN Use Case definition Workshop	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Mike Agate
WS02	BAs	11/04/2017	Payments UK (2 TMS)	WS01-WS02 interlocks		Adrian Burholt
Paym	SME	20/04/2017	Payments UK (2 TMS)	EUN Requirements Review	1. Assurance Data	John Maynard
Consumer Panel	End User	25/04/2017	EY (1 MLP)	EUN Requirements Review	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Dominic Lindley

Stakeholder's name	Stakeholder Type	Date of session	Location	Subject	Solution Reviewed	Representative
Which?	End User	28/04/2017	EY (25 CP)	EUN Requirements Review	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Richard Piggin 2.Jamie Thunder
WS02	BAs and Architects	28/04/2017	Payments UK (2 TMS)	EUN Use Case Review	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Nitin Aggarwal 2. Peter Elliot
Tesco	End User	02/05/2017	Maldon, Shire Park, Welwyn Garden City	EUN Requirements Review	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Bailey, Jake 2. Baines, Stephen 3. Boden, Ian 4. Norris, Tamasin 5. Arnott, Adam 6. Lacey, Colin 7. Condon Gareth 8. Tony Shaw
DVLA	Government	16/05/2017	DVLA, Swansea	EUN solutions cost and benefit analysis	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Rachael Cunningham 2. Natalie S Morgan 3. Kathy Merchant 4. Tacy Nash
Age UK	Charity	17/05/2017	Age UK, London	Payment Strategy Forum - User Requirements and Rules	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Lucy Malenczuk
Home Office	Government	19/05/2017	Teleconference	Requirements definition for Payment Strategy Forum	1. Request to Pay 2. Assurance Data 3. Enhanced Data	De Freitas Liz
Oracle		22/05/2017	Teleconference	PSF NPA Overview of the End User solutions	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Margaret Walsh
HMRC	Government	31/05/2107	EY office	PSF NPA Cost Benefits Analysis Meeting	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Chris Donovan 2. Nancy Gillespie 3. Karen Rhodes-German
DWP	Government	01/06/2017	Video Conference	PSF NPA Cost Benefits Analysis Meeting	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Deborah Farrell
BACs	Scheme	07/06/2017	IR-Waterloo	Catch-up		Anne Pieckielon
ICO		09/06/2017	EY Office	PSF EUN Solutions review - Data protection		Richard Syers
Nationwide	Financial Institution	14/06/2017	EY Office	WS01 Data Protection and Privacy		Tim Pigott
BoE and CHAPS		14/06/2017	MR-TSGd-CD-265-GdM	BoE, CHAPS and WS1		John Jackson
RBS	Financial Institution	15/06/2017	Teleconference	Real-time balance	2. Assurance Data	Jane Barber
WS02	BAs and Architects	14/07/2017	Teleconference	Consultation doc		Adrian Burholt, Paul Goodwin
Paym	Scheme	03/08/2017	Teleconference	CoP and Data Protection	2. Assurance Data	John Maynard
FPS	Scheme	03/08/2017	2 TMS	Request to Pay Overview	1. Request to Pay	Simon Brooks
FPS	Scheme	08/08/2017	EY Office	Request to Pay H2 work plan	1. Request to Pay	Simon Brooks
FPS	Scheme	15/08/2017	EY Office	Joint work plan	1. Request to Pay	Simon Brooks
OBIE		16/08/2017	Teleconference	OBIE/PSF Connection		Aissa Rice-Tagon
PSR		21/08/2017	FCA head office	Data protection issues re Confirmation of Payee and other End-User Needs solutions	2. Assurance Data	1. Kathryn Hardy 2. Robert Sullivan 3. Amanda Butler 4. Michael Begg 5. Adam Boult 6. Tim Pigott
BRC	End User	22/08/2017	Teleconference	Consultation conference call: Blueprint for the Future of UK Payments	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Andrew Cregan and BRC members
FPS	Scheme	22/08/2017	2 TMS	Catch up meeting Sian and Craig		1. Craig Tillotson 2. Sian Williams
Bacs	Scheme	23/08/2017	Teleconference	CASS Potential Beneficiaries		1. Alex Jackson 2. David Core 3. Anne Pieckielon
FPS	Scheme	23/08/2017	Teleconference	Joint NPSO-PSF plan review	1. Request to Pay	1. Simon Brooks 2. Ivan Litovski 3. Sean Doherty
FPS	Scheme	24/08/2017	2 TMS	PSF NPSO Consolidated Project Plan	1. Request to Pay	1. Simon Brooks 2. Ivan Litovski 3. Sean Doherty

Stakeholder's name	Stakeholder Type	Date of session	Location	Subject	Solution Reviewed	Representative
OBIE, WS02		30/08/2017	2 TMS	Open Banking - Collaboration review;		1. Adrian Burholt 2. Paul Horlock 3. Gary Farrow 4. Sailesh Panchal
FPS	Scheme	30/08/2017	Teleconference	Request to Pay API spec	1. Request to Pay	1.Ivan Litovski 2. Sean Doherty
Answer Digital		30/08/2017	EY Office	Request to Pay solution	1. Request to Pay	Imran Ali
LBG	Financial Institution	31/08/2017	LBG 33 Old Broad Street	PSF consultation document overview to LBG	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Nicola Levy
VocaLink	Soution Vendor	01/09/2017	Teleconference	Vocalink / Accura - Confirmation of Payee.	2. Assurance Data	Richard Luff
WS02	BAs and Architects	04/09/2017	Teleconference	Enhanced data and other end user needs	3. Enhanced Data	Pulavarnatham Swamy
Which?	End User	07/09/2017	EY Office	PSF End-User Needs Requirements and Rules: Request for input from Which?	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Jamie Thunder 2. Richard Piggin 3. Vanessa Furey 4. Mark Falcon
Toynbee Hall	Charity	07/09/2017	EY office	Request to pay considerations discussion	1. Request to Pay	1. Carl Packman 2. Sian Williams
OBIE		11/09/2017	2 TMS	OBIE-PSF interlock-Request to Pay	1. Request to Pay	1. Gary Farrow 2. Chris Michael 3. John Maynard
Bacs	Scheme	12/09/2017	2 TMS	Brainstorm session		1. Anne Pieckielon 2. Alex Jackson 3. David Core 4. Keith Hutchison 5. John Stenhouse
OBIE		14/09/2017	2 TMS	OBIE-PSF interlock-Request to Pay	1. Request to Pay	1. Gary Farrow 2. Joss Wilbraham 3. Ivan Litovski 4. Sean Doherty 5. Mike Banyard
WS02	BAs and Architects	19/09/2017	Teleconference	CoP and RtP architectures	1. Request to Pay 2. Assurance Data	Adrian Burholt
Coop	Financial Institution	20/09/2017	Teleconference	Future of UK Payments		Adam Williams
Experian	Credit agency / solution vendor	22/09/2017	EY office	PSF Confirmation of Payee	2. Assurance Data	Darryl Warner
BT	Utility	25/09/2017	BT office - Crawley	Request to Pay	1. Request to Pay	Neil Rowan
HSBC	Financial Institution	27/09/2017	EY Office	Meeting with EY & HSBC		Andrew Slough
Clydesdale Bank	Financial Institution	02/10/2017	EY office	Confirmation of Payee discussion	2. Assurance Data	Dougie Belmore
Metro Bank	Financial Institution	11/10/2017	Teleconference	CoP Review	2. Assurance Data	Simon Cunningham
HMT	Government	23/10/2017		HMT Meeting re CoP	2. Assurance Data	Meeting attendees: 1. Sian Williams 2. Paul Horlock 3. Dora Guzuleva
NPSO		25/10/2017	2 TMS	WS1 Handover sessions	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Tim Yudin 2. Mark Duckworth
LBG	Financial Institution	01/11/2017	Teleconference	PSF- Confirmation of Payee Analysis - Lloyds Feedback	2. Assurance Data	1. Graeme Donald 2. Samuel England 3. Eileen McEwan 4. Susie Harrold 5. Craig Hodgson
Which?	End User	06/11/2017	EY Office	FOLLOW UP: PSF End-User Needs Requirements and Rule	2. Assurance Data	1. Mark Falcon 2. Vanessa Furey
Experian	Credit agency / solution vendor	08/11/2017	EY Office	CoP follow-up with Experian	2. Assurance Data	1. Darryl Warner 2. Nicola Brittliff
FPS	Scheme	13/11/2017	Teleconference	External : British retail consortium	1. Request to Pay	1. Simon Brooks 2. Jacob Tose 3. Sean Doherty
RBS	Financial Institution	14/11/2017	Teleconference	Request to Pay certainty of Payment whitepaper	1. Request to Pay	Jane Barber

Table 51: WS1 Communications Log

7.11 Appendix 11 – Working Group Members

The working group Chairs identified the need to bring on board expertise from the industry in an advisory capacity to the co-chairs. They will form part of the core working group. A request for volunteers able to put in at least 2 days a week was posted on the Forum's website on the 24th of February.

Sian Williams

Head of National Services and Director of the Financial Health Exchange at Toynbee Hall

Joining Capacity: Co-Chair - Advisory Group

Sian is Director of the Financial Health Exchange at Toynbee Hall in London's East End, where she leads systems-thinking programmes aimed at making products and services more inclusive, and skilling up consumers to use them effectively. Successes include the launch of a digital needs and impact measurement tool, MAPT, the development of a highly effective community peer money mentoring programme, and research which helps the industry to address significant access gaps, including for the then Payments Council on the cash and electronic needs of consumers and for Link on the impact of lack of access to a free-to-use ATM.

Sian sits on a range of industry advisory groups, is a Financial Inclusion Commissioner, a member of the Payment Systems Regulator's Panel, and a trustee of the Money Advice Trust. Prior to joining Toynbee Hall, Sian had a 15-year career with the Foreign and Commonwealth Office, including covering the Asian Financial Crisis in Hong Kong and the shift from a planned to market economy in China.

Carl Pheasey

Head of Policy at Money Advice Service (At the time)

Joining Capacity: Co-Chair - Advisory Group

Carl is Head of Policy at the Money Advice Service (MAS). He is responsible for the development of evidence-based policy across a range of financial capability and strategy issues and for the development of consumer advice positions. Prior to joining MAS, he held senior public policy roles with British Airways and TSB Bank.

He previously held a number of roles in HM Treasury, advising on a range of microeconomic and financial issues, including utility regulation, competition policy, infrastructure finance, and financial consumer protection policy. Earlier in his career, Carl held a number of roles in local and regional government.

Gareth Winfield

Head of Commercial for Digital Payments at Barclaycard

Joining Capacity: Subject Matter Advisor - Advisory Group

Gareth is currently Head of Commercial for Digital Payments at Barclaycard. He joined the working group as a subject matter advisor given his expertise in commercial management, strategy management and most recently head of commercial for digital payments, developing and bringing to market new mobile and digital payment propositions.

Giles Rowlinson

Schemes Executive at Bacs Payments Schemes Limited
Joining Capacity: Subject Matter Advisor - Advisory Group
Giles is currently Schemes Executive at BACS. At Bacs, he works with businesses to optimise the effectiveness of their use of Bacs Direct Credit and Direct Debit, giving him a deep understanding of how businesses use payments. He also has relevant experience of payment agnostic messaging systems, having managed the electronic Cash ISA Transfer Service. He is currently working with fintechs on front end innovations utilising the existing Bacs payment rails.

Glyn Warren

Senior Payments Industry Manager at HSBC Bank
Joining Capacity: Subject Matter Advisor - Advisory Group
Glyn is currently the Senior Payments Industry Manager at HSBC. He joined the working group as a subject matter advisor given his cards and electronic payments expertise. He has undertaken a variety of roles in personal banking and payments. Some of the roles have included Debit Card product management for HSBC including working on the launch of contactless payments, Chip and PIN implementation, Switch Card scheme migration to Maestro and oversight of the Link ATM capability from an issuer perspective. Throughout this time Glyn has represented HSBC on a wide range of industry and payment scheme roles and initiatives. Over the last 5 years, he has been working directly in a Payments Industry team.

Simon Brooks

Senior Product Manager at Faster Payments
Joining Capacity: Subject Matter Advisor - Advisory Group
Simon is currently the Senior Product Manager at Faster Payments. He joined the working group as a subject matter advisor given his expertise in payments. He has worked in the financial industry for over 30 years during which time he assisted with the introduction of the Faster Payments Service in the UK as a Product Manager with HSBC and as the Chair of the APACS Faster Payments Communications Working Group. He has worked in many areas of HSBC including Payments Operations and Global Risk.

Simon joined Faster Payments in 2014 as a Development Manager, before taking up his current position.

Ruth Bookham

Payment Strategy Specialist at Nationwide Building Society
Joining Capacity: Subject Matter Advisor - Advisory Group
Ruth is currently a Payments Strategy Specialist at Nationwide Building Society. She joined the working group as a subject matter advisor given her understanding of the payments needs of businesses, government and consumers and knowledge of UK payments systems and wider industry changes relevant to developing the End-User Needs Solutions.

Ruth has over fifteen years' experience in payments and investment banking having previously worked in the Payments Council's policy team and central strategy teams of Visa Europe and NatWest's investment banking arm. Ruth was a member of the End-User Needs Working Group in 2016.

Ruth Milligan

Head of Financial Services & Payments at TechUK

Joining Capacity: Subject Matter Advisor - Advisory Group (Legal)

Ruth is currently head of Financial Services & Payments at TechUK. She joined the working group as a subject matter advisor given her legal and payments expertise. Ruth is a qualified UK solicitor, specialising in competition law, payments and retail financial services at UK and EU level. Currently, she takes the lead on all issues relating to payments, open banking and PSD2, insurance, financial inclusion, identity and block chain, sitting on Open Banking Working groups and the Payments Strategy Forum groups. Previously, Ruth has 8 years of experience as payments expert for the retail sector in Brussels, advising on the evolution of the Interchange Fee Regulation and PSD2 and representing retail on the Euro Retail Payments Board and the Card Standardisation Group.

7.12 Appendix 12 – Glossary

Term	Definition
Account identifier	Combination of numeric, alphabetical or alphanumeric characters used to uniquely identify and account.
Account Information Service Provider (AISP)	A payment service provider which provides account information services.
Account Servicing Payment Service Provider (ASPSP)	A payment service provider providing and maintain a payment account on behalf of the account owner, generally a bank.
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.
Authorised payment	A payment where the customer has given their consent for the payment to be made – and this can include situations where the customer has been tricked into giving that consent.
Back-office	An office or centre in which the administrative work of a business is carried out, as opposed to its dealings with customers.
Bacs	The regulated payment system which processes payments through two principal electronic payment schemes: Direct Debit and Bacs Direct Credit. The payment system is operated by Bacs Payment Schemes Limited (BPSL).
Block	Request to Pay Response Option: Stop a payee from being able to send you requests in the future. Payees will be notified in this instance.
Channel	An interface through which communication can be made.
Cheque & Credit Clearing (C&CCC)	Payment scheme providing net settlement of cheques and paper credits between financial institutions. It operates on a three-day cycle and settles net once a day in RTGS.
CHAPS	The sterling same-day system that is used for high-value/wholesale payments as well as for other time-critical lower-value payments.
Consumer	A person who buys goods or services for their own use.
Contact payee	Request to Pay Response Option: Provides a way for a Payer to contact the Payee that has sent a request. This could be within the Request to Pay service or simply signposting to other communication options (e.g. phone, e-mail, post).
Corporate	Relating to a large company.
Current Account Switch Service (CASS)	Free to use service that lets consumers and small businesses switch their current account from one participating bank or building society to another. It

	has been designed to be simple, reliable and stress-free and is backed by the Current Account Switch Guarantee.
Customer accounts	A customer account that can be debited or credited.
Decline	Request to Pay Response Option: Decline a request for payment and inform the Payee that you As a payer will not be paying a request.
Detriment	The state of being harmed or damaged.
Direct credit	A payment service for crediting a payee's payment account, with a payment transaction or series of payment transactions, from a payer's payment account, by the payment service provider which holds the payer's payment account, based on an instruction given by the payer.
Direct debit	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider.
Due date	The date that the request must be paid by.
En route	During the course of a journey; on the way.
End-User	Refers to payments service users. Includes those who use, or are likely to use services provided by payment systems and is not limited to a specific group of users. Service users will include – banks who use payment services provided by other institutions; businesses; retailers; charities; government and consumers.
Faster Payment Scheme (FPS)	Payment System providing near-real time payments on a 24x7 basis, and is used for standing orders, internet and telephone banking payments. Faster Payments settles net, three times every business day in RTGS.
Financial conduct Authority (FCA)	Financial regulatory body in the United Kingdom, but operates independently of the UK government, and is financed by charging fees to members of the financial services industry.
FinTech	Portmanteau of Financial Technology that describes an emerging financial services sector in the 21st century and includes any technological innovation in the financial sector, including innovation in financial literacy and education, retail banking, investment and even crypto-currencies like bitcoin.
GDPR	General Data Protection Regulation. Regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).
ISO 20022	An international standard for the development of financial messages which ICS will be the first UK payment scheme to adopt.
Know Your Customer (KYC)	Process of a business, identifying and verifying the identity of its clients.
4th EU Money Laundering Directive (MLD4)	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and

	repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, published in the Official Journal of the EU on 5 June 2015.
New Payments Architecture (NPA)	The NPA Design Hub has been established by the Forum to progress the detailed design of the New Payments Architecture ahead of the handover to the New Payment System Operator (NPSO) by the end of 2017.
New Payment System Operator (NPSO)	The new PSO which will be made up of BPSL, C&CCCL and FPSL.
Open banking	PSD2 introduced the concept of open banking which allows third party developers to build applications on the back of open APIs connecting to financial institutions.
Payee	A person who is the intended recipient of transferred funds.
Payer	A person who holds a payment account and allows instructions to be given to transfer funds from that payment account, or who gives instructions to transfer funds.
Pay All	Request to Pay Response Option: Accept a request for payment and proceed to initiate a payment equivalent to the total amount (or more when allowed) asked for in a request.
Pay Partial	Request to Pay Response Option: Accept a request for payment and proceed to initiate a payment equivalent to a portion of the amount asked for in a request, this can be done multiple times.
Payment Channel	A method of payment used to pay for a request. Different Payees would accept different channels, this also includes cash.
Payment Execution	Processes the payment at the payee's or the payer's ASPSP account and manages payment execution.
Payment Service Provider (PSP)	A Payment Service Providers can be any of the following when carrying out payment services; authorised payment institutions, small payment institutions, registered account information service providers, EEA authorised payment institutions, EEA registered account information service providers, electronic money institutions, credit institutions, the Post Office Limited, the Bank of England, the European Central Bank, and the national central banks of EEA States (other than when acting in their capacity as a monetary authority or carrying out other functions of a public nature), government departments and local authorities (other than when carrying out public functions) and agents of Payment Service Providers and excluded providers.
Payment Strategy Forum (PSF)	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 Method	The way that a buyer chooses to compensate the seller of a good or service that is also acceptable to the seller.
Payment Window	The period of time between a request being received and the date that a request must be fully paid by.
Phishing	Is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Payment Initiation Service Provider (PISP)	An organisation that connects the merchant and bank's online banking platform with the intent to facilitate a credit transfer Payments Messaging: A communication channel that facilitates the exchange of non-clearing messages (e.g. reports and adjustments) between the ASPSP and the clearing function.
Payment system Operator (PSO)	A company that operates one or more schemes. All PSOs are regulated by the PSR and additionally certain PSOs are supervised by the Bank of England.
Payment Services Directive2 (PSD2)	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, published in the Official Journal of the EU on 23 December 2015.
PSP	'Payments Service Provider'. Includes the banks, building societies, credit unions and electronic money and payments institutions.
Pull payments	Payments where the person who is due to receive the money instructs their bank to collect money from the payer's bank. Can be authorised or unauthorised.
Push Payments	Push payments are payments where a customer instructs their bank to transfer money from their account to someone else's account. Can be authorised or unauthorised.
Request Payment Extension	Request to Pay Response Option: Request a Payee for an extension to the payment window to give you more time to pay a request.
Real-time balance	Account balance that does not require any waiting period after a transaction happens to get updated. It allows the account holder to determine how much money they have at any point in time.
Real-time payment	A payment transaction that does not require any waiting period to be executed.
Request	Message sent from Payee to Payer with the intention of requesting for a payment to be made.
Response	Choice made by a payer to a request sent by a payee that is then communicated back to the Payee.
Real-Time Gross Settlement (RTGS)	The accounting arrangements established for the settlement in real-time of sterling payments across settlement accounts maintained in the RTGS system.
Service Level Agreement (SLA)	It is a contractual agreement between a service provider and end-user that defines the conditions and level of service expected from the service provider.
Service provider	A payments service provider is technical provider of payment services or the technical infrastructure required to facilitate a payment service. This includes vendors, infrastructure providers, and Technical Payment providers.
Small and Medium sized Enterprises (SMEs)	Any business with fewer than 250 employees.

Third Party Service Provider (TPSP)	TPSPs provide services across the payments value chain to facilitate the processing, acceptance, management and/or transmission of payments, as well as provision of information (e.g. technology providers, telecommunication providers, payment gateways/platforms, point of sale terminal providers, fraud management services).
Unauthorised payment	A payment made without the customer's consent – for example, a payment made due to a bank error or one made using a stolen payment card.
United Kingdom	Is comprised of Great Britain and Northern Ireland.

Table 52: Glossary