payments strategy forum

July 2017

Collaborative Requirements and Rules for the End-User Needs Solutions

Supporting Document

Project/Programme Manager:	Duncan M. Ng'enda
Sponsor:	Payments Strategy Forum
Date of Final Approval:	21 07 2017
Approved by:	Sian Williams

Version / Document History

Version No	Date	Authors	Comments
1.0	21 Jul 2017	Duncan M. Ng'enda Ignacio Badiola Sean Doherty Tanuja Kanade Emilie Akiki	Final Version

Contents

Purpose of this Document

This document presents the work carried out by the User Requirements and Rules workstream (WS01) of the Payments Strategy Forum. It is meant to be a supporting document to the Blueprint paper published for consultation on the 28th of July and should be read in tandem.

The consultation document is available at: https://implementation.paymentsforum.uk/consultation

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 focussed on solving detriments identified as befalling 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. 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.

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. The three components: real-time balance, confirmation of payee and payments status & tracking, make up the components of the Assurance Data solution.

The Enhanced Data solution 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 spur 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 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 purview 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 where the end-user was placed at the very centre. We validated and involved various end-users through our core advisory group made up of end-user experts, intense workshops with end-users and one-on-one interviews. The design 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, associated requirements and rules have been defined. Our work was deliberately restricted to the definition of the core set of use cases only and we expect 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 created end-to-end journeys that illustrate the component stages of each of the solutions in a nut shell.

[1] General Data Protection Regulation.

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 misdirects will be diminished; a governance mechanism that ensures competitive players offering these solutions meet the base requirements stated herein. These enablers highlighted form part of a more complete set detailed in this document with an accompanying recommendation.

This document serves as the main supporting document to the Consultation. It should be read in tandem where more detail is required over and above that presented in the Consultation Document.

As an immediate next step, in parallel with the consultation process, we will carry out workshops with stakeholders in an attempt to achieve an industry wide position on data protection implications that affect each of the solutions. The lack of a common interpretation of the data protection regulations has been identified as an adoption risk for Confirmation of Payee and Enhanced Data. In addition, consultation responses received may result in conducting further work yet to be defined. The output of these will be incorporated in the subsequent issues of this document.

The cumulative output of our working group will be a final report for handover to the New Payment System Operator (NPSO) for further implementation and detailing as part of the New Payments Architecture. In the interim, the requirements, rules and recommendations will provide a base template for existing solutions that are currently in development on existing infrastructure.

1 Introduction

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

1. '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.
2. '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.
3. '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, 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.

The 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, 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 on 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 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, predictability in their nature with an assured certainty of outcome throughout the process including when they fail. EUN solutions should offer 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 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.

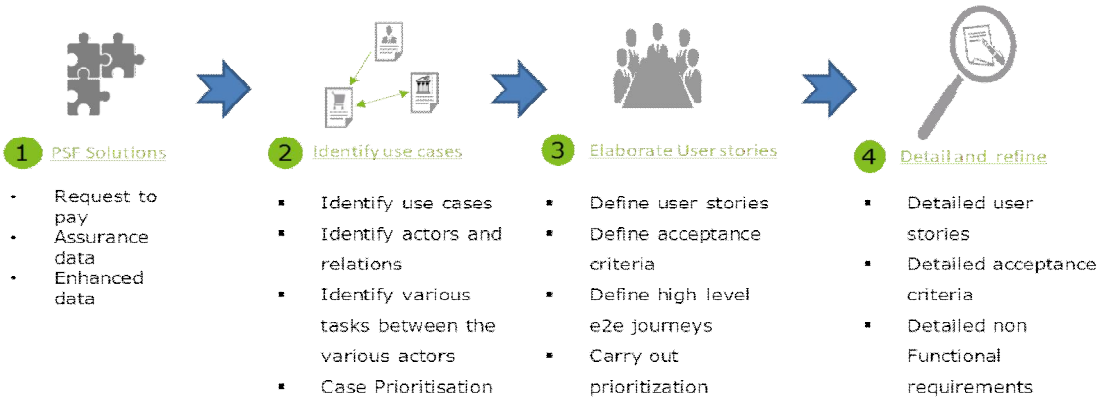


Figure 2: Requirements Approach

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 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 dictates the development of requirements and rules only for essential use cases necessary to address the detriments that the Forum set out to address 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 5.

[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

3.1 Background

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 designed a Request to Pay service that specifically addresses these detriments.

3.2 Detriments Addressed by Request to Pay

Request to Pay aims to solve for 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

3.3 Scope

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

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

3.4 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 will not be defining requirements and rules for the competitive cases.

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

Payee Use Cases Overview

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

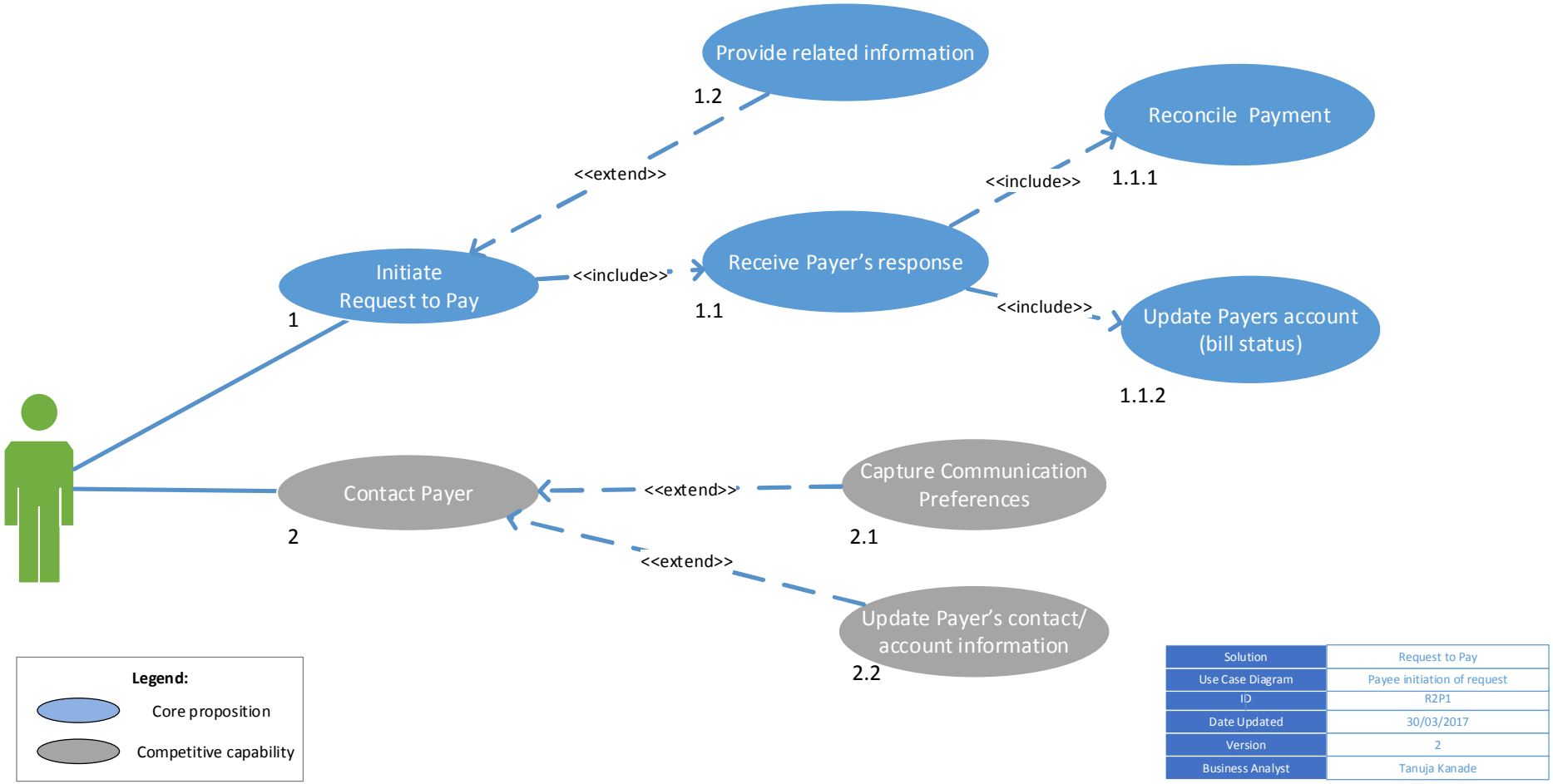


Figure 3: Request to Pay Payee Use Case Diagram

Payer Use Cases Overview

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

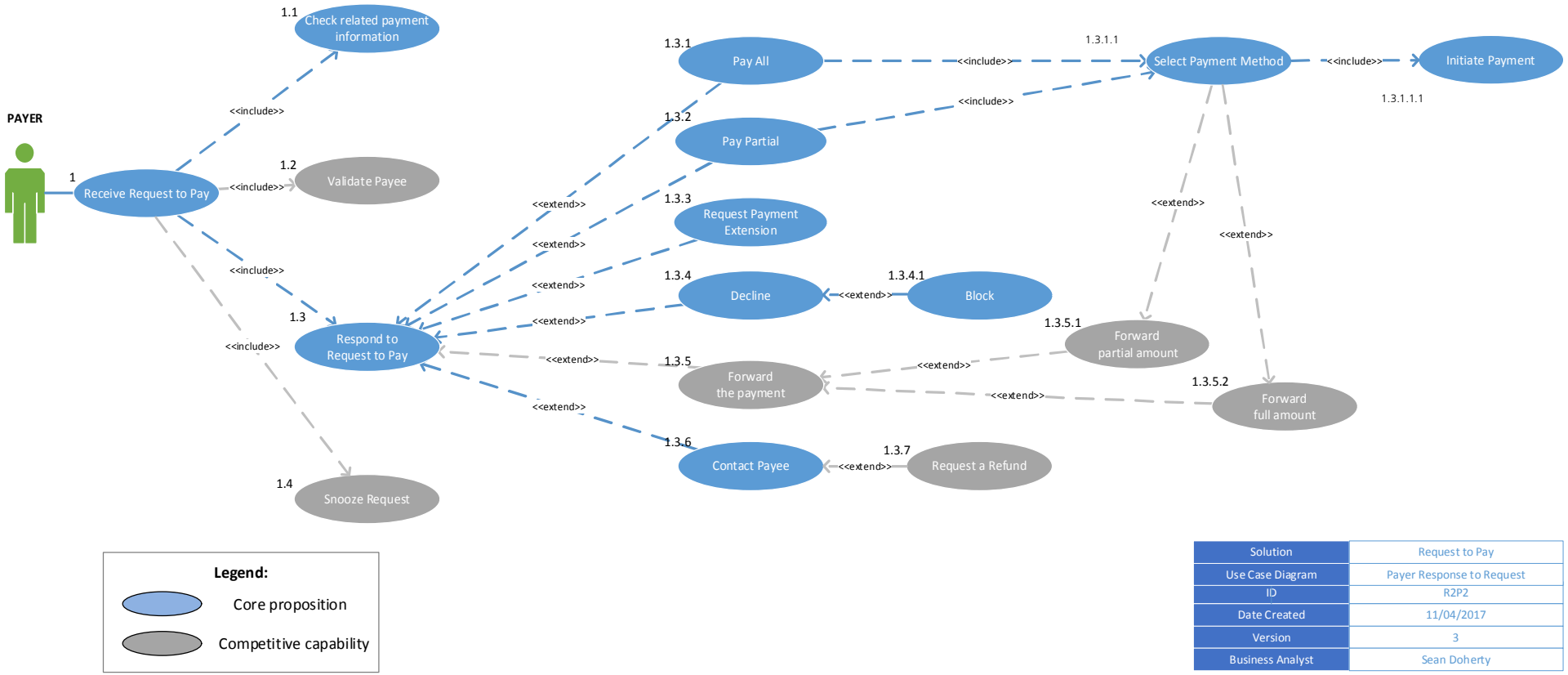


Figure 4: Request to Pay Payer Use Case Diagram

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

3.5 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.

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 pays me. 2. Initiate a Request to Pay through the payer's preferred communication channel, so that I can increase the likelihood of them receiving the request. 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 by 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.

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.

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 to 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.

2.4 Decline

	As a payer, I want to be able to:
Choose to decline the 'Request to Pay' message	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.

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[5] and payee's information transferred automatically[6] from the request to the payment so that this reduces the need to re-enter the payment's information manually.

3.6 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.

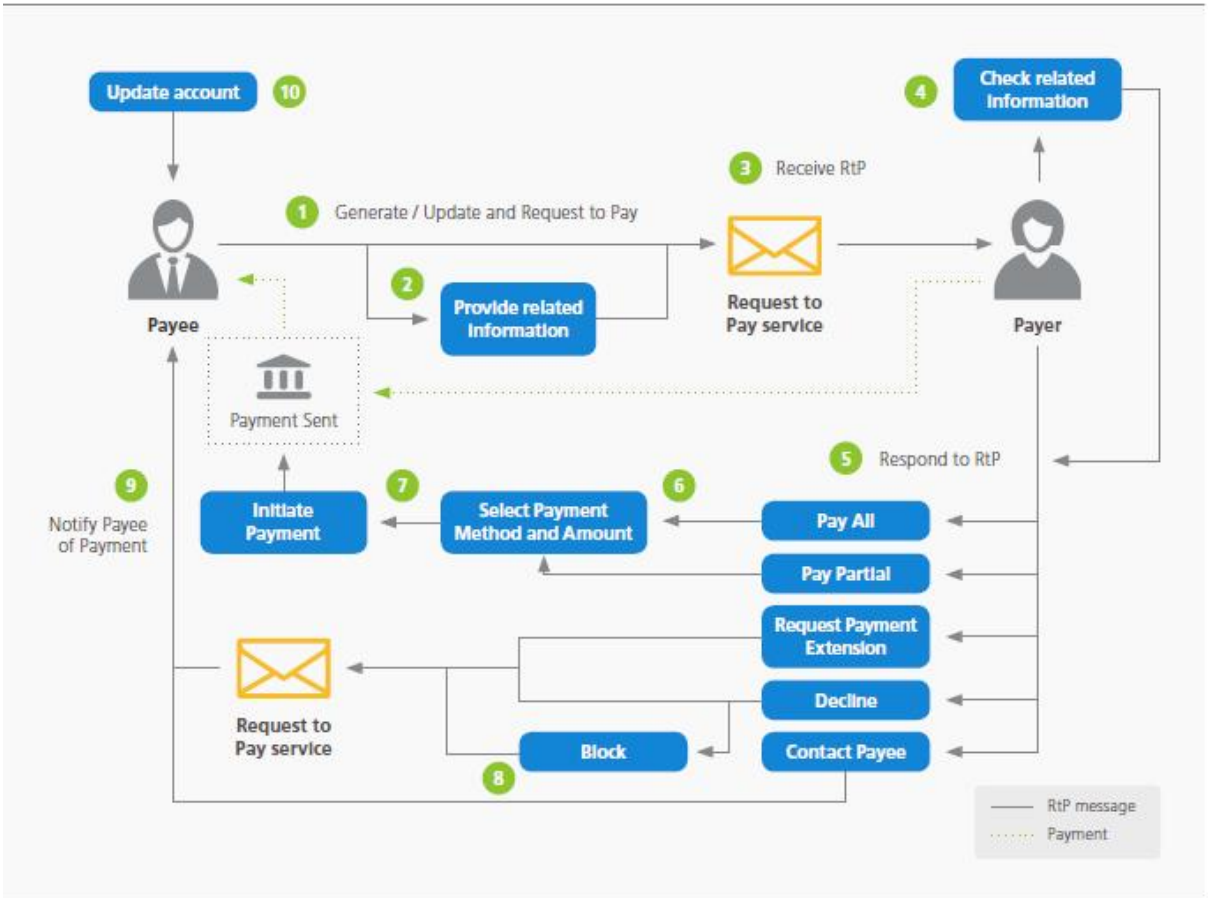


Figure 5: Request to Pay End-to-End Journey

[5] Request information including the reference ID.

[6] 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.

#	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

3.7 Assumptions

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

ID	Title	Description
001	On boarding	It is assumed that to use Request to Pay, payers and payees alike will need to go through an on boarding 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

3.8 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.	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 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 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.

3.9 Dependencies

To successfully deliver the Request to Pay service described, several dependencies were identified. These are summarised in Table 9:

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	On boarding	Payer on boarding/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 on boarding 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 9: Request to Pay Dependencies

4 Assurance Data

4.1 Background

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[7], and the delivery status. This increases end-users' confidence. We proposed a suite of tools collectively called Assurance Data; this 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.

4.2 Detriments Addressed by Assurance Data

The key detriments addressed by the Assurance Data solution are listed in Table 10:

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.
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.

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

ID	Detriment Group	Detriment
30	Customer identity, authentication and knowledge	The industry needs to better understand who the payment recipient (payee) is and the beneficiary account.

Table 10: Assurance Data Detriments

4.3 Scope

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 11: Assurance Data In-Scope

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 12: Assurance Data Out of Scope

4.4 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 6 and 7. 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 13 and 14 providing a short description for each of them.

Payer Use Cases Overview

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

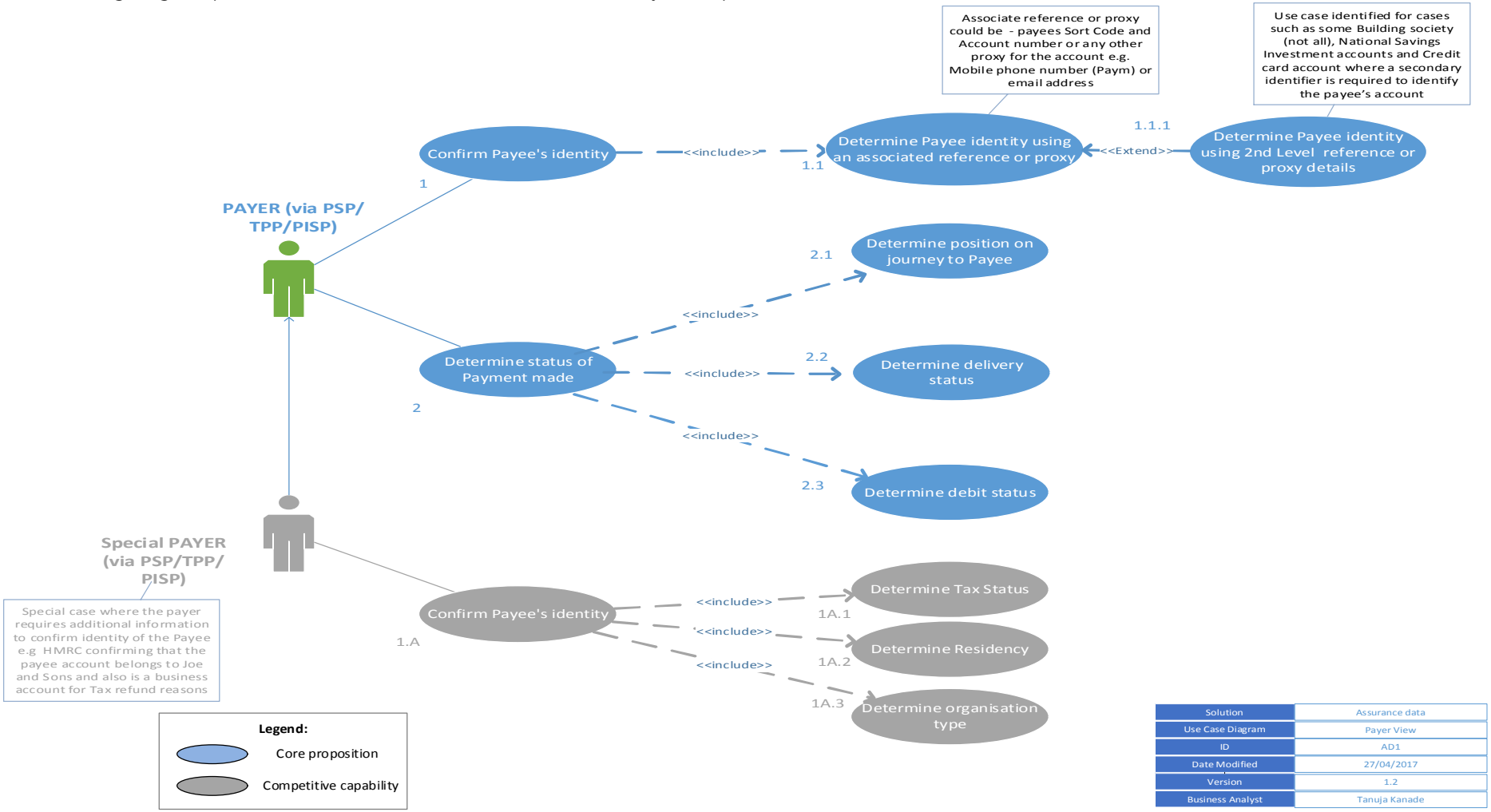


Figure 6: Assurance Data Payer Use Case

Payee Use Cases Overview

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

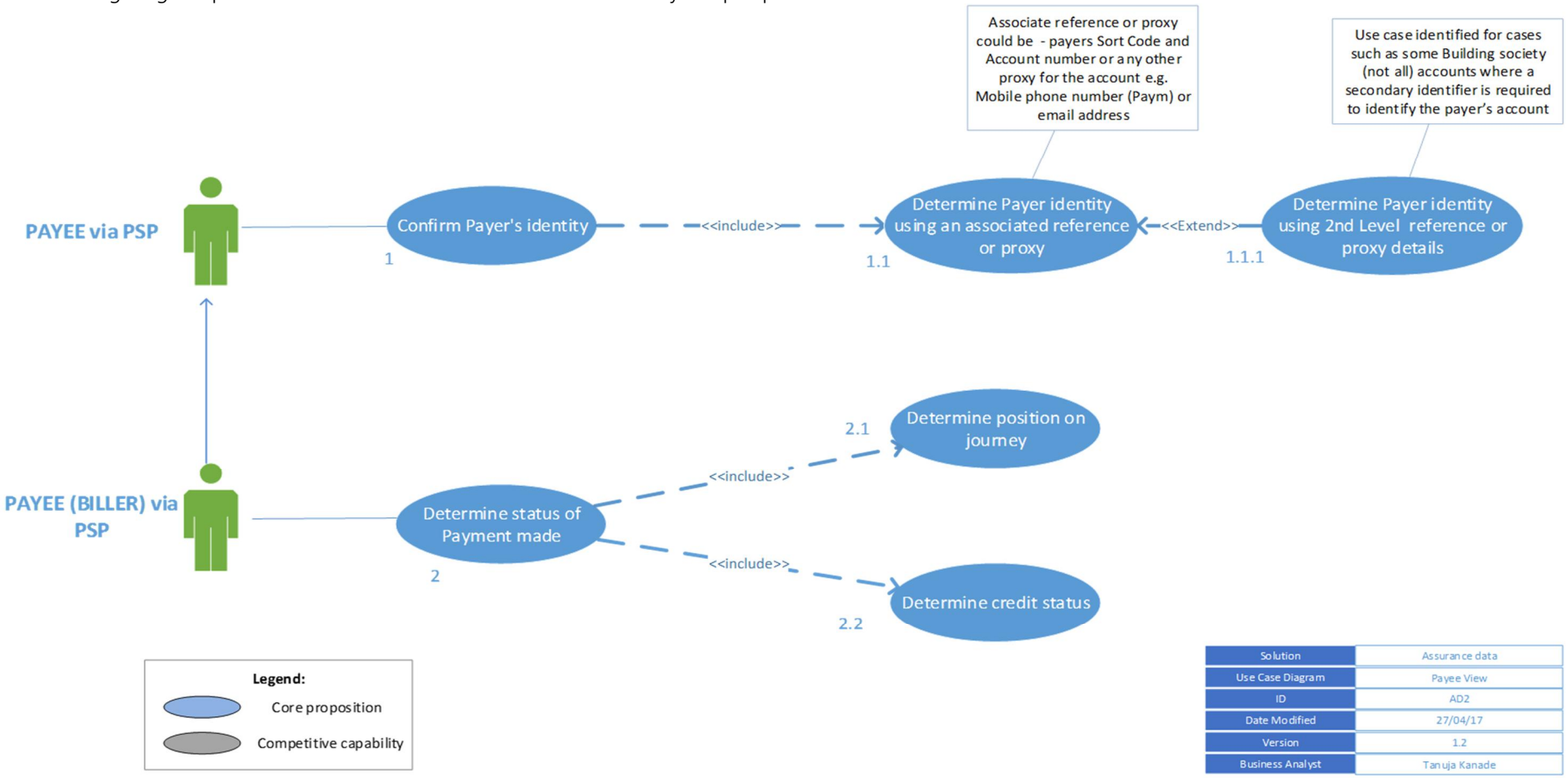


Figure 7: Assurance Data Payee Use Case

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 13: Assurance Data Payer Use Case

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, seeks 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 14: Assurance Data Payee Use Cases

4.5 High-Level User stories and Rules

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.

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.

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. 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 in 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).

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 in 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 resultant change in balance.

4.6 Proposed End-to-End Journeys

Confirmation of Payee

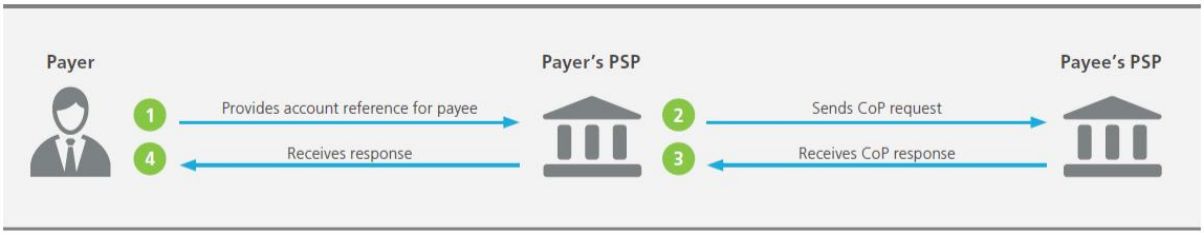
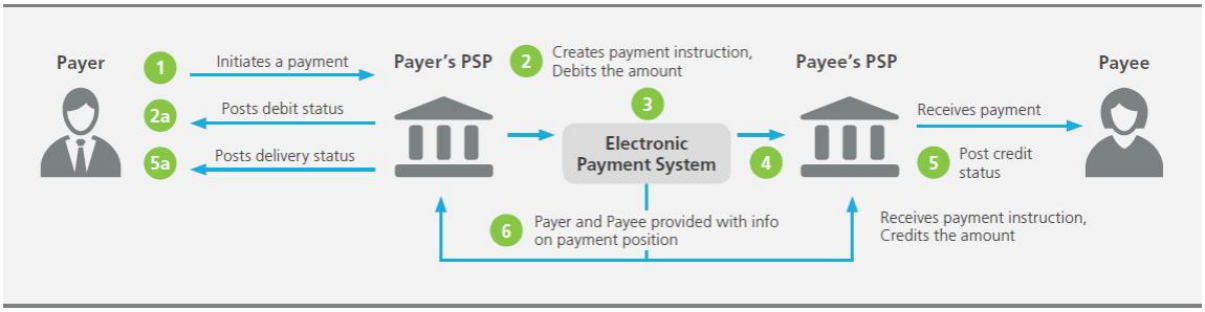


Figure 8: Confirmation of Payee End-to-End Journey

#	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.[8]

Table 15: Confirmation of Payee End-to-End Journey

Payment Status and Tracking



[8] Payer is always in control.

Figure 9: 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 16: Payments Status Tracking End-to-End Journey

4.7 Assumptions

#	Title	Description
001	Governance	The CoP service is mandatory for all the PSPs/TPSPs.
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 17: Assurance Data Assumptions

4.8 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 18.

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 risk in the provision of information on a payment's status and tracking. PSPs must comply with this regulation whilst they provide Payment status and tracking capability to payers.	Service providers must ensure that the design is compliant with this regulation.
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 18: 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:
    a. 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.
    b. 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.[9]

3. **End-user interface design and experience:** CoP and Payment Status Tracking service providers will be tasked with determining the best way to present 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.

4.9 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	Ubiquity of the CoP service is dependent on the majority of the industry participation including PSPs and consumers.

Table 19: Assurance Data Dependencies

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

5 Enhanced Data

5.1 Background

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[10] 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,[11] 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 parties that specifies the input, format, carriage, access of 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.

[10] 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.

[11] 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.

5.2 Detriments Addressed by Enhanced Data

Enhanced Data aims to solve for 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 20: Enhanced Data Detriments

5.3 Scope

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 21: Enhanced Data In-Scope

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 scope of its work.

Table 22: Enhanced Data Out of Scope

5.4 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 10 and 11. 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 23 and 24 providing a short description for each use case.

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.

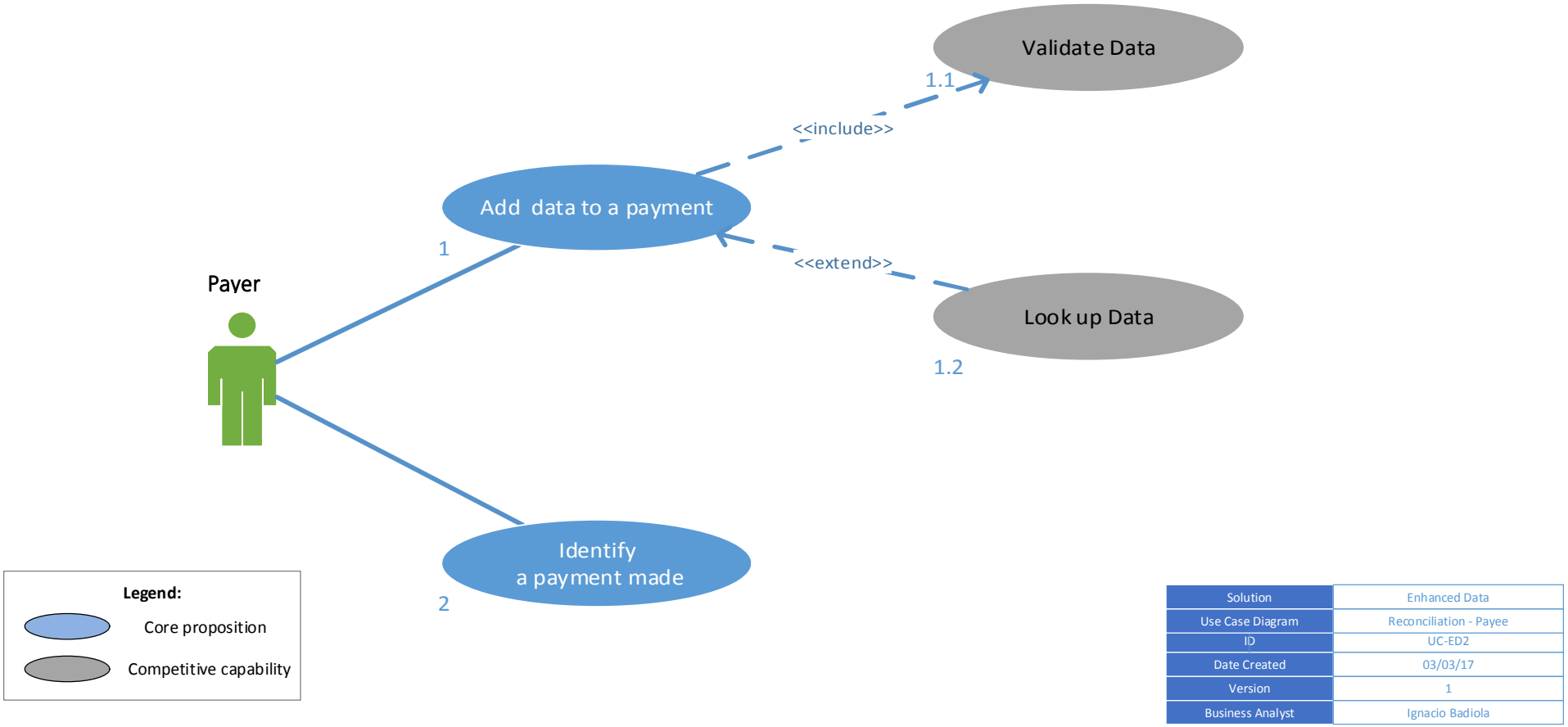


Figure 10: Enhanced Data Payer Use Case

Payee Use Cases Overview

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

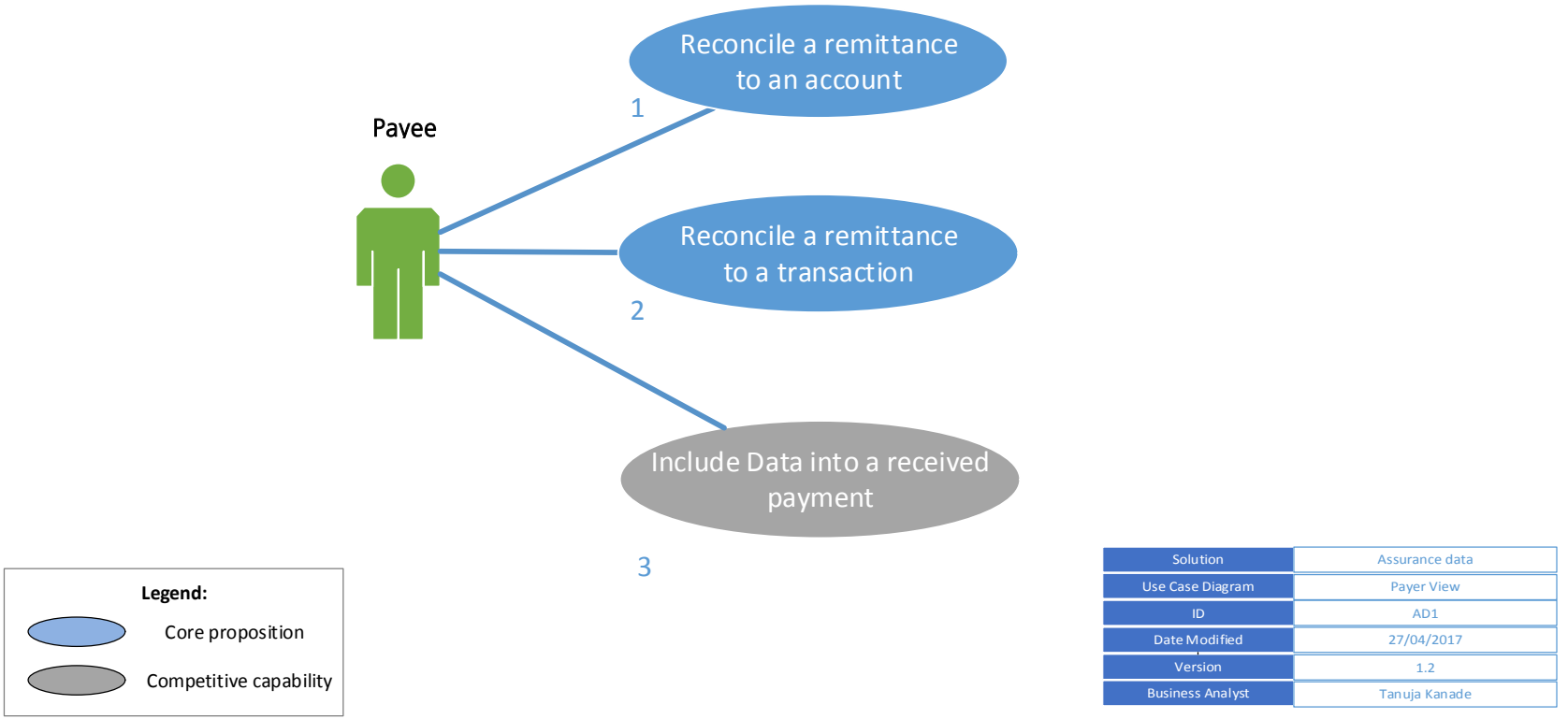


Figure 11: Enhanced Data Payee Use Case

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 23: 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 24: Enhanced Data Payee Use Cases

5.5 High-Level User Stories and Rules

The primary end-users of Enhanced Data will be the payer and the payee. However, with the roll out 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 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. 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.

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.

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[12] 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[13]. 3. All legal and regulatory requirements must be complied with at every time by all data processors and data stores[14].

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

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

[14] 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.

5.6 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.

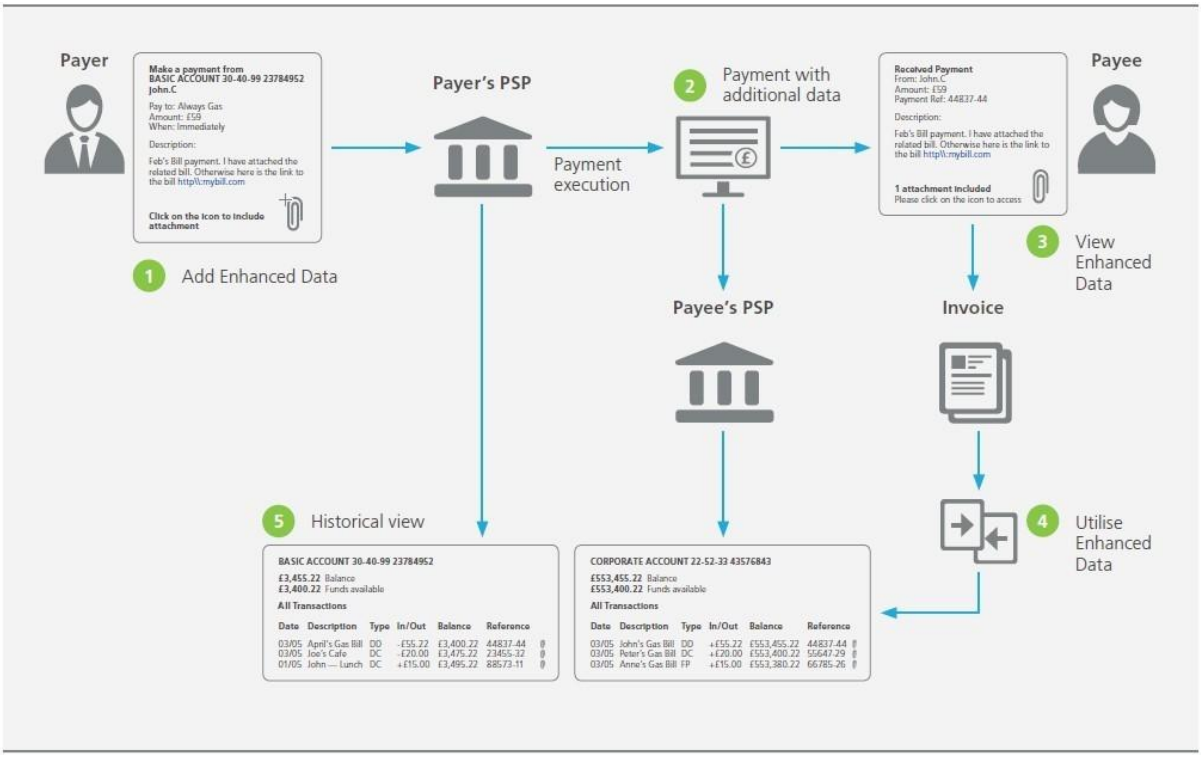


Figure 12: Enhanced Data End-to-End Journey

#	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 25: Enhanced Data End-to-End Journey

5.7 Assumptions

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

Table 26: Enhanced Data Assumptions

5.8 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 27.

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 for 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 27: 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.

2. **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.

5.9 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 28: Enhanced Data Dependencies

6 Appendices

6.1 Appendix 1 – 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.

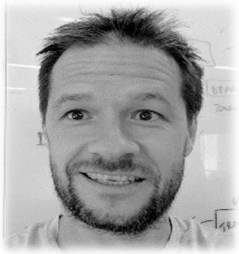
Carl Pheasey

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

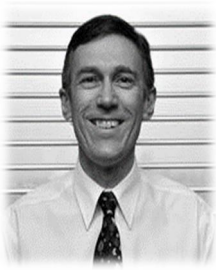
Joining Capacity: Subject Matter Advisor - Advisory Group

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.

6.2 Appendix 2 – 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&CCL 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)	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.

6.3 Appendix 3 – 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.

6.4 Appendix 4 - 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 the already successful commercial Pingit service.
- 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.

6.5 Appendix 5 – Stakeholders Log

Table 29 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
Pauments UK	Scheme	15/02/2017	Payments UK (2 TMS)	Colateral Review - Overview of existing solution work	1. Request to Pay 2. Assurance Data 3. Enhanced Data	Nick Rucker
Vocalink	Soution Vendor	22/02/2017	EY (25 CP)	Solution Presentation	2. Assurance Data	1. Michael Kitt 2.Marc Corbalan 3.Richard Luff
Faster Payments	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

Stakeholder's name	Stakeholder Type	Date of session	Location	Subject	Solution Reviewed	Representative
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
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
Age UK	Charity	17/05/2017	Age UK -Travis House, London	EUN Requirements Review	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Lucy Malenczuk
NPA - WS2		22/05/2017	2 TMS	End-to-End Journeys	1. Request to Pay 2. Assurance Data 3. Enhanced Data	WS2
Nationwide	PSP	25/05/2017	Phone call	Request to Pay	1. Request to Pay	1. Martin French
ICO	Regulator	09/06/2017	EY (25 CP)	Data Protection	1. Request to Pay 2. Assurance Data 3. Enhanced Data	1. Richard Syers

Table 29: WS1 Communications Log