payments
strategy
forum

Blueprint for the Future of UK Payments

A Consultation Paper – July 2017

Contents

Foreword from the Chair

The Forum represents the first time all stakeholders who have an interest in payments in the UK have worked together to plan for a future that meets the needs of all users. To this end we have ensured that the voice of the user is at the heart of our deliberations.

In November 2016 we set out an ambitious vision for the future of UK payments. One that will deliver simpler access, greater innovation, increased adaptability, improved competition and better security. We focussed on simplifying governance, leveraging existing industry activities and modernising our technology. Through these changes our payment systems will be ready to meet the needs of users, both now and in the future.

This document brings together our design work developed during this year for public consultation. We have worked hand in hand with the Payments Community to develop a draft Blueprint for the New Payments Architecture. We have set out a detailed design and implementation approach for a new payment system for the UK. We have developed requirements and rules for the three solutions users have told us they needed, namely Request to Pay, Assurance Data and Enhanced Data. We have completed the design work on four of our seven financial crime solutions and have started the handover to the industry bodies that will carry them forward to completion.

Over the next six months we will review your feedback and finalise our designs. By the end of 2017 we will hand over the final Blueprint to the New Payment System Operator to implement. In parallel, we will complete the handover of the financial crime solutions, with clear plans and accountability in place.

I would like to take this opportunity to thank all those who continue to support the work of the Forum. Over two years, the Payments Community has grown to over 645 individuals, representing 360 organisations, including consumer groups, businesses, Government, Payment System Operators, Payment Service Providers and FinTechs. Our work would not have been possible without your engagement, support and expertise.

It is now over to you. We want to hear your views. We hope that you will join us through this consultation to help refine our thinking as we transform payments systems in the UK for the benefit of everyone who uses them.

Ruth Evans, July 2017

Executive Summary

1. Introduction

Payment systems in the UK are some of the best in the world, performing a critical function for the economy and supporting our day-to-day lives. They are, however, no longer fit for purpose in the 21st century, and their age and complexity make it increasingly difficult for the industry to innovate to meet the changing needs of a diverse group of users.

In November 2016, the Forum published its Strategy.[1] It set out a bold vision for the future of UK retail interbank payment systems that will enable simpler access, ongoing stability and resilience, greater innovation and competition, increased adaptability and better security to meet the needs of current and future generations of payment service users. To achieve our vision we identified 17 solutions.[2]

In particular, we proposed:

- The development and implementation of a New Payments Architecture (NPA) to introduce effective competition between providers of payment services, composed of a layered structure to make it easier for innovation to occur at a quicker pace. It will also provide security, stability and resilience.
- The consolidation of the three main UK retail Payment System Operators: Bacs Payment Schemes Limited (BPSL), Cheque and Credit Clearing Company Limited (C&CCCL) and Faster Payments Scheme Limited (FPSL). A PSO Delivery Group (PSO DG) was established by the Bank of England (BoE) and the Payment Systems Regulator (PSR) to plan the consolidation of the three PSOs into a single entity – the New Payment System Operator (NPSO). The plan has been articulated in the PSO DG report issued in May 2017.[3] The NPSO will take ownership of the NPA design and implementation at the end 2017.
- A set of solutions to help prevent or reduce the impact of financial crime on users.

Since publication of the Strategy, we have focussed on the design and implementation of our solutions in order to deliver end-user benefits and address detriments as soon as possible.

This document builds on the proposals consulted on in 2016 and set out in our Strategy. In developing this document we have engaged a wide range of stakeholders who represent the opinions of various sectors. A list of organisations are included in Appendix 10.

We believe that there is significant financial and social benefit for the UK that can be achieved by implementing our Strategy.

2. The New Payments Architecture

The Strategy concluded that a new architecture is required to meet the changing expectations of users and to create an environment flexible enough to meet future needs. Over time, the new architecture will replace the inherent complexity of running Bacs, Cheque and Credit, and the Faster Payments Service in parallel. To do nothing is not an option. The remedies outlined in the PSR's recently published Infrastructure Market Review (IMR)[4] require the existing Bacs and Faster Payments systems to move to ISO 20022 and be competitively re-procured. The industry could do the minimum required to respond to the IMR, but that would fail to deliver maximum benefits. We are of the view that the best option remains the design and implementation of an innovative New Payments Architecture (NPA).

NPA Design

Our design has been led by the desire to enhance user experiences, address detriments identified in the Strategy and provide a platform for the UK to continue to be a global payments leader.

The key features of the NPA are:

- A layered approach, with a 'thin' collaborative infrastructure to enable competition and innovation.
- A single set of standards and rules with strong central governance.
- Adoption of the common, international messaging standard, ISO 20022, to enable access, innovation and interoperability, both in the UK and potentially for international connectivity.
- Security and resilience, with financial stability a key principle.
- The use of 'push payments' to enable simplicity and increase customer control.
- Flexibility built into the design to support a range of new end-user overlay services such as Request to Pay and Assurance Data (including Confirmation of Payee).

Moving to a new modern architecture based on these key features, alongside PSO consolidation, provides an opportunity to address historical problems of slow innovation, concentration of ownership and control of payment systems.

The combination of a 'thin' centre, overlay services and interoperable standards provides the basis for future payment systems infrastructure to be more agile and flexible than what exists today, while maintaining security, stability and resilience. It aims to drive competition and innovation across the value chain in the interest of users. Where there is demand, there should be the ability to launch new services more quickly. This approach is proven in other industries, such as telecommunications, and is being adopted by other countries as they transform their payment systems.

[1] https://consultation.paymentsforum.uk/final-strategy
[2] A summary on progress can be found in Appendix 1.
[3] https://www.psr.org.uk/psr-publications/news-announcements/PSODG-report-new-payment-system-operator
[4] The "Market review into the ownership and competitiveness of infrastructure provision" https://www.psr.org.uk/sites/default/files/media/PDF/PSR-MR15-2-5-IMR-Remedies-decision-June-2017.pdf

User Requirements and Rules

Three End-User Needs (EUN) solutions were prioritised in the Strategy: 'Request to Pay', 'Assurance Data' and 'Enhanced Data'.

We have developed a minimum set of requirements and rules that any provider of these solutions would have to meet in order to offer them to users. These are anchored around nine principles, shown in Figure 0.1.

When these requirements are finalised, they will be handed over to the NPSO, who will be responsible for administering them. The requirements will serve as a standard to guide the competitive market as rich and compelling propositions are developed for the benefit of end-users.

Options for how the NPA could deliver these solutions have been examined to demonstrate their feasibility and illustrate how the NPA can be deployed and used.

Implementation Planning and Transition

We propose that the NPA is implemented over a period of 5 years, with the first implementation of a push payment capability available at the beginning of 2021. The sequence proposes the migration of Faster Payments traffic first from early 2021, then Bacs from late 2021, and finally Cheque and Credit from the beginning of 2024. It is important to note that existing products and services will continue to be available on the NPA.

Our plan allows for delivery of the EUN solutions on current systems, where possible, in advance of the NPA roll-out. The EUN solutions are based on the minimum set of requirements and rules we have developed. We are aware of competitive, market-led solutions, which could be delivered ahead of 2021.

The payments industry already has a number of related major change programmes underway. Our implementation approach seeks to leverage and align with these programmes where possible. This includes the work done on Open Banking Application Programming Interfaces (APIs); the second Payments Services Directive (PSD2) and the Bank of England's work to deliver a new Real Time Gross Settlement (RTGS) system.

The wider implementation landscape has also been analysed to place the delivery of the NPA firmly within the context of other major initiatives, in particular to identify and manage risks related to concurrently delivering significant change across the industry.

Ongoing availability and stability are critical considerations when moving from current systems to the NPA. Therefore, a transition approach has been set out that will allow dual running of current systems along with the NPA. Dual running will mean that current participants and users can transition over time and can continue or begin to use today's systems without being concerned that they will be 'turned off' as soon as the NPA goes live.

Cost Benefit Analysis (CBA)

We assessed the costs and benefits of adopting the NPA, as well as the three EUN solutions. Our analysis shows that there is a gross benefit opportunity of c. £11 – 14 billion in the period 2019 to 2031. This would not be achievable on our current infrastructure.

FIGURE 0.1 END-USER NEEDS PRINCIPLES

Our estimate of the capital costs of our solutions is c. £1.3 billion, this comprises NPA capital costs and aggregate costs for the three EUN solutions.[5] This results in a discounted net benefit of £6.0 – 7.4 billion after adjusting for up-front and running costs.

In comparison we have considered an alternative minimum upgrade approach of upgrading Bacs and FPS to be minimally compliant with ISO 20022 messaging, which would not deliver the same level of benefit.

Our analysis concludes that the benefit opportunity of delivering the NPA is c.£6.2 – 7.7 billion greater than what could be delivered through an alternative minimum upgrade.

Not all benefits are quantifiable, therefore, the overall benefit to the UK of the NPA is anticipated to be wider in scope than estimated in this study. For example, an important benefit identified by stakeholders is the opening up of the industry to more competition making direct access less onerous to a larger number of aspiring participants, which would not be realised in the alternative minimum upgrade. In addition there are the wider societal benefits of the three EUN solutions, the increased flexibility to support new innovative services, and the ability to make changes more easily, both specific to an institution and at industry level, that the NPA is designed to achieve compared to the alternative minimum upgrade.

The quantitative benefits attributed to NPA adoption and the overlay services in this study should, however, be interpreted as conservative, with substantial potential for greater financial benefit over time.

We have also considered risk when conducting the CBA. Both the NPA and the alternative minimum upgrade require complex industry change and would need to manage similar risks.

In conclusion, we believe that doing nothing is not a viable option, and that both the financial and wider societal benefits of the NPA are significantly greater than the alternative minimum upgrade.

[5] These costs excludes end-user costs such as costs to businesses and government.

Commercial Approach and Economic Models and the role of the NPSO

Different elements of the NPA will be suited to different funding models, depending on whether they are provided through 'competition for the market', that is, the service is better suited to provision by a single competitively selected supplier for a set period of time; or 'competition in the market', where a service is provided competitively at the same time by multiple providers. Our analysis will help to inform the NPSO's decision making on funding for different parts of the NPA.

The NPSO will competitively procure parts of the NPA that are considered to be 'competition for the market'. An example of this could be components of the NPA that relate to clearing and settlement processing. For these elements, the NPSO should consider financing arrangements from new sources, which offer alternatives to how today's systems are funded.

For the elements that are considered 'competition in the market', it is expected that they will be funded by the competitive market and will not require intervention by the NPSO.

The NPSO will maintain standards and rules for the NPA including Open APIs and overlay solutions, which will enable market contestability and interoperability, and facilitate effective competition. Providers of overlay services will need to be 'accredited' by the NPSO according to these rules and standards in order to enter the market.

It is possible that the NPSO may need to perform a 'market catalyst' role if competitive markets are slow to develop. The 'market catalyst' role could include demonstrating proof of concepts for certain services or providing a 'sandbox' environment to encourage entrants to the market. It is anticipated that the NPSO will catalyse the market with a view to services eventually becoming accredited 'competition in the market'.

3. Improving Trust in Payments

Our Strategy proposed solutions to engender user trust in safe and certain payments through collaboratively preventing financial crime. We committed to consult on a subset of solutions, whilst putting in place plans to hand over all activities to appropriate industry bodies[6]. In this document we are consulting on:

Payments Transaction Data Sharing and Data Analytics

In our Strategy, we proposed the deployment of an analytics capability with access to UK payments data to identify criminal money flows between accounts. We have progressed this through a tactical and a strategic solution.

We are consulting on the strategic solution design for a powerful analytics capability of payments data in combination with other information or intelligence (e.g. known fraudulent accounts and Suspicious Activity Reports).

In addition, the tactical solution work has been progressed to provide early benefit in the fight against financial crime in the detection of money mule accounts, and piloting methods for funds repatriation. The tactical solution was handed over in June, and implementation is expected by the end of 2017.

Trusted KYC Data Sharing

We have conducted further analysis on the Trusted Know Your Customer (KYC) data sharing solution, recognising the requirement to balance collaborative solutions with competitive market enhancements.

We have concluded that the sharing of key elements of customer data between financial institutions will improve the speed and efficiency for Payment Service Providers (PSPs) of all sizes in identifying and removing those intent on committing fraud and other financial crime. Our view is that the establishment of a data sharing framework with associated industry governance will lead to a range of competitive value added KYC services being deployed.

4. Next Steps

Over the next 6 months our design and implementation work will continue. We will further develop rules and standards for our EUN solutions and continue to elaborate the design of the NPA.

The finalisation of the Blueprint and other solutions will be informed by the assessment of responses to this consultation. We expect to complete our consultation assessment in late November.

To achieve a smooth transition of responsibility for the NPA to the NPSO by the end of 2017, we will be progressing and agreeing plans for handover as an integral part of our activities for the rest of the year.

By the end of 2017, the NPA Blueprint will be handed over to the NPSO, and our Financial Crime solutions will be handed over to appropriate industry bodies.

Throughout this document, we have posed specific consultation questions. Where questions are pertinent to a subsection of anticipated respondents, we have signposted the questions with the icons below to clarify which are most relevant for your organisations, and where we would most value your feedback. We also welcome input from all respondents on all questions for which they would like to provide answers.

Please use the Consultation Questionnaire to document and submit your responses, which is available for download on the PSF website.[7]

[6] Appendix 8 provides an update on the progress of the solutions handed over.
[7] https://implementation.paymentsforum.uk/consultation

1.0 The New Payments Architecture

This section presents our vision of a New Payments Architecture (NPA). It contains an overview of key elements of the overall conceptual model for the NPA. The conceptual model sets out the relationship between participants, connectivity mechanisms and supporting components.

This section, as a whole, will be of particular interest to Payment System Operators (PSOs), Payment Service Providers (PSPs), Third Party Service Providers (TPSPs), vendors and the Bank of England (BoE). Sections 1.2 to 1.4 are important to all readers since they provide an introduction to the key concepts underpinning the NPA, which will help with understanding subsequent sections.

1.1 Introduction

The Strategy sets out our vision for the future of UK retail interbank payment systems[8] to enable simpler access, ongoing stability and resilience, greater innovation and competition, increased adaptability and better security, to meet the needs of current and future generations of Payment Service Users (PSUs).

To achieve this vision, we proposed the New Payments Architecture.

The NPA will introduce effective competition between providers of payment services, and the layered structure will make it easier for innovation to occur at a quicker pace. The NPA will also provide security, stability and resilience, and bring substantial benefits to payment industry participants and end-users.

1.2 NPA Design Principles

The Strategy sets out a set of core design principles to underpin the NPA. The principles, extended into design outcomes, have guided the NPA development journey as shown in Table 1.1.

TABLE 1.1 NPA DESIGN PRINCIPLES AND OUTCOMES

Core Design Principle	Design outcomes
1. A single set of standards and rules with strong central governance	The NPSO will be the central body that governs the NPA, including setting of standards and rules, such as for overlay services, and for technical considerations, such as security. It will also be responsible for: registration and certification of overlay service providers; defining and maintaining the standards for NPA operation.
2. End-to-end interoperability (including Application Programming Interfaces and a common messaging standard)	The NPA design is predicated on the establishment of a common set of standards to provide interoperability between NPA layers and participants. This will be achieved by: a. Setting clear boundaries for, and separation of, architectural layers. b. Recommending ISO 20022 as the payment messaging standard. c. Support for transitioning methodologies.
3. A collaborative infrastructure, allowing multiple providers of overlay services to compete in the market simultaneously	Existing payment systems are operated as individual schemes with single service providers and access mechanisms. Our approach to the NPA design is to facilitate competition for services, and allow multiple vendors to operate services. This is achieved by: a. Taking a vendor agnostic design approach. b. Specifying a push payment model for all payment types. c. Adopting industry-wide standards and approaches.
4. The need to ensure our payment systems are secure and resilient, with financial stability as a key foundation	The NPA is bound by security and resilience requirements similar to existing payment systems, and financial stability must be enforced. The design proposition takes these requirements into consideration and mandates the following: a. A common security standard. b. Using the Bank of England's RTGS system for settlement; ensuring settlement can always complete. c. The status of a transaction will always be known.

[8] CHAPS, Card Payments and LINK are out of scope for the NPA design.

1.3 NPA Attributes

In the Strategy, we recommended that the NPA should adopt the following dimensions.

Layered Approach

Currently it is very difficult to make changes to payment systems without impacting all who use them. Multiple participants (some of whom will be competitors) have to collaborate on changes and agree joint approaches to implementation and testing. It makes the current systems slow to change and acts as a brake on innovation. To address this, we recommended a layered approach.

A layered model is one in which capabilities are separated into discrete layers. Each provides a defined function or part of the payment value chain, based on an agreed standard. 'Upgrade paths' for the components split across layers will be simplified and each layer can be changed with minimal impact on other layers. Different providers can compete for the delivery of the components within a layer, some layers may support multiple providers delivering services at the same time.

This approach fosters competition, innovation and ease of access to new entrants. It also reduces systemic risk, service outages and overall costs. The reduction is achieved through standardising interfaces and systems.

Overlay Services

A payment involves the transfer of value from a payer to a payee. The exchanges between the payer and payee do not technically need to be part of the underlying payment mechanism. The exchanges and supporting data can be delivered through overlay services.

The NPA has been designed to facilitate the emergence of PSP overlay services and end-user overlay services. These applications will 'plug' into the NPA system to provide 'core' and 'additional' services. The additional services are likely to be tailored to particular payment use cases and end-users.

TPSPs will make use of the accessibility of the layered model to provide end-user overlay services, such as Request to Pay and Confirmation of Payee (CoP). PSPs will also be able to provide both end-user and PSP overlay services. We anticipate a high level of innovation within this layer.

Common Messaging Standards

Common messaging standards are necessary to enable interoperability between payments systems and reduce complexity. In our Strategy we recommended the adoption of ISO 20022 to align the UK with global standards and modernise the UK's payments infrastructure.

We expect the use of ISO 20022 as the common messaging standard to deliver national interoperability and potential for international connectivity (e.g. SEPA immediate payments). Standardising messaging formats will reduce complexity and provide the basis for functional enhancements and innovation. It will also reduce future development and integration costs. The ability of ISO 20022 to support the delivery of enhanced data and the tracking of payments and their status are additional benefits.

'Push' Payment Model

In our Strategy, we proposed the use of a push payment model for all NPA payments to provide simplicity and increase customer control. Today in the UK, push payments (e.g. Faster Payments) work alongside a pull payments model which supports services such as Direct Debits.

During the design phase of the NPA, the concept of a push only payments model has been developed further to assess whether our proposition is suitable in light of the Forum's commitment to enable competition, innovation and minimise risk in payment systems.

In summary, we concluded that a push only model offers many advantages but recognise that for some in the industry, changes will be required to enable them to deliver existing pull based payments products, such as Direct Debits. We have set out our view on the benefits and challenges on page 10.

A transition approach has been defined to minimise impact on existing providers and is set out in Section 8.5.2. It gives time to TPSPs, including current independent software providers, bureaux and gateway providers, to update their systems. This transistion approach enables existing payment formats to continue over the NPA with limited or no negative impact on the current users of services such as Direct Debit.

Overall we believe that the push payment model provides a number of benefits and we do not see a significant impact on the overall risk of undertaking payments by moving to a push-only model. It is on this basis. Therefore that we have continued to base the NPA on a push only approach.

TABLE 1.2 PUSH ONLY MODEL BENEFITS AND CHALLENGES

Category	Benefits	Challenges
Customer Control	• NPA facilitated mandates will offer customers a greater degree of flexibility and control. • Commercially, customers' payments can be protected by a refund guarantee as they are today under the Direct Debit scheme. • Given that the NPA will give more control to the customer when making a Direct Debit payment, there will be fewer instances of collection errors requiring an indemnity claim. • Push payments support features such as variable amount and variable dates for collection as provided for today by Direct Debits.	• The delivery of a new payments system will require contractual customer consent and clear responsibilities for payment liability to be established.
Systems and Processes	• A consistent and simplified payments delivery approach through the use of one payment mechanism with a single set of messaging, APIs, standards and connectivity for all payment types.	• As payment messaging moves to ISO 20022, there will be a need for end-users to upgrade to ISO 20022 or establish, via a TPSP, a service that translates messages from existing formats to ISO 20022. • In this latter case an end-user, such as a utility company, could continue to create their existing collection file via their billing system with limited or no internal technical changes needing to be applied. They would forego the benefits of some new services such as Enhanced Data when using a translation service. • Service providers and vendors that currently provide a bureau service or software solutions to collect Direct Debit payments on behalf of an end-user will need to redevelop their technical solutions for payment collection and submission. These changes will allow them to disaggregate payment files into individual PSP files and support the Confirmation of Payer service or provide new added value services to their customers.

Category	Benefits	Challenges
Operational	• Where there are insufficient funds in the normal cycle, customers and payees can be notified early and customer correction payments can be made on the same-day. • Direct Debit payments will be initiated by the payer as a push payment which is consistent with other payments such as a single immediate payment or a standing order. All payments submitted for clearing will be authorised by the PSP who holds the payer's account. This will result in reduced operational overheads as all payments submitted for clearing will be authorised by the institution where the payer has an account, therefore there would be no need for an 'unpaids' process. In addition, in cases where the payments fail due to lack of sufficient funds, notification and remediation by PSPs and end-users will be much quicker in comparison to current processes. • Push payments may enable the reduction of clearing and settlement time for unattended (mainly bulk) payments. • Enables flexible settlement cycle capability in the future.	• A Direct Debit payment that cannot be applied due to insufficient funds will be rejected as a failed payment using the NPA push payment model. • However the customer and the payee can be notified on the same day and therefore earlier than with the current 3 day cycle. This greatly improves the PSP's payment exception process for unpaid Direct Debits. • There will be a more involved collection process on the payee receiver side which will be required to receive the funds from multiple payers.
Participant Innovation Benefits	• A simplified payment mechanism underpinned by a common set of APIs and messaging will provide current and future TPSPs with increased scope for innovation and the development of more competitive propositions for end-users.	

Question 1.1

Do you agree with our recommendation to move towards a 'push' payment mechanism for all payment types? If not, please explain why.

Question 1.2

In the proposed transition approach it is expected that Third Party Service Providers including current independent software providers, bureaux and gateway providers will update their systems to enable existing payment formats to continue to operate with limited or no negative impact on the current users of services such as Direct Debit.

As a PSP or TPSP, do you agree we have identified the implications of adopting a push model adequately? If not, please set out any additional impacts that need to be considered.

Stable Transition Model

Payments are of national importance and system stability is critical. The NPA has been designed to support the transition from current schemes with minimal risk and service disruption by avoiding a 'big bang' launch and ensuring payment interoperability on 'Day 1'. We have defined a clear transition roadmap to allow existing payment systems to co-exist during the transition period with parallel running of the current and new systems. Please refer to Section 3 for more detail on the transition approach.

Common Security Standard

The UK payments infrastructure is highly regarded globally for good security, relatively low fraud levels and high overall resilience. The design of the NPA will focus on maintaining these standards and intends to improve them in the future.

We expect the NPSO to mandate a common security standard for all participants of the NPA, thus providing security, resilience and stability across a more open payments architecture. The standards and recommendations from the PSD2 will be incorporated into this common security standard. Where relevant and possible, we expect to use the security functions being developed by Open Banking to minimise delivery and operational impacts.

Alignment to Key Regulatory and Payments Industry Initiatives

The design of the NPA has taken account of ongoing regulatory and industry initiatives where possible, in particular:

- The Bank of England's Real Time Gross Settlement (RTGS) renewal.
- Second Payment Services Directive (PSD2).
- Competition and Markets Authority (CMA) Open Banking remedies.
- General Data Protection Regulation (GDPR).
- Fourth Money Laundering Directive (4MLD).

Please refer to Appendix 2 for more detail on how the NPA aligns to the above.

Question 1.3

As a potential vendor, participant or user of the NPA, are there any other design considerations that should be included in the NPA, especially with regards to considering the needs of end-users? If yes, please provide a description of those areas and why they are important to explore.

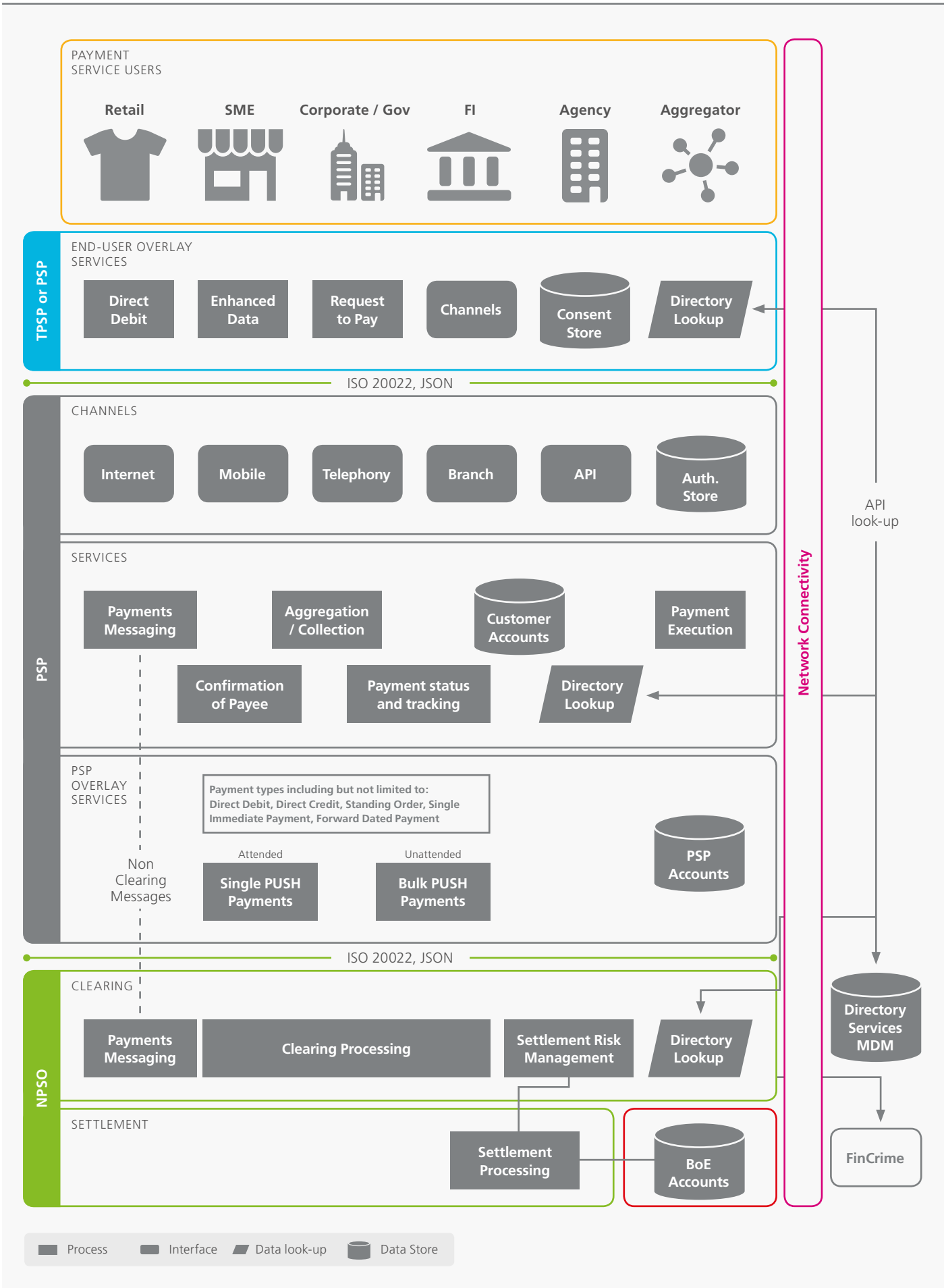
1.4 NPA Conceptual Model and Description

1.4.1 Overview

We have produced a conceptual model for the New Payments Architecture (NPA). This conceptual model defines the relationship between participants, connectivity mechanisms and supporting components across the layered architecture.

The NPA conceptual model is presented in Figure 1.1.

FIGURE 1.1 NPA CONCEPTUAL MODEL



1.4.2 Participant Roles and the Access Models

In the NPA, there will be a number of actors carrying out different roles and bearing different responsibilities; we refer to them as participants. Participants in the NPA fall into three categories: Payment Service Users (PSUs), Payment Service Providers (PSPs) and Third Party Service Providers (TPSPs):

1. Payment Service Users (PSUs) represent a person or organisation making use of a payment service in the capacity of a payer, a payee, or both. This includes individuals, businesses and organisations.
2. Payment Service Providers (PSPs) are entities involved in the carrying out of payment services. In the NPA, this includes authorised payment institutions, small payment institutions, registered account information service providers, registered payment service providers, electronic money institutions, credit institutions, the Post Office Limited, the Bank of England, government departments and local authorities and agents of PSPs.
3. Third Party Service Providers (TPSPs) provide services across the payments value chain to facilitate the initiation, 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).[9]

In addition, there are several other entities who are responsible for governance, including but not limited to, regulation, authorisation, registration and accreditation of the participants:

1. The Payment Systems Regulator (PSR) is an economic regulator for the payment system. It has the role of promoting competition and innovation in payment systems and ensuring that they work in the interests of PSUs.
2. The Bank of England (BoE) provides the RTGS service used for settlement in central bank money and is the prudential supervisor of some types of PSPs as well as payment systems, with an objective of protecting and enhancing financial stability.
3. The Financial Conduct Authority (FCA) regulates the financial services industry in the UK. Within the context of the NPA and its participants, the FCA will be responsible for authorising and registering applicable PSPs and TPSPs.
4. The New Payment System Operator (NPSO) will be the key vehicle for the delivery and governance of the NPA. It will be responsible for the procurement and contract management of the NPA. It will also run some NPA components, in particular those related to clearing and settlement, and the required integration with the Bank of England RTGS. It will be the central body that governs the NPA, including setting of standards and rules, such as for overlay services and for technical considerations such as security. In addition, the NPSO will be responsible for the accreditation and certification of certain participants, for example, Request to Pay, Confirmation of Payee and Enhanced Data service providers.

PSPs can access the NPA directly or indirectly. The manner in which they do so is summarised in the Table 1.3 below.

TABLE 1.3 ACCESS MODEL

Direct Settling access	Direct Non Settling access[10]	Indirect access[11]
• Bank of England settlement account is mandatory. • Direct technical connection to the NPA infrastructure. • Mandatory to receive payments 24/7. • Expected to offer send payment capability 24/7. • Funds authorised prior to submitting transactions for clearing (as per the current model). • Liquidity and risk management tools required.	• Bank of England settlement account is not required – settlement provided by the Direct Settling Participant acting as a sponsor PSP. • Direct technical connection to the NPA infrastructure. • Mandatory to receive payments 24/7. • Expected to offer send payment capability 24/7. • In the NPA model, funds will be authorised by the PSP before submitting the transactions to clearing.	• Bank of England settlement account is not required – settlement provided by the Direct Settling Participant acting as a sponsor PSP. • No direct technical connection to the NPA infrastructure – the technical connectivity is between the indirect participant and their sponsor PSP. • Fully reliant on the NPA service offering to the sponsor PSP. • Not mandatory to receive or send payments 24/7.

[9] TPSPs and PSPs may include some PSD2 regulated participants such as Account Information Service Providers (AISPs), Payment Initiation Service Providers (PISPs) and Account Servicing Payment Service Providers (ASPSP). A full list of PSD2 and FCA defined service providers can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/588961/Annex_B.pdf

[10] Also called 'Connected Non Settling Participant'

[11] Also called 'Non Connected Non Settling Participant'

1.4.3 Layers

The NPA is made up of several layers namely:

Payment Service Users Layer

PSUs include: retail (or consumers); Small and Medium Enterprises (SMEs); corporates and government; financial institutions; agency organisations and aggregators. PSUs make use of payment services in the capacity of either a payer, a payee, or an intermediary.

End-User Overlay Services Layer

End-user overlay services are used by payment services users. End-user overlay services will be delivered by PSPs and TPSPs. NPA overlay services will include Confirmation of Payee, Enhanced Data and Request to Pay. Other potential innovative services are expected to be provided within this layer. The end-user overlay services layer interface to the lower layers of the architecture via APIs.

This layer also holds the consent store against which PSPs or TPSPs will verify end-user authorisation for payment execution. Alongside the consent store, the end-user overlay services layer provides a directory look-up service through which TPSPs or PSPs will be able to access a subset of the reference data held, e.g. intended recipient details, which will support the routing of payments. The consent store and directory service are referenced in greater detail in the supporting components section.

In addition to providing new APIs that enable TPSPs to submit payments and provide overlay services, it is envisaged that PSPs and TPSPs will provide channel mechanisms enabling customers to continue to submit payments in a similar manner as today. Specifically, corporates and PSPs with indirect access (traditionally called 'agency payment service providers') should be able to continue to submit payments by using accredited software sponsored by a direct settling payment service provider.

We envisage that the NPSO will set minimum standards for TPSPs to be able to accredit them to provide corporate and indirect participant access in a similar manner to Bacs suppliers today. However, they would not mandate the use of particular standards between participants in the end-user overlay services layer.

PSP Channels Layer

PSUs will be able to transact directly through a variety of channels provided by PSPs, such as the internet, mobile, telephony and branches, as they do today. In addition, TPSPs will be able to provide additional payment service channels by using APIs to interface with PSPs and gain secure access to customer accounts. Rules and standards for APIs are yet to be defined. These will be overseen and governed by the NPSO and, where possible, align to PSD2 and Open Banking.

The 'Authorisation Store' is a data store holding the payer's authorisation codes.

PSP Services Layer

PSPs hold customer accounts which store customer funds and run the services required to execute and process a payment against customer accounts within this layer.

PSP Overlay Services Layer

This layer contains the payment mechanisms through which PSPs can carry out attended and unattended push payments to emulate existing payment types including Direct Debit (e.g. utility bill payments), Direct Credit (e.g. salary payments), standing orders, Single Immediate Payments (SIPs) and forward-dated payments. Therefore the NPA will support today's payment types into the future. New payment types can also be developed with the NPSO overseeing the approval process and ensuring interoperability between PSPs.

To support attended and unattended payments, this layer contains the interfaces to support initiation of push payments and bulk push payments into the clearing layer.

Overlay services to support settlement could be required to provide the configuration, and validation for a payment request. The specification for these overlay services could include settlement cycle, Net Sender Cap (NSC) and financial modelling.

Clearing Layer

The clearing layer allows PSPs to access the common infrastructure that transfers all payments. It coordinates the non-clearing payments messaging (e.g. threshold alerts), clearing and settlement processing for attended and unattended payments. It also carries out the following functions:

- Assures validation of non-clearing payment messages and their routing.
- Performs settlement risk management.
- Notifies participants of the payment outcome.
- Notifies participants of the settlement outcome.

Payment clearing processing in the NPA is logically split between attended and unattended batch payments. It allows Single Immediate Payments (SIPs) to be processed immediately but also provides the flexibility for bulk payments processing to be handled based on configuration parameters.

The settlement risk component is responsible for processing settlement risk checks for clearing processes. Its primary function is to check the transactions can settle by ensuring the clearing and settlement participants (PSPs / authorised submitters) are operating within their NSC.

Settlement

The Settlement layer is the single point of control for all payment instructions. It is where the actual movement of funds is finalised. It provides configurable settlement options with the Bank of England (BoE). The primary responsibility of settlement processing is to create settlement obligations for cleared transactions and to facilitate settlement completion with the BoE according to configured cycles for particular payment types.

The Bank of England (BoE) accounts provide cash collateral to ensure that the multilateral settlement of cleared payments will take place. These accounts hold funds for each participant. Such cash collateral is only used in the event of a participant being unable to settle from the relevant settlement accounts.

Network Connectivity

The Network Connectivity Layer will provide the networking infrastructure to access the NPA. To maintain security integrity, it is expected that participants accessing the NPA will conform to industry best practice and adhere to the network authentication, security requirements and specifications to be defined by the NPSO.

Connectivity between the layers and components will be open to multi-vendor competition and will not be tied to a single provider or a particular network element to ensure that competition is enabled and vendor 'stickiness' reduced.

Supporting Components

1. ISO 20022 and JSON:

The ISO 20022 messaging standard will be used for payment messages sent from the TPSP and the PSP layers, through to the clearing and settlement layers.

JavaScript Object Notation (JSON) has been proposed to provide the ISO 20022 data representation for the NPA. JSON is a lightweight data interchange format and has been selected by the Open Banking Working Group for its ISO 20022 data representation and consequently we are recommending its adoption for the NPA.

We are not mandating the use of ISO 20022 messaging standards between the participants in the End-User Overlay Services layer or between the PSU and the End-User Overlay Services layer. We recognise however, that a level of API definition may be required for certain core end-user services (such as Request to Pay and Confirmation of Payee) to enable interoperability, and therefore increase competition between different service providers.

2. Directory services:

Directory services are an essential feature of the NPA that enables participants to access reference data essential for the secure routing and execution of payments.

There is no single architectural component that comprises the directory services; rather it is best to consider it a sub-system of interacting components. The directory will need to provide a number of functional capabilities such as participant enrolment, identity access management and be a certificate authority.

The directory will also provide essential reference data to support payment initiation and execution. These data sets will need to be mastered and governed. The proposal is that the function of 'Master Data Management' is a centralised function controlled, administered and governed by the NPSO. It is envisaged that access to data within the directory will be available to all layers between the end-user overlay services and settlement layers. This is central to the enablement of greater competition in the payments systems market.

An assessment of the Open Banking directory service indicates that it can meet the requirements of the different roles and layers within the NPA such as supporting the delivery of the key functions of participant registration, identity access management and security authentication. As a result, it is recommended that consideration is given to adopting Open Banking directory services once it is clear how it will support all the potential users of the directory (and not just the nine PSPs initially mandated by the CMA to implement Open Banking).[12] If the market chooses an alternative directory services supplier, the NPA will support this requirement from an architectural design perspective.

The deployment options (e.g. centralised vs. distributed, replication vs. look-up) for the directory services will be subject to a number of technical and commercial considerations and it is recommended that these are further reviewed in the post consultation paper phase.

3. Financial Crime analytics:

A real-time feed of transaction information, in keeping with prevailing data protection laws, will be provided to the payments transaction data analytics capability described in more detail in Section 6.2.

[12] The Competition and markets authority issued The Retail Banking Market Investigation Order 2017 and has mandated nine banks namely, RBS, Lloyds, Barclays, HSBC, Santander, Nationwide, Danske, Bank of Ireland and Allied Irish Bank to set up an 'implementation entity' by 16 February 2017 to 'implement, maintain and make widely available' the new standards as set out in the Retail Banking market investigation: Final report.

Question 1.4

The nature of the layering approach enables new components to be added or updated with minimal impact on components in the other layers. We believe this will support greater levels of competition and innovation especially in the upper layers of the NPA.

In your view, as a vendor or service provider, will layering the NPA in this way simplify access and improve your ability to compete in the UK payments market? If not, please explain why.

1.5 Clearing and Settlement

In the Strategy, we identified two main approaches to clearing and settlement, centralised and distributed. We have since performed further analysis into these two options to determine our preferred approach that must align with the following:

- The renewal of the Bank of England (BoE) RTGS system.
- Settlement taking place in central bank money.
- Funds being available to ensure that settlement can complete.
- The ability to support:
  - Cap adjustments in real-time.
  - Flexible settlement options as agreed between the NPSO and the Bank of England.
  - Both attended (single) and unattended (bulk) payment types.
  - 24/7 clearing.
  - Settlement in line with the Bank of England RTGS.
- The NPSO applying to the Bank of England for designation of the NPA arrangements for the purpose of settlement finality in compliance with the relevant legal requirements.

We have considered the two clearing and settlement options. Our analysis suggests a centralised model would be the best approach.

1.5.1 Clearing and Settlement Options

Centralised Model Overview

In the centralised model, the routing, settlement risk and settlement processing is managed centrally. The central clearing node will be responsible for the routing and clearing of payments. Participants do not need to exchange payment messages directly with each other.

Figure 1.2 shows how the centralised model operates between individual PSPs and the central clearing node:

All payment messages are routed via central participant messaging.

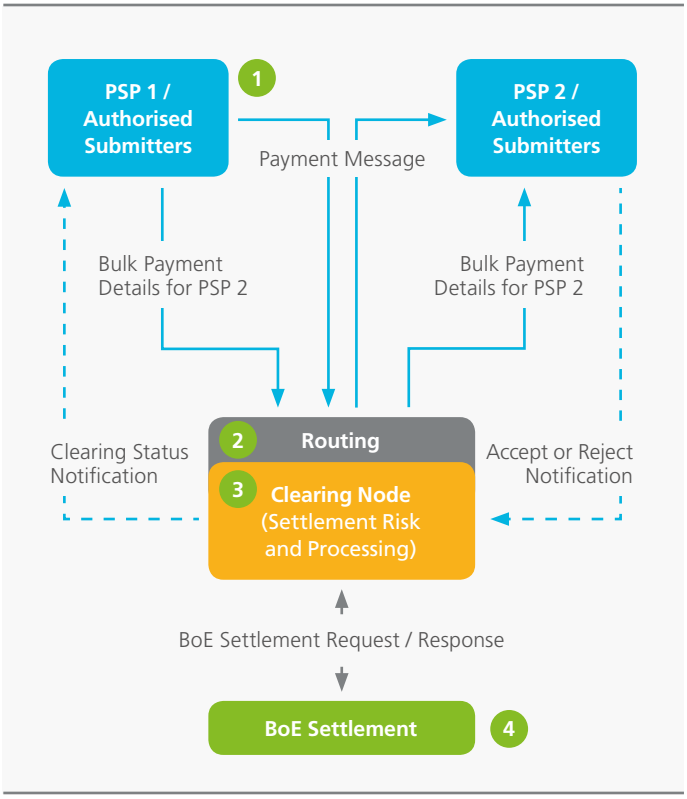
1. PSPs send payment messages to a central clearing node.

2. The routing node is responsible for:
- Receipt of payment message(s).
- Routing of messages.
- Relay of payment messages to other PSPs.
- Clearing status notifications.

3. The clearing node is responsible for:
- Maintenance and checking of the participating PSP's settlement risk position.
- Creating settlement risk positions for cleared payments.

4. BoE settlement initiates settlement according to configured cycles.

FIGURE 1.2 CENTRALISED MODEL



Distributed Model Overview

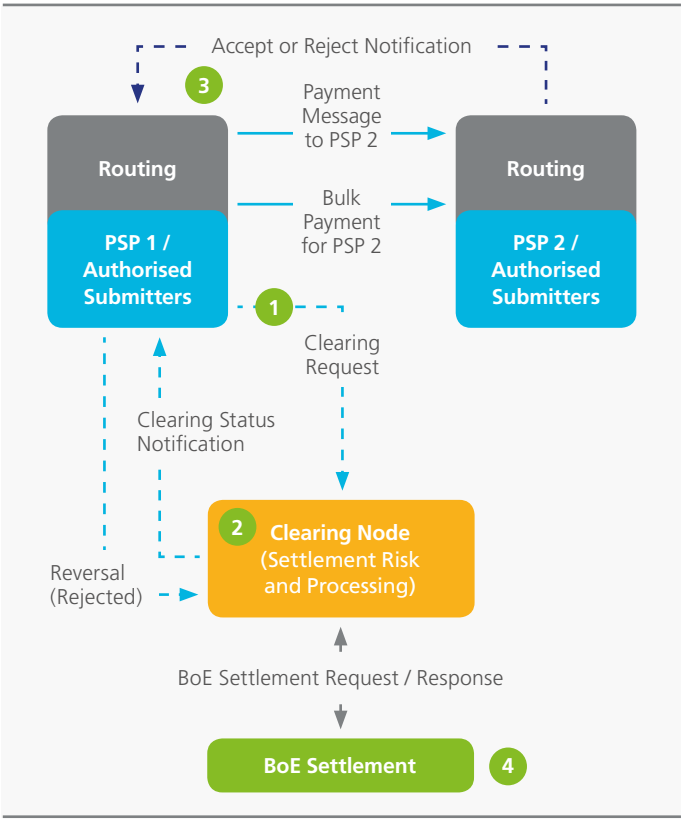
The distributed model (peer-to-peer participant messaging with centralised risk and settlement management) requires the participants to exchange payment messages with each other, with the sender accountable for ensuring settlement via a common settlement risk and settlement processing service (clearing node). The clearing node validates that the sending participant is operating within its Net Sender Cap and adjusts the settlement positions for the cleared transactions.

Figure 1.3 shows how the distributed model operates between individual PSPs and the clearing node.

Similar to centralised, the sender PSP initiates clearing and settlement but each PSP is responsible for routing its own payment messages, checking redirection and separating files by receiving PSPs.

1. The PSP sending the payment (PSP 1) sends a clearing request to the clearing node.
2. The clearing node is responsible for:
   - Checking the risk position.
   - Creating a settlement obligation.
   - Sending a clearing status (with token) notification to sender.
3. The sending PSP (PSP 1) sends cleared payments to receiver (with a token) and a receiver (PSP 2) sends a response notification to the sender (PSP 1) – Accept or Reject.
4. BoE settlement initiates settlement according to configured cycles.

FIGURE 1.3 DISTRIBUTED MODEL



Centralised and Distributed Models Comparison

The pros and cons of each approach are summarised in Table 1.4 below:

TABLE 1.4 SUMMARY OF PROS AND CONS FOR THE CENTRALISED VS. DISTRIBUTED MODELS

Approach	Pros	Cons
Centralised	• Multiple vendors can bid for each of the central components. • Provides a clear and manageable risk model that aligns the routing with settlement risk management. • Reconciliation of transactions between participants is simplified compared with the distributed model. • The 'insulating' nature of the layered concept mitigates systemic risks associated with individual participant failures. • Provides consistent and accurate settlement information in real-time. • Expected to result in lower overall costs and risk to the payments industry as the centre will handle the routing complexity. • Expected to support greater levels of innovation through the reduction in PSP integration and management complexity compared to a peer-to-peer clearing approach. • Operational management, governance and control are more efficient with a single point of contact for support. • Offers a simpler mechanism for direct (payment) submitters as it does not require them to carry out directory look-ups before routing payments.	• Competition in the clearing and settlement layers will be 'for the market' only. • Precludes third-parties from offering their own settlement routing services to individual PSPs. • Potentially exposes participants to higher costs for routing since there may be fewer options to seek competitive pricing.
Distributed	• For routing, each PSP can scale to its own required volumes, which introduces flexibility and makes the model commercially competitive. • Multiple suppliers can compete for providing routing services encouraging competitive pricing.	• Requires specific message flow implementation to enforce the requirement of the receiver only receiving cleared and settled payments. • Stakeholders saw the opening up of the clearing layer as adding technical complexity and cost for PSPs (e.g. clearing message routing) without any demonstrable benefit to payment service users. • Introduces a risk of PSPs not following message protocol and debiting/crediting accounts without confirmation of settlement. • Coordination of change was also considered to be more complex with this option since more controls would be needed to implement and mitigate cyber risk.

Based on the analysis above, we believe that the centralised model is the best approach for the NPA.

Question 1.5

With the recommended centralised clearing and settlement option, as a participant or vendor who is accessing or delivering the clearing and settlement service, do you think:

a. We have reached the right conclusion in recommending this option?
b. The right balance of managing risk versus competition has been achieved?

If not, please explain why.

1.5.2 Clearing and Settlement Deployment Approach

The clearing and settlement model can be deployed as either a single or multi-vendor approach. The design of the NPA caters for both approaches. The NPSO will decide which approach of these two to implement and the corresponding procurement process.

Single Vendor Deployment Approach

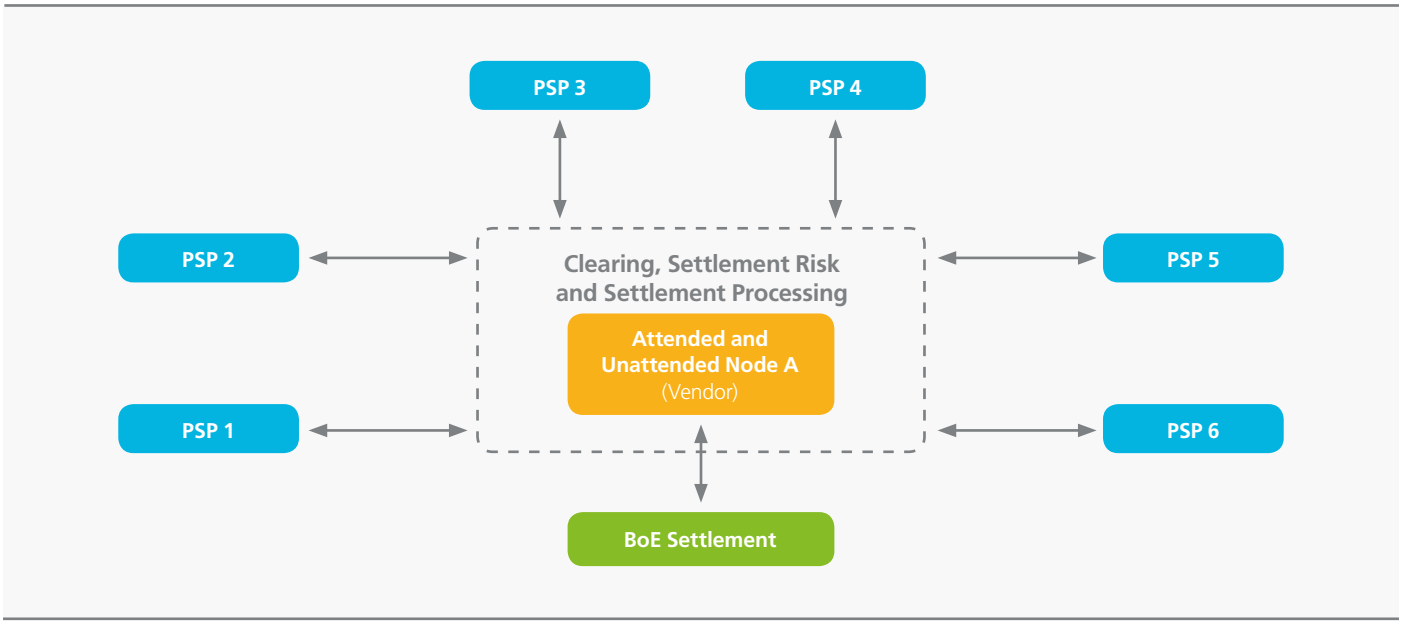
A single vendor deployment approach is one where a single vendor (node) provides settlement risk and settlement processing for all attended and unattended payment types.

The single vendor option supports participant liquidity efficiency through the use of a single participant debit cap and multilateral netting between each participant for all their payment types. Simplified reconciliation and reporting is achieved with fewer settlement requests being sent to the Bank of England compared to the multi-vendor approach.

Other advantages include efficient oversight and management by the NPSO ensuring simplicity, consistency and standardisation in the service and operational models.

However, reliance on a single vendor could make migration to an alternative supplier for extended capacity (payment handling or PSP on-boarding) or new services technically and commercially more challenging. The use of ISO 20022 along with the adoption of the layered model of the NPA and contract structure could be used to materially mitigate against these risks.

FIGURE 1.4 SINGLE VENDOR DEPLOYMENT APPROACH



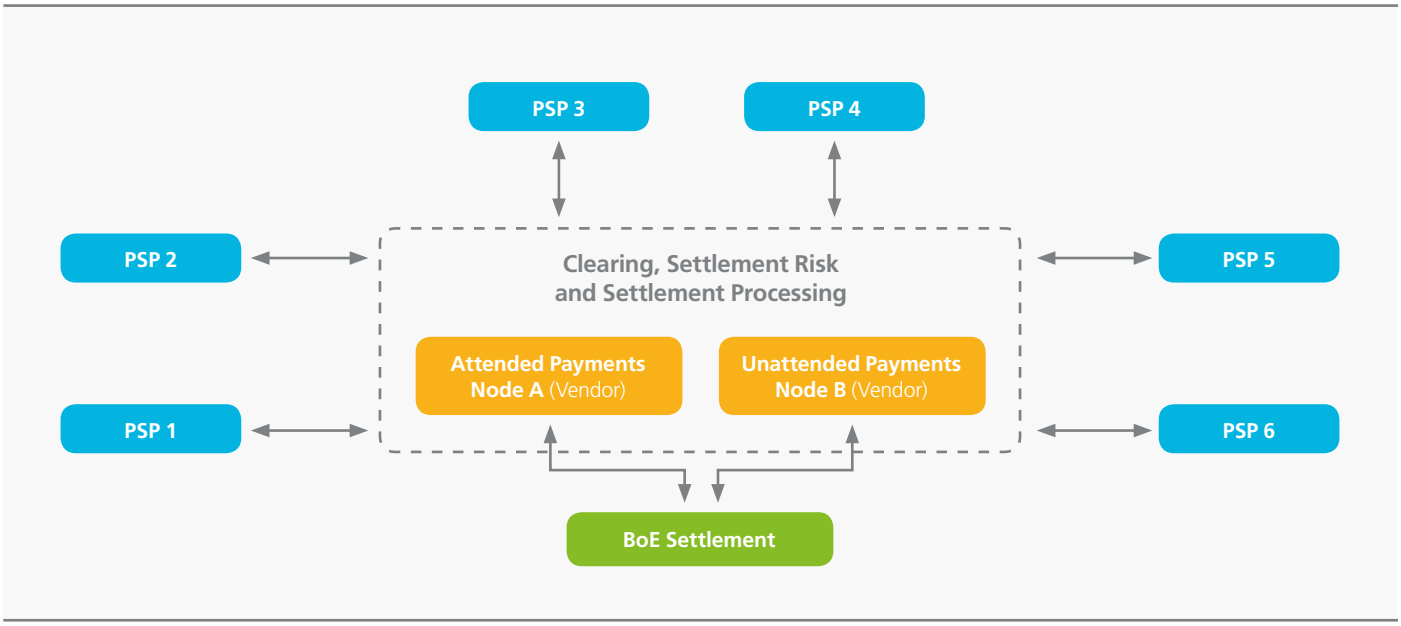
Multi-Vendor Deployment Approach

A multi-vendor deployment approach is one where clearing would be provided by different vendors (nodes). This can be one node per PSP, akin to the SEPA model or one node per payment type (e.g. attended or unattended). The 'per payment type' multi-vendor approach is expected to offer advantages over the 'per PSP' approach. It is expected to offer more flexible settlement options, enable the automation of cap management, support the ability to deliver new innovative payment services independently of the clearing and settlement layers, increase resilience, as well as allow for the delivery of new payment types with minimal disruption.

Opportunities also exist to provide a more sophisticated cap management approach in the future where nodes exchange data in real-time to enable dynamic debit cap adjustments according to the settling position of each node.

Based on stakeholder feedback, the option to assign a single clearing node to each payment type was considered to provide a good balance between technical implementation challenges and the enablement of competition for the market.

FIGURE 1.5 MULTI-VENDOR DEPLOYMENT APPROACH



In this approach, it is envisaged that the NPSO would be responsible for managing an overall agreed Net Sender Cap (NSC) (i.e. the available balance) position for each participant and then allocating a debit cap for each of the clearing nodes. The settlement participant is responsible for determining the overall NSC and allocating it between its sponsored non-settlement participants. To achieve optimal liquidity efficiencies with the multi-vendor approach, the economic and operational aspects in the settlement and clearing layers require consideration.

The NPSO is also expected to be able to reallocate debit caps for participants between the clearing nodes as long as the aggregate debit cap across all nodes remain within the participant's agreed NSC position with the Bank of England.

The multi-vendor option is considered to be more challenging from an NPSO management perspective as it requires a degree of technical build complexity, technical interoperation and management that is not required with the single vendor model.

Question 1.6

Do you agree with our analysis of each of the clearing and settlement deployment approaches?
Which is your preferred deployment approach?

1.6 Proof of Concept

In the Strategy, we suggested that carrying out a Proof of Concept for specific aspects of the NPA that might have been needed for new and untried concepts for the payments industry. Examples include demonstrating potential interoperable standards, and proving that the layered design is scalable and extensible.

Following evaluation of the proposed design and engagement with payments industry stakeholders, it was deemed not necessary to carry out a Proof of Concept at this stage. This is because the concepts presented in the proposed architecture were either already:

- Understood within the payments industry (e.g. the use of ISO 20022 to support interoperability).
- Under development by other industry programmes (e.g. API development through Open Banking).
- Successfully deployed in other technology-based service industries (e.g. layering within the telecommunications industry).

The NPSO could choose to carry out a Proof of Concept as part of a procurement process at a later date.

Question 1.7

As a vendor of services in any layer of the NPA, do you think that more work is required to prove any of the main concepts of NPA before embarking on the procurement process? If so, please explain which areas and why.

1.7 Next Steps

In addition to receiving and assessing consultation responses, further work will be undertaken throughout the rest of 2017 to develop certain aspects of the NPA design. That is:

1. Carrying out more analysis on how Open Banking APIs and capabilities can be used to support the delivery of the NPA.
2. Additional analysis of areas of the NPA to aid handover of the NPA to the NPSO. Potential areas include the API delivery plan and development of the requirements for the directory, consent and authorisation stores.

2.0 Collaborative Requirements and Rules for the End-User Needs Solutions

This section focuses on three End-User Needs (EUN) solutions: Request to Pay, Assurance Data and Enhanced Data.

This section will be of particular interest to payment end-users: corporates, government, SMEs and individual consumers. End-users will be able to review the solutions we are proposing and determine whether they address their needs as identified in our Strategy (Sections 2.2-2.4). In addition, this section will be useful to providers of any of the EUN solutions: Payment Service Providers (PSPs), Third Party Service Providers (TPSPs), governing bodies and investors.

2.1 Introduction

In our Strategy, we prioritised the collaborative development of requirements and rules for 3 EUN 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, 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.

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 2.1.[13] For each use case, we have designed 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.

FIGURE 2.1 END-USER NEEDS PRINCIPLES

EUN Principles

1. Payer is always in control
2. Transparent
3. Available, secure and stable
4. Common Rules and Standards
5. Open to competition and innovation
6. Regulatory compliant
7. Payment agnostic
8. Accessible and inclusive
9. Scalable, future proof

[13] For a more detailed definition of each principle refer to the "User requirements and rules" supporting document which can be found at: https://implementation.paymentsforum.uk/consultation

2.2 Request to pay

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.

Question 2.1

As a payee,

a. Does your organisation serve customers who experience challenges paying regular bills?
b. Does your organisation experience unpaid direct debits?

Please comment on the extent, to which you experience this and any trends you see in this area.

What is Request to Pay?

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

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

End-users (individuals, SMEs, corporates and government) could benefit from Request to Pay. Payees will be provided with visibility on what the payer's intention is with regards to a bill payment.[14] Currently, once a payee sends out a bill, they have limited visibility on whether the payer will make a payment or not and when they will pay. Increased visibility has a positive impact on cash flow management, payment reconciliation, debt management and overall customer relationship management. Cash flow management is especially important to SMEs who tend to have limited cash reserves making them vulnerable to cash flow challenges.

[14] This benefit is dependent on the payer choosing to respond to a Request to Pay.

FIGURE 2.2 SUMMARY OF KEY BENEFITS OF REQUEST TO PAY

Request to Pay provides visibility to the payer on outgoing payments; it opens a communication channel to the payee; and it provides a tool through which a payer can flex[15] how they make their payments - when, how, and how much. We provide further analysis of the potential quantifiable benefits arising from the use of Request to Pay by end-users in the cost-benefit analysis in Appendix 6.

Request to Pay is independent of the payment mechanism used to make a payment. We have taken an approach to separate the messaging and the payment mechanism in our design. This approach provides more flexibility to both payers and payees on the payment mechanisms through which they make and collect payments, as well as fostering competition for both the messaging component and the payment mechanism of Request to Pay, which could be provided by different service providers.

End-User Requirements – Request to Pay

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 etc. 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 in figure 2.3 and 2.4 below. The requirements and rules are classified into payee and payer requirements.

Question 2.2

Request to Pay provides visibility to payees on the intentions of a payer. Would the increased visibility benefit your business? If so, how?

Question 2.3

Request to Pay will result in increased communication between the payee and the payer. As a payee:

a. Would the increased communication present a challenge? If so, in what way?

b. What benefits could you envisage from this increased communication?

c. Do you see any additional potential benefits resulting from Request to Pay other than those described? If so, which ones?

[15] The nature of the flexibility is subject to existing contractual terms between the payer and the payee.

FIGURE 2.3 PAYEE REQUIREMENTS AND RULES – REQUEST TO PAY

A **payee** utilising Request to Pay must be able to carry out the following use cases and associated requirements.

Use case 1. Create a Request to Pay message and send it to the payer.

Requirements:

Through the Request to Pay service, a payee will generate a Request to Pay message. Each request will contain several items of information required by the payer or to fulfil certain functions in the service or the NPA. We recommend that, as a minimum, every request should include:

a. **Payee's Name:** The name of the payee from whom the Request originates.
b. **Payment Description:** A description of what the payer is being asked to pay for that clearly allows the payer to identify the payment.
c. **Payment Amount:** The total amount due from the payer.
d. **Payment Period:** The payment period is the time period during which the payee requires the payer to pay them. The payee provides a start and end date defining the payment period, in line with any contractual agreements.
e. **Payment options available to the payer:** The payment options supported by the payee that the payer can use when they choose to make a payment. The payee will include account details where appropriate and additional information about costs and incentives associated with the different payment methods.
f. **Reference ID:** A reference ID which allows the request to be traced. It also provides a means by which the request and an associated payment can be linked for reconciliation.

Once the request has been generated, the payee will then address it to the intended payer through the payer's preferred channel.

Rules:

a. A Request must have at least one recipient.
b. A Request amount cannot be less than £0; a payee can set a maximum amount if they wish.[16]
c. A Request due date or payment window end date cannot be in the past.
d. A Request must specify at least one payment method that a payer can use should they wish to make a payment.
e. A Request must have a reference ID that allows it to be identified and tracked.

Use case 2. Provide additional information.

Requirements:

The payee may wish to provide more information in addition to the payment description. For example, a line item breakdown of the payment, an invoice or a hyperlink etc.

Rules:

a. Additional information is not necessary to send a request.
b. Additional information provided should only be accessible to the intended recipients.

Use case 3. Receive responses from the payer and act upon them.

Requirements:

Request to Pay is a two-way messaging system. Once the payer has received a request, the payer will be able to:[17]

a. Accept a request and make payments: In addition, the payee is provided with information on the nature of the acceptance (i.e. the payer has made a full payment or partial amount); the amount paid, and the date.
b. Decline a request: Should the payer decline a Request to Pay, the payee is notified and they can initiate a line of dialogue with the payer.
c. Request a change to the payment period: In the situation where the payer is not able to make a payment within the payment period and they request an extension to the payment period, the payee will be notified. They can then respond accordingly.
d. Request to be contacted: Should the payer request that the payee contacts them, the payee will be notified.

Each response could trigger other ancillary back-office processes. Examples include contact centres in the case of a request for contact, PSP processes once a payer has initiated a payment, or debt management in the case of a decline.

Rules:

a. Where multiple payment options are provided, a payer cannot be prevented from making multiple partial payments via different payment methods.

[16] Particular payees such as mortgage providers and tax bodies require the ability to define a maximum amount payable. E.g. mortgage overpayment limits.

[17] The responses available to the payer are subject to contractual terms that exist between them and the payee.

FIGURE 2.4 PAYER REQUIREMENTS AND RULES – REQUEST TO PAY

A **payer** utilising Request to Pay must be able to carry out the following use cases and associated requirements.

Use case 1. Receive a Request to Pay through their preferred communication channel and be able to block requests from particular entities.

Requirements:

A payer will receive Request to Pay messages through their preferred channel of those available.[18] The request will contain the information provided by the payee on what it pertains to, its value, payment period and payment methods accepted. In cases where the payee has also added additional information such as an invoice, a payer will be able to access this information. The payer can then make a decision on the appropriate response based on the information presented.

Request to Pay presupposes that the payee and the payer have a relationship, under which a regular or one-off payment is expected. If not the case, for example, the payee receives a request by mistake, spam or fraud, the payer will be able to block receipt of requests from a specific payee or reject unsolicited requests. The payer can also entirely opt out of the Request to Pay service, in relation to a specific payee, which will prompt a notification to the payee.

Use case 2. Receive a Request to Pay through their preferred communication channel.

Requirements:

A payer will be able to respond to a Request to Pay in several ways:

a. **Accept the request and make a full or partial payment:** The payer will have flexibility on whether to make the payment in one single payment or multiple partial payments.[19]

b. **Decline the request:** In some cases, the payer may refuse the request outright. For example, if they believe the request has been sent in error, for an incorrect amount, or already paid via other means.

c. **Request an extension of the payment period:** If the payer cannot make the full payment within the payment period provided by the payee, they could request an extension from the payee.

d. **Contact payee:** The payer may choose to contact payee to obtain more information on the payment or discuss the payment to aid them in determining the appropriate response.

Rules:

a. Once payment for the full amount is initiated the request is considered 'closed'.

b. Where a payee has provided a maximum amount payable, a payer cannot pay more than this amount.

c. Partial payments can be any portion of the total amount.

d. 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.

e. A request is considered once the last of the partial payments amounting to the total request sum is initiated.

f. An extension can only be after the original due date or the payment period ends.

g. A payer can decline requests, notifying the payee that payment will not be made.

h. Payees must provide at least one contact method.

Use case 3. Select a payment method and Initiate Payment.

Requirements:

If a payer accepts a request, they will have a choice of payment type within the range available. In instances where there is cost or incentive associated with a payment method, relevant information will be explicitly displayed to the payer.

Once the payer chooses the payment method, the payment will be initiated and relevant information will be added to the payment. This will include: the payee's payment details specific to the payment method (e.g. sort code and account number), the payment amount and the request reference ID. This automatic transfer of associated information reduces friction and reconciliation error.

Once the final payment is initiated and sent, the Request to Pay cycle is complete.[20] The payer is considered to have accepted the request.

Rules:

a. 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.

[18] Consideration has to be given to segments of the population who do not use electronic channels. This aligns with our principle to ensure that the solutions are accessible and inclusive.

[19] When a payer accepts a Request to Pay, it will also trigger a payment being initiated and the payee will get notified once initiation is complete.

[20] Note, this does not guarantee that the payment has reached the payee's account or the payee has reconciled it to the payer's account. Assurance Data, the second EUN solution, addresses the payer's ability to determine the status of a payment. If the payment was made in cash, this should also be communicated to the payee.

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.

A governing body will ensure the aims of the service are met and the end-users are protected. The governing body will ensure that the minimum end-user and technical standards are met by stakeholders and the service is not abused or used for fraudulent purposes. We expect this to be the NPSO.

Question 2.4

We have recommended the minimum information that should be contained in a Request to Pay message. As a payee:

a. With the exception of reference ID, are you able to provide other items of information with every payment request?

b. Is there additional information, specific to your business, that you would have to provide to payers as part of the Request to Pay message?

Question 2.5

We envisage payees stipulating a payment period during which the payer will be required to make the payment. As a payee, how do you think this payment period might be applied within your organisation?

Question 2.6

Request to Pay will offer payers flexibility over payment time as well as amount and method. As a payee:

a. Does your business model support offering payment plans and the ability for payers to spread their payments? If so, please provide more details as to how these plans are offered, their conditions and to which customers.

b. Do you have a predominant payment method used by your payers? If so, what percentage of customers use it?

c. Do you offer your payers a choice of payment methods? If yes, what determines how much choice you offer? If not, what are the barriers preventing you from doing so?

d. Are there any incentives to use one payment method over another? If so, what is the rationale?

Question 2.7

A minority of payers may not be able to pay within the payment period.
Through Request to Pay they will be able to request an extension to the payment period. As a payee:

a. Do you currently offer your payers the capability to extend a payment period, request a payment holiday or make late payments?

b. What are the conditions and eligibility criteria under which this is offered?

c. If you currently don't, what are the barriers preventing you from offering this capability?

Question 2.8

Request to Pay will offer payers the option to decline a request.
The purpose of this option is to provide an immediate alert in case the request was received as an error or will be paid by other means. As a payee:

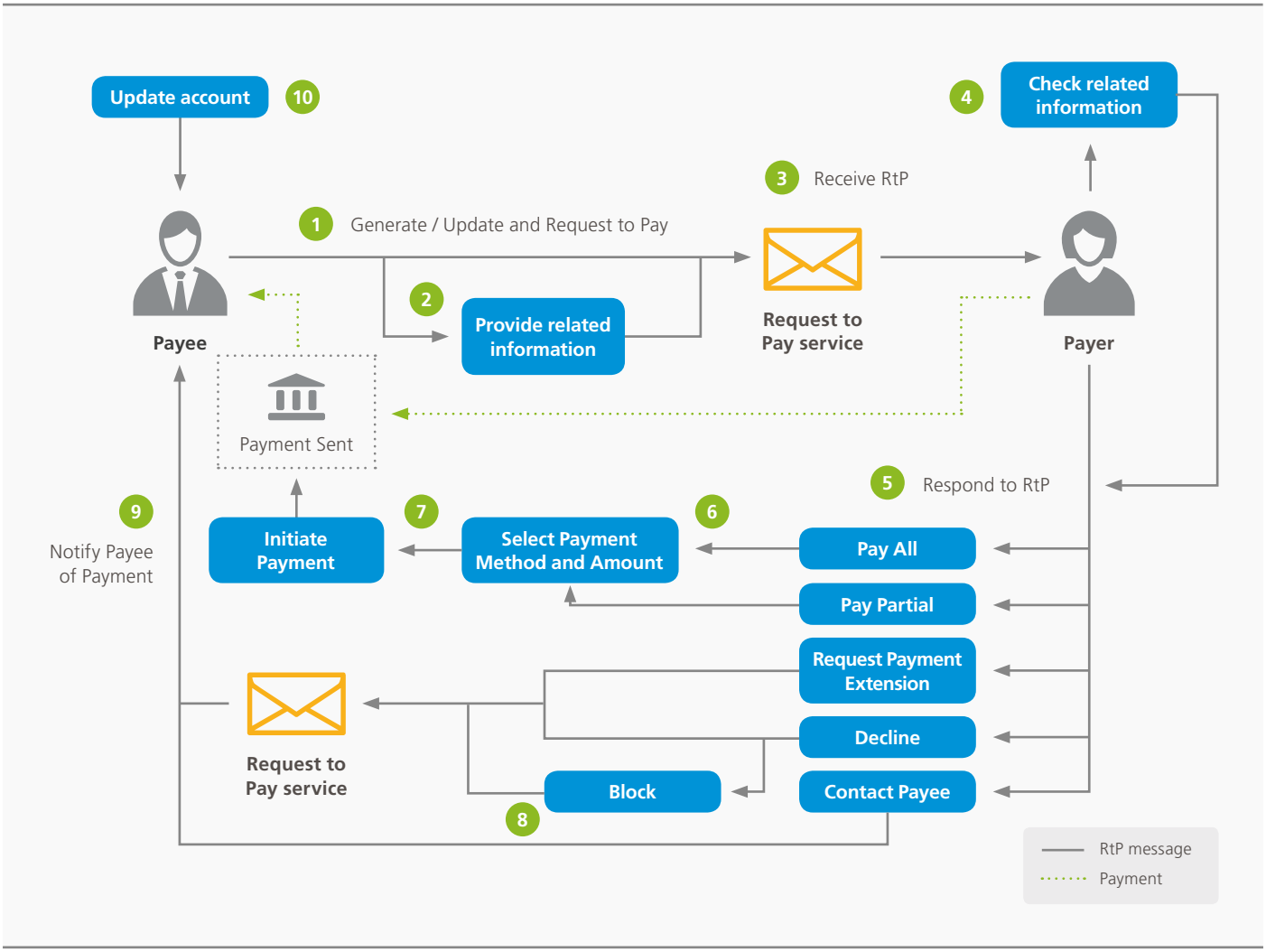
a. Would you find this information useful?

b. Do you have any concerns about providing this capability?

End-to-End Journey for Request to Pay

The end-to-end Request to Pay journey is shown in Figure 2.5.

FIGURE 2.5 REQUEST TO PAY END-TO-END JOURNEY



Step 1 A payee generates a new Request to Pay (or updates an existing Request to Pay), which is then sent to the payer.

Step 2 A payee has the option to provide additional information for the payer. This could take the form of a hyperlink to related information stored elsewhere or an attached document for example.

Step 3 The payer receives the Request to Pay through their preferred channel.

Step 4 The payer reviews additional information related to the received request – if the payee has provided this.

Step 5 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.

Step 6 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.

Step 7 The payer initiates payment.

Step 8 The 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).

Step 9 The payee receives a notification with the payer's response.

Step 10 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.[21]

[21] Further detail on how Request to Pay will be supported by the NPA can be found in Appendix 4.

Question 2.9

Does the Request to Pay service as described address:

a. The detriments identified in our Strategy?

b. The challenges experienced by your customers? Does it introduce any new challenges?

Question 2.11

What are the features or rules that could be built into Request to Pay that would make it more valuable to your organisation, or more likely for you to adopt it?

Question 2.10

As a payee, considering the information provided in this document,

a. What is the extent of change you think you will need to carry out internally to offer Request to Pay?

b. What challenges do you see that might prevent your organisation adopting Request to Pay?

c. What is the timeframe you think you will need to be able to offer Request to Pay?

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 taken into account. For each risk we have identified mitigation summarised in Table 2.1.

TABLE 2.1 KEY RISKS AND MITIGATION FOR REQUEST TO PAY

Risk	Mitigation
1. Uncertainty of payment Request to Pay provides payers with the ability to defer or decline a request which 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 getting into debt. • If the payer's response does not reach the intended payee, this could result in a non-payment and payer getting 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.

Additionally, the following aspects 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, terms of payment extensions etc.
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, there must be consideration 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 the adoption of the service, payers will need to be made aware of the existence of the service through 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 concept.
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.

Question 2.12

We have highlighted several risks and considerations relevant to the delivery of Request to Pay. As an end-user of Request to Pay:

a. Are there any risks that we have not addressed or highlighted that you would like to add?

b. Are there additional unintended consequences that we should consider?

Question 2.13

We recognise that additional work needs to be done in identifying safeguards including liability considerations associated with Request to Pay. As an end-user of Request to Pay:

a. What are some of the liability concerns that you may have?

b. Would you be interested in working with the Forum to define, at a high level, the liability considerations for Request to Pay? If so, please contact us as soon as convenient through the Forum website so we can get you involved.

2.3 Assurance Data

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,[22] and the delivery status. This increases end-users' confidence.

We proposed a suite of tools collectively called Assurance consisting 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.

2.3.1 Real-time Balance

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

End-User Requirements: Real-time balance

To address the lack of real-time information, we recommend that PSPs provide payers with real-time balance information, including information on uncleared funds or payments made which are yet to settle. Payers will be able to determine how much money they have at any point in time including before they make a payment. Currently, several PSPs already provide real-time balance information and we therefore do not propose to do any further collaborative work in this area.

Question 2.14

As a PSP:

a. Do you currently offer real-time balance information to your clients? What information do you offer them?

b. If not, what are the constraints?

2.3.2 Confirmation of Payee (CoP)

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

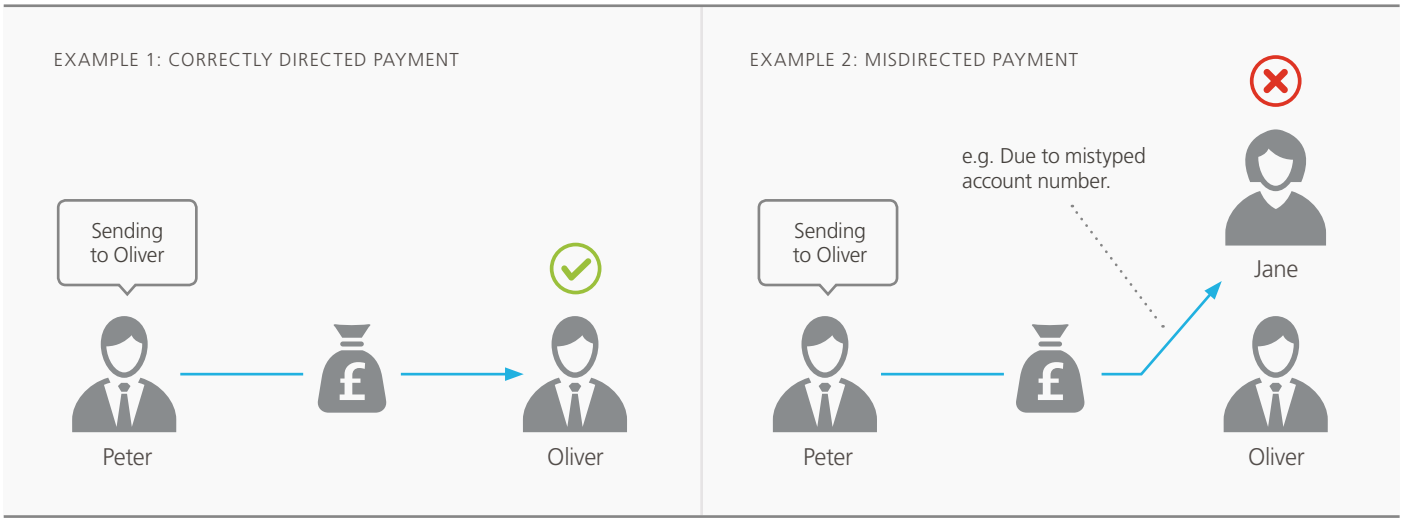
As a special case, CoP will also include a Confirmation of Payer capability. Confirmation of Payer addresses the need for a payee setting up a payment mandate (direct debit) to verify that the account, from which they will be initiating the payment, belongs to the intended payer.

Misdirected Payments

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

A misdirected payment is a payment where the beneficiary is different from the payer's intended payee, as seen in Figure 2.6. Misdirected Payments are due to several causes which are summarised in Figure 2.7.

FIGURE 2.6 WHAT IS A MISDIRECTED PAYMENT?



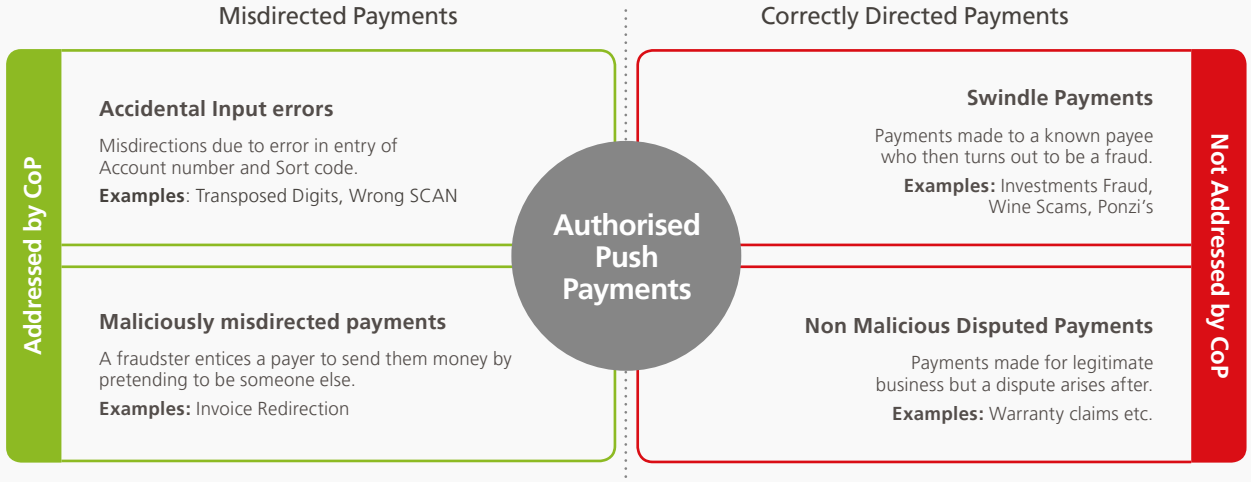
[22] The level and nature of status tracking varies across the payment methods.

Where a payer successfully pays their intended payee, but the goods or services the payment relates to fails to materialise (i.e. because the payee is a fraudster or scammer), this is not considered to be a misdirected payment. CoP will not solve this type of scam.

This is, however, one of the detriments under consideration within the 'Improving Trust in Payments' work.

Figure 2.7 illustrates the types of misdirected payments addressed by CoP. It also provides a comparison to those not addressed.

FIGURE 2.7 TYPES OF PAYMENT MISDIRECTS ADDRESSED BY CONFIRMATION OF PAYEE



End-User Requirements - CoP

The primary end-user of the CoP service will be the payer.[23]

The service will need to meet several requirements as a minimum. These are shown in Figure 2.8.

FIGURE 2.8 PAYER REQUIREMENTS AND RULES – CONFIRMATION OF PAYEE

A **payer** utilising CoP must be able to carry out the following use case and associated requirements.

Use case 1. Determine whether the account they are making a payment to belongs to the intended payee.

Requirements:

Using an account identifier (e.g. sort code and account number) the payer will be able to confirm that the related account belongs to the intended payee.

We identified the following accounts as being in scope:

a. 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 e.g. current accounts, head office collection accounts and some saving accounts.

b. 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 account, if additional information is provided, e.g. roll number accounts, credit card accounts, some savings accounts, mortgage accounts and investment accounts.

Rules:

a. The CoP response provided to the payer will be as clear and unequivocal as possible to allow the payer to make a decision that he or she is making the payment to the intended payee.

b A payer will be able to carry out a CoP at any time (24/7) and receive the response in real time.[24]

c. In cases where the account details related to an account that has been transferred using the Current Account Switch Service (CASS), the payer will be notified.

d. The CoP service can only be utilised for the purposes of making a payment. PSPs will ensure relevant safeguards are put in place to ensure prudent use. E.g. to guard against phishing, profiling etc.

[23] The payee in the case of Confirmation of Payer.

[24] We recommend a response time of 5 seconds maximum.

We have proposed that the CoP response provided to the payer will be clear and unequivocal. In our work, we have identified two main forms that a CoP response can take:

Approach 1

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

Approach 2

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

Each of the approaches above has specific considerations that must be taken into account. In particular:

- Data protection regulations must be considered to ensure that payer data is handled lawfully especially in the case where the account information is played back.
- Consideration must be paid to ensure the confirmation provided is accurate (minimal false positives / negatives, liability in case of errors).

In addition to the payer, several parties will play supporting roles. These are both the payer's and payee's PSPs as well as a governing body. The payer's PSP will provide the CoP service to the payer. The payee's PSP will provide the relevant payee information.

A governing body, we expect this to be the NPSO, will ensure the aims of the service and appropriate technical standards are met, and the service is not abused or used for fraudulent purposes.

Question 2.15

We have presented two CoP response approaches (Approach 1 and Approach 2).

a. As a payer, what would be your preferred approach? Why?

b. As a PSP, what would be your preferred approach? Why?

c. As a regulator,
   i. What applicable considerations must be made for each approach?
   ii. What safeguards must be put in place for each approach?

End-to-End Journey for CoP

Figure 2.9 illustrates the end-to-end journey for CoP.

Step 1 The payer provides the account reference details (e.g. sort code and account number) to their PSP.

Step 2 The payer's PSP sends CoP request to the payee's bank.

Step 3 The payee's PSP sends a response back to the payer's PSP.

Step 4 The payer's PSP presents the response to the payer. The payer makes a decision based on the CoP response.[25] [26]

FIGURE 2.9 CONFIRMATION OF PAYEE END-TO-END JOURNEY

Question 2.16

As a PSP:

a. Would you be able to offer CoP as described to your customers?

b. What is the extent of change that you would need to carry out internally to offer CoP?

Question 2.17

The successful delivery of CoP is largely dependent on universal acceptance by all PSPs to provide payee information. As a PSP:

a. Would you participate in a CoP service?

b. Are there any constraints that would hinder you providing this service?

[25] Payer is always in control.

[26] Further detail on how CoP will be supported by the NPA can be found in Appendix 4.

2.3.3 Payments Status and Tracking

Once a payment is initiated, the payer will want to know the status of the payment and, if not in real-time, its position on its journey to the payee. Figure 2.10 summarises the main parts of the payment journey and what is being tracked.

End-User Requirements – Payment Status and Tracking

The primary end-users of a payments status tracking functionality will be:

- **The payer:** Once the payer has made a payment, they will be interested in determining the status of the payment.
- **The payee:** A payee expecting a payment will use the functionality to determine the status of a payment that has been made to them.[27]

In addition, a payment tracking functionality will need to meet the requirements of the payee and payer. These are illustrated in Figure 2.11 below.

To support the service the payers and payees PSPs will need to provide the required status information to the payer and payee using their preferred channel.

FIGURE 2.10 ILLUSTRATION OF THE MAIN COMPONENTS OF PAYMENT STATUS AND TRACKING

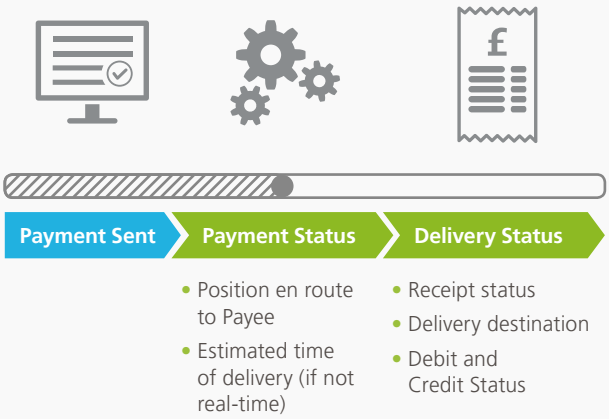


FIGURE 2.11 PAYER AND PAYEE REQUIREMENTS – PAYMENT STATUS AND TRACKING

A **payer** must be able to carry out the following use case and associated requirements:

Use case 1. Determine the status of a payment made.

Requirements:

For all applicable electronic payments[28], a payer will be able to determine the status of the payment. In particular, they will be able to:

a. Determine whether the payment made has been debited from their account.
b. Determine the position of the payments on its journey to the payee.
c. Determine the estimated time of delivery.
d. Determine the delivery status.
e. Determine delivery destination and in cases where the payment is redirected, as is the case with CASS, the new destination.

Rules:

a. Confirmation of receipt must include time, date and delivery account number.
b. In the event that a payment does not reach the payee's account in real-time either by design or in error, then a payer must be able to determine where the payment is in the process and the reason.

A **payee** must be able to carry out the following use case and associated requirements:

Use case 1. Determine the status of a payment made.

Requirements:

Similar to the payer, a payee will be able to determine the status of a payment made to them. In the case of a payee, they will be able to:

a. Determine the position of the payments on its journey to them.
b. Determine the estimated time of delivery.
c. Determine when the funds have been received.

Rules:

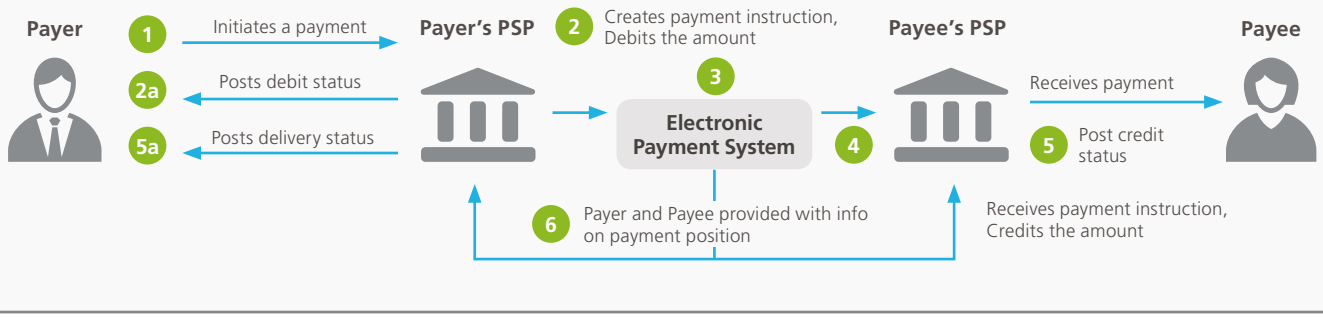
a. In the event that a payment does not reach the payee's account in real-time either by design or in error, then a payee should be able to determine where the payment is in the process and the reason if it has been halted or delayed.
b. Any advice to an end-user concerning the processing/non-processing of a payment should consider regulatory requirements including, for example, provisions around 'tipping off'.
c. Confirmation of receipt must include time, date and delivery account number.

[27] Feedback from our conversations with corporates and government was that they will only use this functionality in exception cases - when a payment has failed or gone wrong.
[28] Cash payments will not be tracked. Before they are paid in, cheques will also not tracked. Once paid in, they will become electronic and thus trackable.

End-to-End Journey – Payments Status and Tracking

Figure 2.12 illustrates the end-to-end journey for Payments Status and Tracking.

FIGURE 2.12 PAYMENTS STATUS TRACKING END-TO-END JOURNEY



Step 1 Payer initiates a payment by providing PSP with payment details and instructions.

Step 2 Payer's PSP creates payment instruction and initiates it. The payer is provided with information on the debit status of the payment (2a).

Step 3 Payment passed on to the payment systems.

Step 4 Payee's PSP receives payment instruction and credits payment to payee's account.

Step 5 Information on credit status provided to the payee. The payer is provided with information on the payment being credited to the payee (5a).

Step 6 Throughout the journey, the payer and payee are provided with information on the payment's position.[29]

Question 2.18

The NPA will fully support the functionality for PSPs to provide payment status and tracking.

a. As a PSP, what is the extent of change you think you will need to carry out internally to offer Payments Status Tracking?

b. What challenges do you see that might prevent your organisation adopting Payments Status Tracking?

[29] Further detail on how Payments Status Tracking will be supported by the NPA can be found in Appendix 4.

Key Risks and Considerations for Assurance Data

We identified several key risks and considerations. For each risk, we have identified mitigation. The risks are summarised in Table 2.2 below.

TABLE 2.2 KEY RISKS AND MITIGATION FOR ASSURANCE DATA

Description	Mitigation
1. 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.
2. Data privacy, protection and ownership As CoP could require sharing sensitive information and data between end-users, there is a 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.
3. Proceeds of Crime Act and 'Tipping off' clause Proceeds of Crime Act 2002 make it an offence for any PSP to 'tip off' (i.e. inform) a payer if they are under investigation for any offences covered by this act. This is a risk in the provision of information on a payment's status and tracking. PSPs must comply with this regulation whilst they provide payments status and tracking capability to payers.	Service providers must ensure that the design is compliant with this regulation.
4. 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 an end-user can opt-out of the service.
5. 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.

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 re-confirm 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.[30]
3. **End-user interface design and experience:** CoP and Payments Status Tracking service providers will be tasked with determining the best way to present the various functionality and capability to the end-user. In doing so, there must be consideration to ensure that these interfaces allow the end-user to interact 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 and receive 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.

Question 2.19

We have highlighted several considerations relevant to the delivery of Assurance Data. As an end-user of Assurance Data:
a. Are there any risks that we have not addressed or highlighted that you would like to add?
b. Are there any unintended consequences that we should consider?

2.4 Enhanced Data

Background

In our Strategy, we identified several detriments 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 free-form in nature; 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.

What is Enhanced Data?

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[31] 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.

[30] PSPs may choose to recycle account numbers once a payee closes an account. We have only identified two PSPs who recycle accounts.
[31] 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.

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,[32] 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.

End-User Requirements – Enhanced Data

The primary end-users of Enhanced Data will be the payer and the payee. 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:

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

In our 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 reconcile a payment to their internal systems accurately and efficiently. We are however conscious that this is not the only use case for Enhanced Data. In our work with the various end-users we have identified numerous additional use cases. E.g. business intelligence through data analytics and processing, customer marketing and loyalty programs, machine learning, fraud detection etc.

With this in mind, we have specified a core set of requirements that address the key detriment 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 Figures 2.13 and 2.14.

FIGURE 2.13 PAYER REQUIREMENTS – ENHANCED DATA

A **payer** must be able to carry out the following use cases and associated requirements.

Use case 1. Add additional data to the Payment.

Requirement:

A payer making a payment will be able to add information related to the payment.

Rules:

a. Where applicable, all additional data[33] must be formatted suitably, compliant with NPA message standards at either end.

b. The payer must be able to see detail of their payment independent of whether the payment has actually been settled.[34]

c. All legal and regulatory requirements must be complied with at all times by all data processors and data stores.[35]

Use case 2. Identify Payment.

Requirement:

Payment identification is through the provision of sufficient information on the payment.

Rules:

a. Where applicable, all additional data must be formatted suitably, compliant with NPA message standards at either end.

b. The payer must be able to see detail of their payment and the data attached independent of whether the payment has actually been settled.

c. All additional data included in payments must be accessible through any channel through which the payer is able to see the payment. This may not be possible through analogue channels.

[32] 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.

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

[34] In cases of failed payments or non-instant payments (Bacs) the payer must be able to always access the payments enhanced data.

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

FIGURE 2.14 PAYEE REQUIREMENTS – ENHANCED DATA

A **payee** will be able to use Enhanced Data to:

Use case 1. Reconcile a payment to an account.

Requirement:

The payment will be able to carry sufficiently structured remittance information to allow the payee to identify the appropriate account to apply the payment – to whom does this payment belong to?

Rules:

a. Payee must receive all data exactly as included by payer.

b. To allow ubiquity, a common standard data structure will be required[36] for the remittance information.

c. The NPA will provide standard APIs to load or extract Enhanced Data to and from a payment.

d. The integrity of the data will be assured between any two end points i.e. no truncation, alterations, loss etc.

e. Adequate security will be put in place to ensure the data is secure at all points.

Use case 2. Reconcile a payment to a transaction.

Requirement:

The payment will also carry sufficiently structured remittance information to allow the payee to determine what the payment is for – what transactions does this payment relate to?

Rules:

a. To allow ubiquity, a common standard data structure will be required for remittance information.

b. The NPA will provide standard APIs to load or extract Enhanced Data to and from a payment.

c. The integrity of the data will be assured between any two end points i.e. no truncation, alterations, loss etc.

d. Adequate security will be put in place to ensure the data is secure at all points.

Question 2.20

As a payer:
a. How would you use Enhanced Data?
b. What Enhanced Data would you add to payments?

Question 2.21

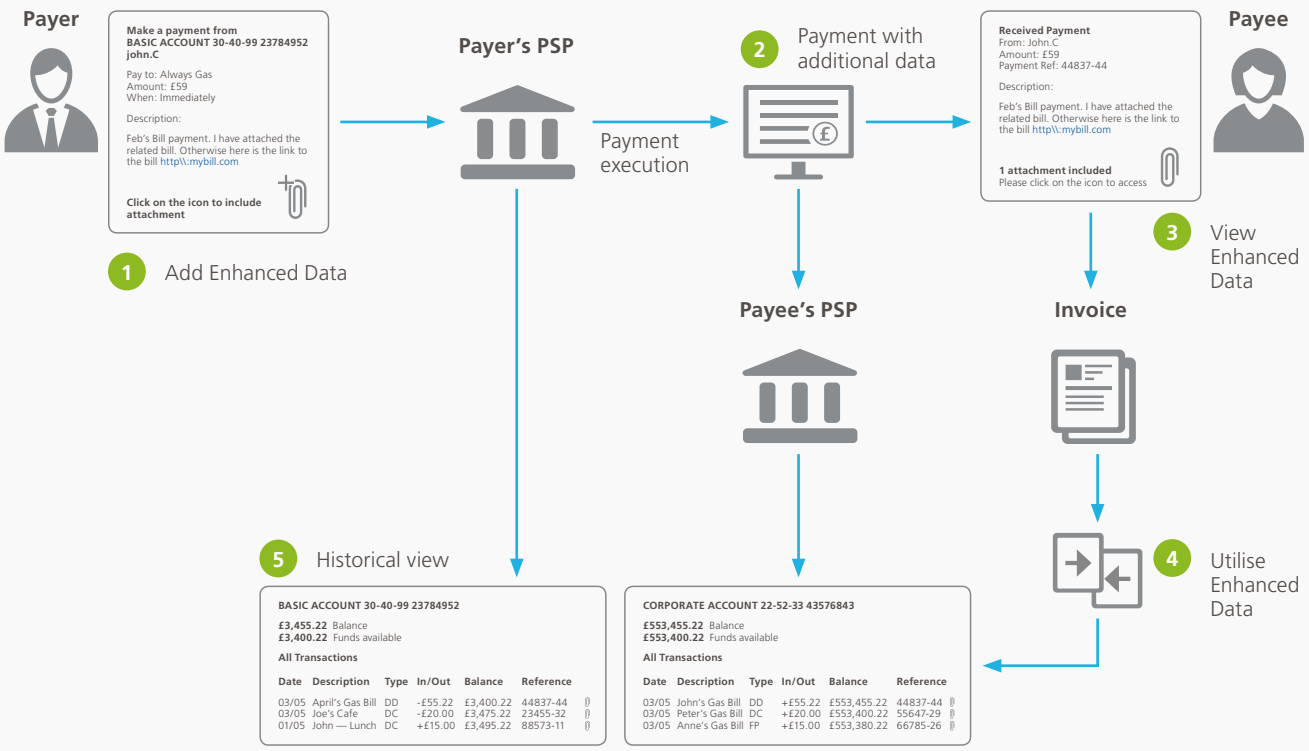
As a payee:
a. How would you use Enhanced Data?
b. What Enhanced Data would you add to payments?

[36] The Enhanced Data capability will use ISO 20022 as a common messaging standard in line with the NPA.

End-to-End Journey – Enhanced Data

The overall end-to-end Enhanced Data journey is shown in Figure 2.15.

FIGURE 2.15 END-TO-END JOURNEY ENHANCED DATA



Step 1 The payer adds Enhanced Data to a payment. E.g. gas bill or hyperlink.

Step 2 Payment travels to the payee's PSP with Enhanced Data included by the payer.

Step 3 Payee accesses the Enhanced Data provided through APIs or PSP interfaces.

Step 4 Payee utilises Enhanced Data to reconcile the payment to the payer's account.

Step 5 Both payer and payee are able to access Enhanced Data added to historic payments[37] made or received through APIs or interfaces provided by PSPs.[38]

Question 2.22

Does the Enhanced Data capability as described address the detriments identified in our Strategy?

Question 2.23

Some changes will be required to enable the loading and retrieval of Enhanced Data. For example, corporates will need to modify their internal systems.

As an end-user, what internal change will be needed to allow you to add and receive Enhanced Data through the NPA?

[37] Length of time data is accessible subject to prevailing Data retention policies and regulations.
[38] Further detail on how Enhanced Data will be supported by the NPA can be found in Appendix 4.

Key Risks and Considerations for Enhanced Data

Several risks were identified related to Enhanced Data. They are summarised in the Table 2.3.

TABLE 2.3 KEY RISKS AND MITIGATION FOR ENHANCED DATA

Risk	Mitigation
1. 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 existing and upcoming data privacy regulations, including but not limited to 4MLD and GDPR.
2. 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 existing and upcoming data ownership regulations, including but not limited to 4MLD and GDPR.
3. Data Structure There is the risk that if 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 4MLD. It's important to be aware that existing regulations might not completely cover data structure risk mitigation in its entirety.
4. 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 4MLD and GDPR. It's important to be aware that existing regulations might not completely cover data storage risk mitigation in its entirety.

Additionally, the following should be considered:

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.
2. 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.
3. **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.

Question 2.24

We have highlighted several considerations relevant to the delivery of Enhanced Data. As an end-user of Enhanced Data:

a. Are there any risks that we have not addressed or highlighted that you would like to add?
b. Are there any unintended consequences that we should consider?

Question 2.25

We recognise that additional work needs to be done in identifying safeguards including liability considerations associated with Enhanced Data. As an end-user of Enhanced Data:

a. What are some of the liability concerns that you may have?
b. Would you be interested in working with the Forum to define, at a high-level, the various liability considerations required for Enhanced Data? If so, please contact us as soon as convenient through the Forum website so we can get you involved.

2.5 Next Steps

We have assessed the next stages of activity required to complete development of the Requirements and Rules for the 3 EUN solutions. In addition to receiving and assessing responses to the consultation questions, we will carry out further work across the EUN solutions on:

1. Risks and liabilities across the EUN solutions.
2. Data Protections and Privacy implications across the EUN solutions especially as pertains to GDPR.

We invite expressions of interest from various end-user groups to participate in the above two activities.

3.0 Implementation Plan

This section outlines our proposed implementation plan and approach for transition to the NPA. We list the principles and assumptions underpinning the implementation plan and detail our four transition states. Beneficial impact to end-users, risks and mitigations as well as dependencies on developments across the industry influencing the implementation plan are also discussed. We present a strawman implementation timeline, as well as a customer delivery timeline.

Whilst the implementation plan and transition phases should be viewed in its entirety, the architectural timeline in section 3.3 will be of particular interest to vendors and Payment System Operators (PSOs). The customer timeline in section 3.4 will be most pertinent to vendors, PSOs, Payment Service Providers (PSPs) and end-users (corporates, government and individuals).
The transition approach in section 3.5 will be most relevant to PSOs, who will be able to see the migration status of payment types as implementation progresses.

3.1 Introduction

3.1.1 Key Principles

Six key planning principles have been defined to support the creation of the implementation plan. The principles are in line with our Strategy:

Ensure customer considerations are at the heart of any solution development plans.

- Requirements driven and aligned to end-user needs: Shall be fit for purpose and there will be a clear need for any functionality being implemented.
- Ubiquity and ease of use: Subject to legal and regulatory consideration, services will be commonly available to all (both end-users and PSPs). The plan will ensure simple access and be easy to adopt by all.

Facilitate collaboration with industry participants in the development of solutions where appropriate.

- Standards compliant and interoperable: The plan will map out steps required for migration to the defined and agreed industry standard. Adoption of this standard will be a requirement for participation to ensure interoperability.
- Simplicity: The plan will avoid unnecessary complexity in order to reduce risk and to support a simple delivery of the NPA.
- Adopt and enhance market best practice: The plan will align to existing or emerging industry activity recognising that the plan may need to set new market practice in some areas.

Recognise wider industry developments when developing the plan.

- Flexible and extensible: The plan must be capable of being adapted or extended to meet emerging changes to business requirements and to allow for varied pace of participant adoption.
- Optimal: The plan will be optimised to account for concurrent industry activity and other deliverables, ensuring timely delivery and benefits realisation.

Use best practice in technology implementation.

- Safe and Secure: The plan must maintain and, where possible, improve the existing security, integrity and fraud resistance of all aspects of the end-to-end payment transaction.

Provide optimum benefits for stakeholders.

- Maximum benefits at lowest cost and risk: The plan will aim to maximise benefits generated for the customer, the industry and wider UK economy at the lowest overall risk and cost.

Agree plan approach with regulatory bodies including transition through to end solutions.

- Trust and confidence: The plan must maintain the trust and confidence that participants have in the environment today, while minimising residual risks in existing processes.
- Business continuity and integrity: Plan sufficient resilience and controls to accommodate both planned downtime and unforeseen incidents without service loss or impact on data integrity, maintaining continuous deployment.

Question 3.1

Are there any additional principles you think we should add or significant amendments that should be made to those already stated?

3.1.2 Planning Assumptions

Assumptions outlined in this section have been used to inform activities in undertaking the overall NPA design and plan. The assumptions are:

End-users will have the same transaction capabilities as they do today or better.

- End-users comprise consumers, businesses and the government.
- They will receive communications about any beneficial changes throughout the implementation.
- As a minimum they will be able to transact as they do today with any changes being due to enhancements such as more functionality and greater choice.

NPA implementation will mitigate systemic risk.

- NPA will supersede the existing BPSL, FPSL and (in time) ICS infrastructures through a safe and sensible transition whilst maintaining the resilience and robustness of payment processing.
- Bacs Direct Debit functionality will become an NPA overlay service.
- CHAPS, Cards and LINK are out of scope.
- RTGS will be used for settlement in central bank money.

Existing payment services functionality will continue or improve under NPSO oversight.

- Existing services include (but are not limited to): mobile proxy look up service, account transfer services (current accounts and Individual Savings Accounts), bulk payment redirection, biller update service and EISCD.
- These services will need to continue during and after transition to the NPA.
- Any services that are discontinued for BAU reasons will not need to be supported and can be closed once the activity has ceased.

A managed and phased approach to implementation.

- Existing schemes, their services and systems will be maintained to run in parallel with the NPA for sufficient time to allow a phased migration; 'roll back' capability (within the determined period) will provide migration flexibility.
- All users of the schemes will be able to migrate to NPA in phases to mitigate volume transition risk, allowing for a broad range of readiness timeframes; there will be no 'big bang' implementation.
- Where appropriate, new overlay services will support the execution of payment instructions across existing payment schemes (e.g. BPSL, FPSL and ICS) and the NPA to enable early delivery of end-user benefits.

Each payment scheme can be transitioned independently.

- BPSL, FPSL and ICS transition to NPA will be independent of each other and can run in parallel.
- Institutions will be able to send and receive payments via existing and/or NPA route during the transition phase.
- Close down of BPSL, FPSL and ICS infrastructures will occur at pre-determined dates and can happen independently of each other.

NPSO will be responsible for governance, rules, standards and delivery.

- PSPs / TPSPs will require accreditation before using the NPA.
- The operation of any overlay services will need to comply with the NPSO rules and governance and will be approved by the NPSO to ensure NPA interoperability.
- NPSO will determine the closing dates for legacy infrastructure.

PSPs / TPSPs will manage end-user interfaces and proposition competitively.

- User interfaces and customer channels will remain in the competitive space.
- Individual institutions will be able to develop and tailor their own propositions independently, unless there is a compelling end-user benefit from rules specifying some elements of the user's experience (such as for consistency and ease of adoption).

Transition solutions will be in place to support the close down of legacy infrastructure.

- Transition solutions will alleviate the burden of having to immediately change formats enabling a phased adoption – e.g. converting payment messages from 'old' format to NPA format.
- Transition solutions will still require a definitive end date to ensure transition solutions can 'retire'.

Transition will be planned to provide continuity with minimal user impact.

- Transition and migration will be carefully planned to ensure maximum availability.
- From a predetermined date, all PSPs will be required to receive NPA derived payments.
- All PSPs will be required to continue to receive the legacy payments that they currently receive until legacy infrastructures are closed or switched through a transition solution.
- PSPs can make other account types (e.g. mortgage accounts) reachable at their own discretion.

Question 3.2

Are there any additional assumptions you think we should add or significant amendments that should be made to those already stated?

3.1.3 Stakeholders

The fundamental objective of the Forum is to identify, prioritise and develop strategic and collaborative initiatives to promote innovation in the interests of Payment Service Users (PSUs). PSUs, in the capacity of either a Payee or Payer when making use of a payment service, are the ultimate stakeholders (beneficiaries) of these initiatives.

It follows that the benefits of collaborative initiatives can only be achieved through the involvement of all other parties that create the payments environment including: PSUs; PSPs (existing and new); Third Party Service Providers (TPSPs); PSOs (existing and new); infrastructure and solution providers and Regulators. Therefore, we will continue to engage all relevant stakeholders throughout the implementation of the NPA.

3.2 Relevant Industry Change

The payments environment is undergoing a period of significant change and the Forum recognises the dependencies on other important industry-wide programs. The NPA has been designed to leverage industry initiatives where possible and to manage risk in areas where it is not feasible to align the NPA to broader change.

The risks involved with the level of complexity and volume of change is discussed in Section 3.4.1.

Further detail on the following industry initiatives can be found in Appendix 2; the considerations for implementation planning in light of these initiatives are in Table 3.1.

TABLE 3.1 INDUSTRY CHANGE AND IMPLEMENTATION PLAN CONSIDERATIONS

Industry Change	Considerations
Bank of England – Real Time Gross Settlement Review	• Relevant Settlement functionality is expected to be delivered in 2020. • The change will impact all direct settlement users across existing and future payment solutions. • Changes in access may increase the number of new 'direct' participants. • Any amended resilience / liquidity requirements may also impact the final NPA design.
NPSO – Set-up and Governance	• Dependency on the NPSO becoming operational and putting in place the required governance. • This could include rules for how the NPA and overlay services can operate within the NPA.
PSR – Infrastructure Market Review (see below for further detail)	• Definition of principles for procurement of new infrastructures. • Requirement for introduction of common standards. • There are requirements to run a competitive procurement and introduce ISO 20022 for the next central infrastructure services contract for the existing BPSL and FPSL systems.
PSD2 and Open Banking regulations – UK implementation	• Defining how TPSPs and PSPs will operate in the new Open Banking environment. • Successful delivery of the API ecosystem. • NPSO rules and governance will leverage the registration and accreditation processes, avoiding unnecessary duplication.
EU GDPR regulations	• Critical development that will shape data handling within the NPA and any overlay services such as Confirmation of Payee.
Structural Reform – Ring Fencing	• Constraints upon impacted PSPs: o Conflicting development resource. o Change capacity constraints.

3.3 High-Level Illustrative Timeline

Using the principles, assumptions and relevant industry change as a guide, our implementation plan and transition approach has focused on the creation of a core timeline with the beneficial impact on users in mind.

3.3.1 Strawman

Figure 3.1 illustrates the strawman phased approach for the NPA's implementation. It is acknowledged that historically, migrations involving bulk payments (e.g. Bacstel IP and SHA-2) have taken two to three years, plus implementation planning. A key planning assumption for this timeline is, however, that the market will provide transition solutions to support users, particularly for bulk payments. Early interactions with solution providers suggest that such solutions can be made available and have the potential to provide a faster track to migration onto the NPA. Our approach assumes a transition period of 1.5 years for FPSL and BPSL, and 1 year for ICS.

Sequencing

It is expected that requirements gathering for the new payment mechanism will continue into 2018 and will lead into the procurement phase. With the delivery of the majority of functionality expected in 2020 from the Bank of England's RTGS renewal, we have aligned the NPA implementation date to Q1 2021.

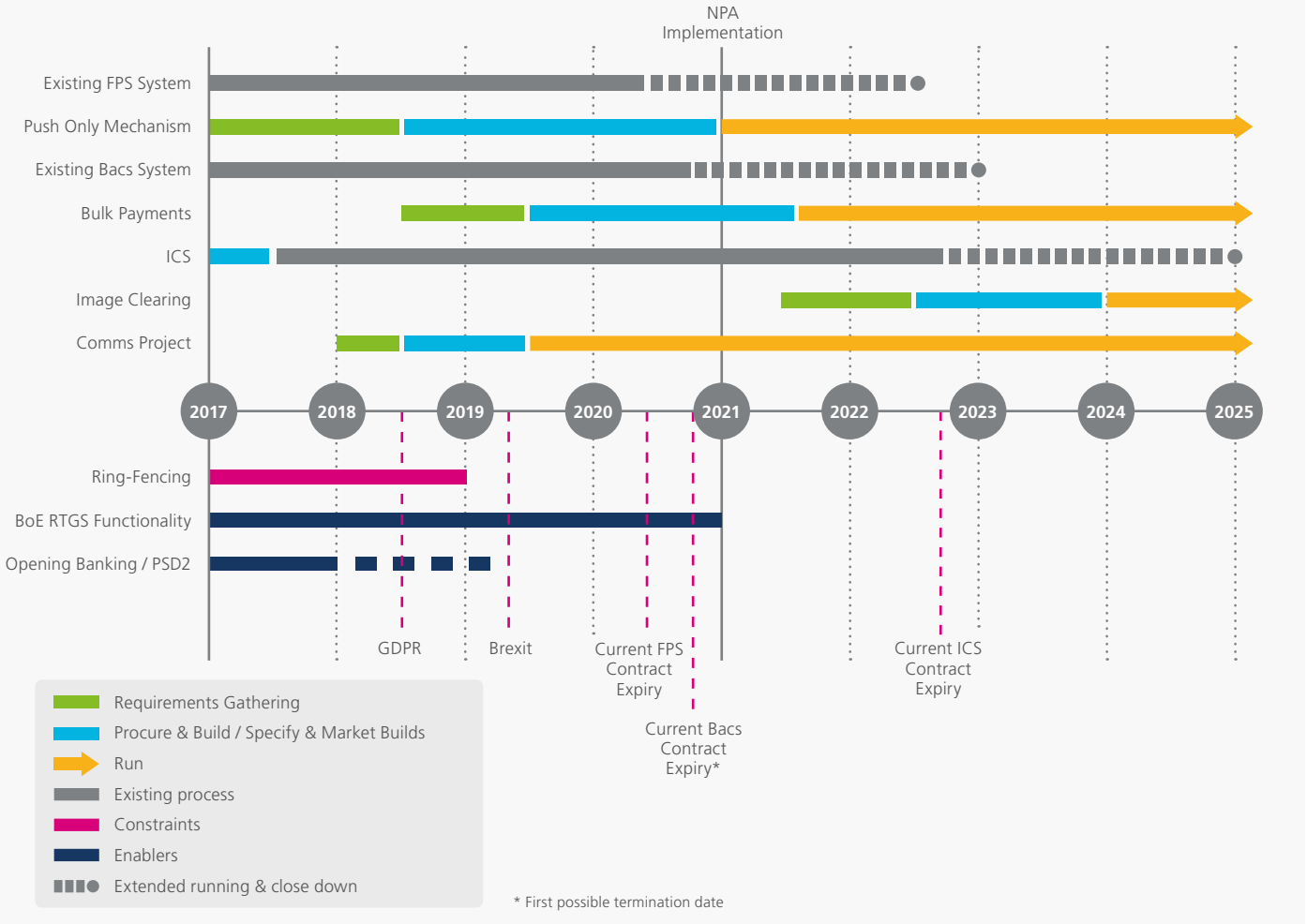
It is envisaged that the capability to handle bulk payments will be available six months later, enabling the start of Bacs payment volume migration. Image clearing functionality will be added by the start of 2024, enabling the migration of the ICS volume.

By 2025, all payment volume from legacy Faster Payments, Bacs and ICS infrastructures will have migrated to the NPA and the legacy systems will have been closed down.

Question 3.3

Do you agree with the sequence of events laid out in the implementation plan? If not, what approach to sequencing would you suggest?

FIGURE 3.1 STRAWMAN IMPLEMENTATION TIMELINE



3.3.2 Influencing Factors

As set out in Section 3.2, the industry is engaged in significant change activity. This has to be accounted for alongside any planning activity for the NPA, adding to the overall complexity to be managed across the industry. There is an appetite however, to deliver the NPA promptly to achieve the benefits at the earliest opportunity.

Any timeline delay, either as a result of dependencies or a specific NPA delay, will likely have impacts such as:

- Delayed benefits realisation.
- Extended legacy infrastructure costs.
- Potential interim procurement need (for existing schemes).
- Increased risk of existing ageing technology infrastructure requiring renewal.

The changes being contemplated are significant and wide ranging in their impacts. Therefore, precise timings, including aspects such as dual running periods for legacy infrastructures, will not be determined until a full specification is defined in the subsequent work phases. This could include planning for sequencing of different payment types, e.g. bulk credits and bulk debits.

The PSR's Infrastructure Market Review has now published its final remedies. PSR Specific Directions 3 and 4 place requirements on FPSL and BPSL (and NPSO in due course) to undertake competitive tendering for the next contract for central infrastructure when the current contracts terminate in 2020. The transition to the NPA, as shown in the high-level timeline in 3.2.3, indicates that the existing FPSL and BPSL systems will terminate not long after this time – by June 2022 and end 2022, respectively.

The PSR's Infrastructure Market Review has now published its final remedies. PSR Specific Directions 3 and 4 place requirements on FPSL and BPSL (and NPSO in due course) to undertake competitive tendering for the next contract for central infrastructure when the current contracts terminate in 2020.

The transition to the NPA, as shown in the high level timeline in 3.2.3, indicates that the existing FPSL and BPSL systems will terminate not long after this time – by June 2022 and end 2022, respectively. The PSR noted in its final remedies decision that the directions need to be flexible to allow for the implementation and transition to the NPA. The PSR's directions allow for FPSL and BPSL to apply to extend the due date for when they must complete a competitive procurement.

3.4 Customer Timeline

End-user needs will be satisfied through both new (e.g. enhanced data), existing and competitively delivered service propositions. Figure 3.2 below sets out a customer delivery timeline, illustrating when customers may begin to realise benefits from the NPA.

It is important to note that end-user overlay solutions will be delivered competitively. In order to achieve ubiquity, and thus a successful service, a wider set of end-users will have to adopt those solutions. Existing overlay services such as Current Account Switch Service (CASS), bulk redirection etc. will be in place to support the NPA as transition commences.

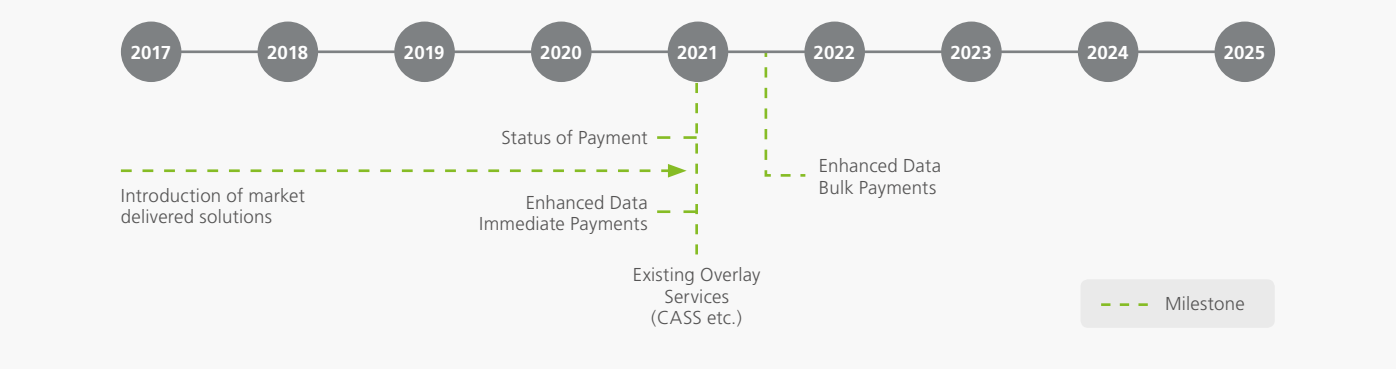
The timeline takes into consideration the development of overlay solutions. We are aware of competitive, market-led solutions, based on our requirements and rules that could be delivered ahead of 2021. Any implementation will be independent of payment methods and therefore could be delivered onto existing schemes prior to the NPA's implementation and ported into the NPA at a later date.

It is expected that CoP and Request to Pay overlay services will be available through the NPA from the start of 2021, and will be provided competitively by TPSPs and PSPs. We have also assumed that the NPSO will ensure that its governance, rules and NPA configuration will be able to support such solutions. The market delivery of these services is not within the remit of the NPA and NPSO. It should be recognised that the timeline shown is indicative only.

Question 3.4

Do you agree with the the high-level timetable laid out in the implementation plan? If not, what timing would you suggest?

FIGURE 3.2 CUSTOMER DELIVERY TIMELINE



3.4.1 Risks

A number of implementation risks under the five key headings of Customer, Industry, Delivery, Technology and Stability were identified in the Strategy. For this phase of activity, we have re-examined these risks in light of the proposed architecture, potential implementation and phasing timeline.

At this stage, we have identified ten major risks needing mitigation, which have been classified into four key risk types illustrated in Figure 3.3 below. Subsequent phases will continue to analyse and define these proposed risks.

Further detail on the risks we have examined can be found in the Implementation Plan supporting document.[39]

The NPSO will further consider these risks as the definition for the NPA becomes clearer. This will enable more detailed assessment of the associated mitigations. The outcome of this assessment will be critical to ensuring that the mitigations proposed are robust and deliver both a timeline and architecture that fits within the overall risk appetite for the NPSO and wider industry stakeholders.

FIGURE 3.3 IMPLEMENTATION RISKS AND MITIGATIONS

Risk Type	Description	Mitigation
Design	• The high level design is conceptual with unproven parts – e.g. bulk payments solution. • High dependency on parallel change programmes – e.g. PSD2 / Open Banking. • Over-engineering may deter suppliers.	• Extensive stakeholder engagement to validate the detailed definitions prior to tendering. • Ensure the NPSO has the right delivery capability and approach. • Effective design socialisation and validation.
Implement	• Lack of transition capacity to implement, build and test within the timescales. • Industry and customer ability to adapt to change.	• Deliver in-depth industry agreed implementation and transition plan. • Develop detailed understanding of all end user needs and incorporate into overall programme.
Operate	• Service is interrupted during transition. • No embedded knowledge of new system elements. • Resilience / vulnerabilities are exposed.	• Agree phasing of migration and parallel running. • Extensive consultation and knowledge transfer to all stakeholder groups. • Resilience and security to be at the core of programme.
Adopt	• Increased fraud exposure during transition. • Pace of change is impacted by end user / PSP capabilities with insufficient priority delaying transition and adoption.	• Engagement with financial crime prevention representatives across industry. • Best practice implementation techniques for large scale projects with clear migration milestones.

Question 3.5

Are there any significant potential risks that you think the implementation plan does not consider? If the answer is yes, then please provide input about what they are and how we can best address them.

[39] The Implementation Plan supporting document can be found at: https://implementation.paymentsforum.uk/consultation

3.4.2 Communications

Effective communication will be a critical success factor for implementation given the wide reaching nature of the changes being introduced to the UK's payments landscape. Sufficient lead time needs to be factored in to allow organisations to budget and plan for any required changes they may need to make, such as registering and / or gaining accreditation for participation in the NPA.

Communication and socialisation could potentially include traditional media such as TV and radio, online media, social media, email and dedicated websites. Engagement methods could include working groups, workshops, roundtables, 1-2-1 meetings, agency days and webinars.

A more detailed communications plan will be developed in subsequent work phases. It will leverage the learnings and best practices from other large scale industry projects such as Faster Payments, Paym, CASS and the C&CCC Image Clearing System.

3.5 Transition Approach

3.5.1 Transition Objectives

In developing the transition approach, we have taken into account the PSR's recent market review report 'Ownership and Competitiveness of Infrastructure Provision'. The transition approach proposed is designed to ensure interoperability, continuity of service and minimal disruption.

In addition, the transition to the NPA must achieve the primary goal of ensuring that the migration does not introduce any instability or excessive risks. To achieve this goal, a number of transition principles have been established. The transition approach should:

- Be phased, as this is least disruptive to the market, reduces transition risk and the likelihood of failures and introduces a transitionary period that allows PSPs to develop or upgrade their systems over time.
- Keep transition periods as short as possible, without creating unnecessary risks to keep the costs low and reap the benefits as early as possible.
- Avoid detrimental impact to the integrity of UK electronic payments during the migration to and adoption of ISO 20022; avoid detrimental customer impact (across all customer segments) and avoid introducing uncontrolled risks.
- Facilitate the transition of PSPs from the current payment models to the NPA.
- Ensure that the current and new systems run independently of each other for clearing.
- Minimise the impact on the existing payment schemes during transition.
- Permit an orderly and prompt closure of the existing schemes, to ensure optimal benefits realisation.

Our analysis discounted a 'big bang' approach due to the inherent risk to stability. It also discounted a 'phased send and receive approach' on the grounds that there are additional complications of sending data between the NPA and the current payment systems that would result in data truncation and create the need for too many disposable transition development states.

3.5.2 Transition Approach – Component Phasing

We have defined four periods of phased activity. Together they will deliver a successful implementation of the NPA and migration of legacy payment volumes, as well as subsequently ensuring that existing scheme processing capability is closed down.

The phases use a series of architectural positions known as 'Transition states' to describe the particular layers and components that need to be delivered to provide the functionality described within each state. Further detail on each of the transition states and what each will mean to end-users can be found in Appendix 5.

Transition State 1: Single Payments
(all PSPs capable of receiving Single Payments).

Transition State 2: Bulk Payments
(all PSPs capable of receiving bulk Payments).

Transition State 3: Image Clearing System.

Transition State 4: Close down of legacy services completed
(a parallel activity aligned to the status of the other transitions) – FPSL in June 2022, BPSL at the end of 2022, ICS at the end of 2024.

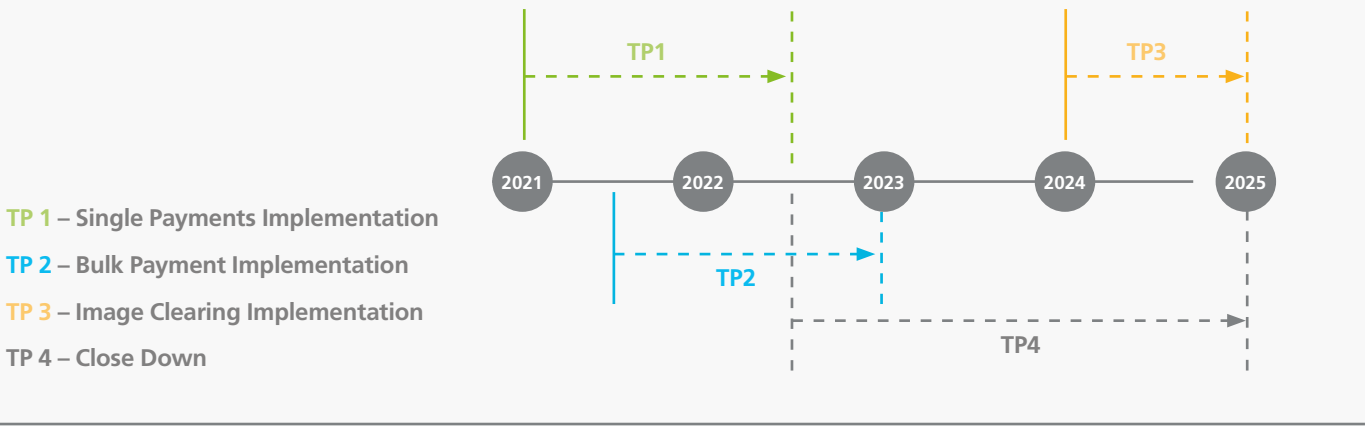
The first three transition states will coincide with the delivery of the layers of the NPA. The final fourth transition state will coincide with the close down of the existing infrastructure once all payments have migrated to the NPA. This process is expected to start with FPS.

We propose that all participants should be able to receive single immediate payments on the day of the NPA launch ('Day 1'). We rely on all PSPs being ready on Day 1 to receive payments from the NPA, which aligns with the approach taken by ICS also. The implication of this approach is that PSPs may need to run existing, as well as new, payment systems in parallel and cover such set-up costs until the old payment scheme is shut down.

The strawman implementation timeline in Figure 3.4 illustrates the period that each of the Transition States will exist for and how they overlap.

The implementation timeline proposes 4 key transition periods (TP).

FIGURE 3.4 TRANSITION PERIODS



Question 3.6

Do you agree with our proposed transition approach? If not, please provide your reasoning.

3.6 Next Steps

We have assessed the next stages of activity required to ensure a successful handover to the NPSO at the end of 2017. We will define a handover process with a detailed timeline which will take into consideration the consultation responses, further expanding on the principles and assumptions underpinning the implementation plan and a record of artefacts.

Another action is to manage risks appropriately. It is envisaged that we will review the assessment of the mitigation factors, socialise our findings with a wider audience and define minimum hurdles to satisfy industries appetite for risk.

Due to the number of industry related initiatives impacting the payments community, we plan to identify synergies between the NPA and current industry initiatives to ensure a smooth handover to the NPSO.

Further detailed analysis is also needed for the implementation timeline and options for Bacs Direct Debit and Direct Credit solutions. We will expand on our current high-level transition plans and consider options available to the NPSO. This will require a consensus view from the wider payments community to ensure our assumptions are correct, which will feed into a refined plan.

Lastly, we will analyse the consultation responses and assimilate appropriate changes. A revised final output will go through a socialisation process with sign off from the Forum.

4.0
Cost Benefit Analysis of the NPA

In this section, we set out our analysis of the costs and benefits associated with delivering the three End-User Needs (EUN) solutions. We compare this to the costs and benefits of keeping the existing systems separate and carrying out a minimum upgrade of each. We believe this section will be of most interest to PSPs, PSOs and vendors.

4.1 Introduction

We prioritised three EUN solutions (the 'overlay services'): Request to Pay, Assurance Data and Enhanced Data. This section looks at the benefits these solutions would deliver, and the costs that would be incurred to implement the NPA to deliver them. We compare these to the costs and benefits of an alternative upgrade that would be a minimum approach in the absence of the NPA, as we believe that to 'do nothing' is not an option. This is largely as a result of the PSR's Infrastructure Market Review, which requires BPSL and FPSL to upgrade their existing central infrastructure to be ISO 20022 compliant at re-procurement, that is, by 2020.

In this alternative minimum upgrade, we assume that the three EUN overlay services are not delivered. We take this view due to technical limitations, for example, the lack of full end-to-end ISO 20022 compliance inhibiting the delivery of Enhanced Data; and ongoing complexity that would be inherent in a minimum upgrade, which would continue the parallel running of three infrastructures.

The remainder of this section considers the costs and benefits of the two scenarios. We consider:

- The benefits of adopting the NPA.
- The cost of delivering the NPA.
- The benefits of the Alternative Minimum Upgrade.
- The cost of the Alternative Minimum Upgrade.

4.2 NPA Benefits

Our analysis shows that there is a gross benefit opportunity of between £11.5 billion and £14 billion associated with the NPA in the period 2019 to 2031. This includes the incremental benefits of the EUN solutions and a continuation of the benefits delivered by the existing Bacs, FPS and Image Clearing System (ICS) services. We include the latter as these services (and their benefit) will continue to be provided through the NPA.[40]

We estimate that the incremental gross benefit of introducing the three overlay services is £7.4 billion – £9 billion.

Details of benefit narratives and estimates can be found in Appendix 6. Table 4.1 provides a high-level summary of the range of benefits associated with the implementation of the NPA and overlay services.

There are also significant qualitative benefits that will come from deploying the NPA and the EUN solutions. The NPA, underpinned by the flexible layered architecture and simplified access, will support easier access and more competition between PSPs and other providers relative to existing systems. Less onerous direct access for PSPs is an important qualitative benefit identified by stakeholders. The flexible architecture will also make change easier at both institutional and industry levels. It will enable simpler delivery of new innovative services – future user needs will be more easily met.

For the overlay services, qualitative considerations include the wider societal benefits of the three EUN solutions. Overlay services could improve financial inclusiveness, customer experience and trust in electronic payment systems. For example, Request to Pay aims to give more control to end-users, notably when they have irregular cash flows due to the nature of their work schedule. These particular customers are currently reluctant to adopt a Direct Debit payment plan due to the risk of unarranged overdraft charges and other penalties.

We do not present a quantification of government benefits in this analysis. We understand however, that these solutions will provide benefits to government institutions as one of the major users of payments systems. The drive for a more efficient public sector will undoubtedly be aided by the NPA and these overlay services. Further, the expected greater financial inclusion which will come about from the planned changes will help drive the government's agenda in that area. In addition, the innovative solutions that will be facilitated by the NPA will also help support the government's digital agenda with benefit to the UK as a whole.

Therefore, the quantitative benefits attributed to NPA adoption and the EUN overlay services in this study should be interpreted as conservative, with substantial potential for greater financial benefit over time.

[40] We have conservatively assumed the benefit of the Bacs, FPS and ICS services are equal to the current operating costs of these services. This is based on the assumption that Bacs, FPS and ICS as they are currently being run generate benefits that are equal to the costs that participants in the current UK payments system pay to run them. We have also done this for the alternative minimum upgrade benefits.

TABLE 4.1 BENEFITS SUMMARY

Solution	Benefit	Benefits (2019 - 2031)
Enhanced Data	Auto-reconciliation could reduce payees' manual and invoice reconciliation costs.	£3,710m – £4,530m
Assurance Data	The solution would help reduce losses associated with invoice fraud.	£1,300m – £1,600m
Request to Pay	The solution would reduce average unit cost of producing and sending invoices for medium and large businesses.	£850m – £1,030m
Request to Pay	Improvement in liquidity and subsequent reduction in financing costs.	£550m – £670m
Request to Pay	Request to Pay is cheaper for businesses than re-presentation of a failed Direct Debit (DD).	£460m – £560m
Assurance Data	The solution would help reduce the losses to payers associated with misdirected payments.	£420m – £515m
Request to Pay	Request to Pay will make late payment processing for non-Direct Debit customers cheaper for medium and large businesses.	£80m – £100m
Assurance Data	The use of Confirmation of Payee by payers would help reduce the number of misdirected payments and thereby reduce their administrative costs to PSPs.	£45m – £55m
Benefits of Bacs, FPS, ICS services[41]	We have conservatively assumed the benefit of the Bacs, FPS and ICS services are equal to the current operating costs of these services.	£4,040m – £4,940m
Total benefits		**£11,455m – £14,000m**

Question 4.1

Are there any material quantifiable benefits that have not been included? If so, please provide details.

4.3 NPA Costs

In this section, we consider the aggregate costs faced by PSPs, PSOs, and infrastructure providers. These aggregate costs include the one-off capital costs of the NPA and the three EUN solutions, and the ongoing run costs associated with a migration to NPA.

Furthermore, costs considered comprise all required expenditure for the development and maintenance of the new system as well as the costs of maintaining the old systems during the transition period.

The costs estimated can be classified into a number of categories:

1. Capital expenditure.
2. Run costs i.e. operating expenditure of the NPA. This includes voluntary change costs and change costs that will be incurred to comply with regulation.
3. Parallel running costs i.e. running the current systems concurrently with the NPA temporarily until current systems are decommissioned.
4. Costs of overlay services, including capital expenditure and run costs.

[41] As noted above, this has been conservatively assumed to be equal to the operating costs to run the services.

The estimates for implementing and running the NPA (the capital expenditure, run costs and parallel running) do not include costs for end-users of the system (e.g. costs for corporate customers to connect to NPA and migrate from FPS and Bacs); these costs are assumed to be absorbed by either TPSPs or vendors, or as part of the natural upgrade cycle of end-users' systems. We do include end-user costs in our cost estimates of the overlay services to the extent where businesses must incur costs to use the overlay services to be able to realise the associated benefits of them (see Section 4.4).

4.3.1 NPA Capital Expenditure

The required capital expenditure will include a number of components: TPSPs & PSPs will be required to build or procure ISO 20022 gateway services for payment initiation, for example to facilitate Direct Debit over the NPA 'push' mechanism, PSPs will be required to receive and process payment files from a TPSP. This will involve ISO 20022 message construction, validation and transmission. In addition, network connectivity will be required to meet standards mandated by the NPSO. Furthermore, PSPs and TPSPs will be required to build the business processes to support these activities.

Finally, capital expenditure will include the resources required to procure and build NPA clearing and settlement for payments processing.

The estimate of these total costs to deliver the NPA, excluding the three EUN solutions is c. £850 million as shown in Table 4.2.

TABLE 4.2 UNDISCOUNTED NPA DELIVERY COSTS

Layer	Cost
TPSPs	£336m
PSPs	£444m
NPA clearing and settlement	£72m
Total	**£852m**

Assumptions

- Based on stakeholder feedback, in previous payments infrastructure initiatives such as FPS, ICS and Current Account Switch Service (CASS), the ratio of central infrastructure capital expenditure to costs to the rest of the industry costs is estimated to be 10:90. As per Table 4.3, our central infrastructure cost estimate is around 8% of the overall cost.
- As part of initiatives to improve the UK payments systems, PSPs and C&CCC have already invested in the Image Clearing System. These ICS capital costs, having been incurred, will be considered as sunk and excluded from the NPA costs.

4.3.2 NPA Run Costs

In order to estimate the run costs of the NPA (not including the run costs of the overlay services), it is necessary to understand the structure of the current interbank payment systems and the aggregate costs of all participants.

Modelling the run costs of the NPA will require adjustments to be made to the run costs of the current interbank payment system to reflect potential efficiency savings associated with the amalgamation of the current schemes.

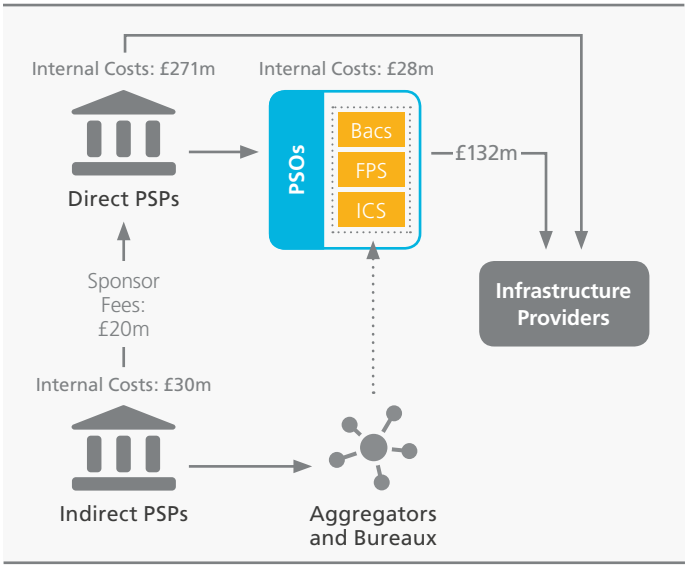
Run Costs Assumptions

The main assumptions made while estimating NPA run costs include:

- As with the current interbank payment systems, the NPA will have annual run costs to support and maintain the system.
- Subject to adjustments to reflect structural changes, the current systems' run costs are used as a proxy for the run costs of the NPA.

Figure 4.1 shows the parties in the payment infrastructure and the payment flows in and between the participants.

FIGURE 4.1 DESCRIPTION OF MAGNITUDE OF ANNUAL RUN COSTS



The total interbank system cost is estimated to be £480m per annum after adjustment for double counting.

Adjustments to annual current interbank run costs to model NPA

Evidence from stakeholder interviews suggest that a potential reduction in the payment systems annual run costs may occur if the existing schemes evolve into one system. In other words, efficiency savings may accrue as a result of a consolidation of the three existing systems when the NPA is adopted.

Table 4.3 shows the equivalent, estimated annual run cost efficiencies for different participants associated with a transition from the current schemes to the NPA.

TABLE 4.3 ADJUSTMENT TO ANNUAL CURRENT INTERBANK RUN COSTS AS A RESULT OF SCHEMES' CONSOLIDATION

Cost elements	Current services run costs	Potential cost savings %	Potential cost savings	Adjusted run costs
Direct PSP participants internal costs	£271m	15%	£41m	£231m
Indirect PSP participants internal costs	£30m	10%	£3m	£27m
PSO internal costs	£28m	10%	£3m	£25m
Infrastructure provider costs	£132m	30%	£39m	£93m
Sponsor fees	£20m	N/A	N/A	£20m
Total annual run costs	**£481m**	-	**£86m**	**£395m**

4.3.3 Parallel Running Costs

This section considers the cost implications of a phased transition from the current interbank systems to the NPA.

The transition assumption is that the current interbank payment systems (Bacs, FPS, ICS) will continue to run temporarily after the NPA goes live. The length of time of this parallel running will influence the magnitude of the parallel running costs.

On the basis of the parallel running assumptions made below, the total estimated parallel running cost is c. £1.9 billion – £2.3 billion.

Parallel running costs assumptions

The assumptions below have been made in modelling parallel running costs. These assumptions include:

- NPA will go live in 2021.
- Each participant in the payment system will have elements of their costs that are fixed and elements that are variable.
- To the extent that the costs incurred by the participants are fixed, they will be wholly incurred in existing systems and the NPA (the same level of fixed costs will be incurred in the current interbank systems as well as the NPA) as they run in parallel irrespective of payment transaction volumes. Variable costs on the other hand will vary with the volume of transactions i.e. these will be incurred on a per unit transaction basis.

Table 4.4 shows the fixed and variable cost proportions of the costs of the players.

TABLE 4.4 COST BEHAVIOUR (EXCLUDES SPONSOR FEES; ANNUAL COSTS)

Cost Element	Current annual run costs	Fixed Element	Variable Element
Direct PSP participants internal costs	£271m	£108m	£162m
Indirect PSP participants internal costs	£30m	£3m	£27m
PSO internal costs	£28m	£8m	£20m
Infrastructure provider costs	£132m	£119m	£13m
Sponsor fees	£20m	-	£20m
Total	**£481m**	**£239m**	**£242m**

During the transition from the existing interbank systems to the NPA, both existing schemes and the NPA will incur fixed costs as these will not vary with the number of transactions, so the aggregate value will be constant throughout the transition period. After the sunset of the legacy infrastructure however, only one set of fixed costs will be incurred. The implication of this is that the longer the transition period, the higher the aggregate parallel running costs will be.

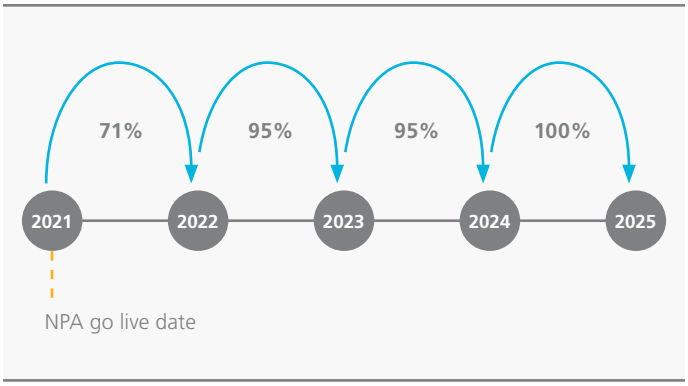
NPA adoption curve assumptions

The assumptions adopted for the transition from the current schemes are:

- FPS and Bacs payment transactions will migrate to the NPA within a 2-year timeframe from when NPA goes live; ICS will migrate by year 4.
- For FPS and Bacs, 75% of transactions will migrate in Y1 and the remaining 25% in Y2.
- A transition approach, as described in Section 3.5, will be in place to support the sunset of the legacy infrastructure. This will alleviate the burden of having to immediately change formats for corporate and government end-users.

Figure 4.2 shows the adoption and sunset curves over the four-year time horizon. The initial quick take-up is influenced by the two-year transition of the FPS and Bacs schemes.

FIGURE 4.2 AGGREGATE TRANSITION INTO NPA



Considering the three schemes of FPS, Bacs and ICS in aggregate, 71% of payment transactions will migrate to the NPA in the first year of NPA going live, and growing to 95% in the second year – at this point all of FPS and Bacs is assumed to have migrated. Finally, ICS payment transactions will commence migration in 2024 and this migration will take 12 months.

4.4 Overlay Services Cost

In our analysis, we include costs incurred by the NPSO, PSPs and TPSPs. Because we include the benefits of the overlay services to corporates, the government and charity end-users, we also include the costs these end-users incur with the introduction of the services.

For the purpose of this analysis, we assume that the majority of micro and small businesses are unlikely to invest in solutions to take advantage of the benefits of overlay services, hence we exclude potential overlay services costs and associated benefits of these business groups. The excluded businesses represent 33% of the UK turnover.

4.4.1 Request to Pay

It is estimated that capital costs across the industry (i.e. NPSO, PSPs and TPSPs) to deliver the Request to Pay solution will be approximately £100m (this excludes the cost to end-users). This cost will be incurred by TPSPs/PSPs on items such as building databases to store requests; user interfaces for consumers and back offices; applications; integration into billing systems etc.

In addition to this £100m, we estimate end-user costs of a further £100m, based on the adoption assumptions of Request to Pay by end-users (as shown in Appendix 6).

TABLE 4.5 REQUEST TO PAY COSTS

Cost type	Capital costs	Run costs (annual)
Establishing collaborative rules and standards admin by NPSO	£5m	£0.5m
TPSPs / PSPs	£95m	£9.5m
Total (excluding end-user costs)	**£100m**	**£10m**
End-user costs	£100m	£10m
Total (including end-user costs)	**£200m**	**£20m**

The total run costs are assumed to be approximately 10% of the capital expenditure to deliver the solution.

4.4.2 Assurance Data

We estimate the capital expenditure across the industry to deliver the Assurance Data solution to be c.£200m. The cost of this solution has been benchmarked with the cost to deliver other similar initiatives such as Paym, although in due course we may be able to refine this estimate using further analysis of API implementation costs. These capital costs will be incurred on one-off elements such as amending customer data, changing user interfaces, making core channel changes etc.

Unlike Request to Pay, there are no end-user costs associated with this service because it is assumed that an end-user can access this service using their current means of accessing payment services without modification.

TABLE 4.6 ASSURANCE DATA COSTS

Cost type	Capital costs	Run costs (annual)
Central Infrastructure	£20m	£2m
TPSPs / PSPs	£180m	£18m
Total	**£200m**	**£20m**

The total annual run costs are assumed to be about 10% of the capital expenditure to deliver the solution. This includes maintenance, support and change costs.

4.4.3 Enhanced Data

Our analysis assumes the bulk of the Enhanced Data solution capabilities will be provided by the NPA. There will however be incremental costs to TPSPs and PSPs, such as provision of security tokens and implementation costs to include additional data in payment fields. We estimate this additional capex will be up to £100m. In addition to this £100m, we estimate end-user costs of c. £200m, based on anticipated adoption costs of the solution by end-users (see Appendix 6).

TABLE 4.7 ENHANCED DATA COSTS

Cost type	Capital costs	Run costs (annual)
Central Infrastructure	N/A	N/A
TPSPs / PSPs	£100m	£10m
Total (excluding end-user costs)	**£100m**	**£10m**
End-user costs	£200m	£20m
Total (including end-user costs)	**£300m**	**£30m**

4.4.4 Overlay Service Cost Summary

Table 4.8 provides a high-level summary of estimated capital expenditure and annual run costs for the provision of the three EUN overlay services.

TABLE 4.8 OVERLAY SERVICE COSTS SUMMARY

Cost type	Capital costs	Run costs (annual)
Request to Pay	£100m	£10m
Assurance Data	£200m	£20m
Enhanced Data	£100m	£10m
Total (excluding end-user costs)	**£400m**	**£40m**
End-user costs (All 3 EUN Solutions)	£300m	£30m
Total (including end-user costs)	**£700m**	**£70m**

Question 4.2

Do you agree with the cost assumptions with regards to the NPA and each of the overlay services (Request to Pay, Enhanced Data, and Assurance Data)? If not, please state your reasons and, if possible, please suggest alternatives analysis.

4.5 The Alternative Minimum Upgrade

We believe that to 'do nothing' is not an option. Not least due to the upcoming re-procurement of FPS and Bacs. Therefore, we have used an alternative minimum upgrade approach as a comparison for the NPA. This is consistent with the PSR's Infrastructure Market Review remedy that requires the schemes (Bacs and FPS) to upgrade to be ISO 20022 compliant at re-procurement.

In this alternative minimum upgrade, we assume that the three EUN overlay services are not delivered. We take this view due to technical limitations, for example, the lack of full end-to-end ISO 20022 compliance inhibiting the delivery of Enhanced Data; and ongoing complexity that would be inherent in a minimum upgrade, which would continue the parallel running of three infrastructures.

Alternative minimum upgrade assumptions

- The central infrastructure for FPS and Bacs will be upgraded to ISO 20022.
- The infrastructure outside the centre for both FPS and Bacs will not be upgraded.
- There will be no overlay services in the Alternative Minimum Upgrade, hence no costs or benefits associated with overlay services are accounted for.

4.6 Alternative Minimum Upgrade Benefits

Our analysis estimates that there is a gross benefit of between c. £4 billion – £4.9 billion associated with the Alternative Minimum Upgrade in the period 2019 to 2031. This is equivalent to the current benefits of the Bacs, FPS and ICS services based on our conservative estimate that these benefits are equal to the running costs of these systems. This is consistent with the assumption that there will be no overlay services in the alternative minimum scenario, hence no overlay services benefits.

It should be noted that the qualitative benefits associated with the alternative minimum upgrade are also significantly less than the NPA as a consequence of the continued running of multiple infrastructures and lack of end-to end ISO 20022 adoption, which would inhibit delivery of Enhanced Data and other EUN solutions, and therefore their wider societal benefit. Furthermore, this would impact simplification of access, innovation, competition benefits, and the ease with which future user needs could be met.

Finally, as with the NPA, there are delivery risks associated with upgrading the current infrastructure to ISO 20022, these delivery risks have been assessed across both options. The end-to-end nature of the NPA delivery may incur greater risk. The risks are explored in Section 3.4 of this document.

Question 4.3

Do you agree with our description of the alternative minimum upgrade? If not, please explain your reasoning.

4.7 Alternative Minimum Upgrade Costs

The costs are made up of an upgrade of the current central infrastructure to deliver ISO 20022 capability, and translation services between PSPs / TPSPs and the new central infrastructure. It is estimated that this will be equivalent to the expenditure required for the NPA's central infrastructure of c. £72 million.

Overlay services costs have been excluded from the alternative minimum. This is because this scenario assumes a minimum upgrade and overlay services are not considered to be provided as part of a minimum upgrade.

TABLE 4.9 ALTERNATIVE MINIMUM CAPITAL EXPENDITURE COSTS

Layer	Alternative Minimum Upgrade Costs
TPSPs	N/A
PSPs	N/A
Clearing	£72m
Total	**£72m**

We estimate that the run costs of the alternative minimum upgrade would be £480 million per annum. This is based on the assumption that these run costs would be equal to that of the existing systems. The alternative minimum upgrade run costs are expected to be higher than the NPA as more than one system will need to be run and maintained.

The parallel running costs in the alternative minimum are estimated at an aggregate of £1.7 billion – £2 billion during the transition period. This is lower than the equivalent parallel running costs in the NPA as it is assumed that multiple components will not need to be maintained in parallel in the PSPs and the TPSPs.

4.8 Conclusion

The cost benefit analysis of the two options indicates that an alternative minimum approach of upgrading FPS and Bacs central infrastructure to support ISO 20022 messaging, without delivering EUN solutions, would not deliver the same level of benefit as the NPA – both in quantitative and qualitative terms.

Table 4.10 shows the respective discounted net benefits (gross benefits less costs discounted over 2019-2031) of the NPA and the alternative minimum upgrade options: a positive net benefit of £6 billion to £7.4 billion in the NPA scenario, compared to a negative net benefit of £0.2 billion to £0.3 billion in the Alternative Minimum Upgrade scenario.

The higher net benefit of the NPA compared with the alternative minimum upgrade reflects the benefits of the overlay services, as well as the efficiency savings from the consolidation of the schemes.

Furthermore, the qualitative benefits such as simpler access, increased competition and innovation would also be significantly higher in the NPA compared with the alternative minimum.

*Appendix 6 includes a table with a breakdown of the benefits and costs.

We have also considered risk when conducting the CBA. Both the NPA and the alternative require complex industry change and would need to manage similar risks in respect of the replacement of central infrastructure. The risks are explored in Section 3.4 of this document.

In conclusion, the NPA will deliver significantly greater quantitative benefits compared with the alternative minimum upgrade which would occur absent the NPA, recognising that doing nothing is not an option. Furthermore, there are significant qualitative benefits associated with the NPA that upgrading the existing systems would not deliver.

TABLE 4.10 THE RESPECTIVE NET BENEFITS OF NPA AND ALTERNATIVE MINIMUM UPGRADE

Description	NPA (including EUN)	Alternative Minimum Upgrade
Discounted Benefits	£11.5 billion – £14.0 billion	£4.0 billion – £4.9 billion
Discounted Costs	£5.4 billion – £6.6 billion	£4.3 billion – £5.2 billion
Discounted Net Benefits	£6 billion – £7.4 billion	(£0.2 billion) – (£0.3 billion)[42]

[42] The overall estimated benefits of the alternative minimum approach do not necessarily represent what we believe to be the overall outcome that may be delivered as a consequence of the IMR remedies as a whole. Furthermore, our analysis does not suggest that doing nothing would be preferable to this alternative minimum upgrade.

5.0 NPA Commercial Approach and Economic Models

This section focuses on the commercial and economic models of the NPA. We present a series of frameworks to help the NPSO assess funding options, present our assessment criteria, and identify pre-requisites for the adoption of new solutions. Finally we outline funding options for the NPA.

This section will be of most interest to vendors looking to engage in the markets that result from NPA changes and investors looking to invest in new initiatives in the payments industry. As such they may be interested in the implications of providing NPA elements as outlined in Sections 5.2.1 and 5.3.1.

For other stakeholders, this section shows how the NPSO could fund the development of core NPA components.

5.1 Introduction

5.1.1 Objectives and Scope

The Forum has set out to answer questions about how the New Payments Architecture and end-user solutions should be funded, particularly the investment stage required to design and deliver the NPA to market. We answer the following questions in this section:

- How can we ensure funding approaches facilitate appropriate competition?
- How might NPA elements be funded and what would the incentives be for various investors?
- What impact do the different funding approaches have on the stated assessment criteria?
- What is the NPSO's role in the payments lifecycle?

Any potential funding arrangements must align to the Forum's overall objectives. These are the key criteria we have identified against which funding options should be assessed: systemic risk, competition, accessibility, efficiency, financial risk, and intellectual property.

In this section of the consultation, we analyse the approach to competition, stakeholder incentives and funding arrangements, as well as the impact these will have against our assessment criteria. The NPSO will decide upon the funding model and our findings should inform their decision.

5.1.2 Assessment Approach

A three-step approach has been taken to consider potential funding options.

Firstly, we analyse the current state of the UK market and the commercial relationships underpinning PSOs. This includes a consideration of their procurement processes, governance arrangements and the flow of finances between payments participants. Furthermore, we provide a perspective on how other countries approach some of the challenges identified in payments infrastructure procurement. The detail of our findings can be found in Appendix 8.7.

Secondly, in section 5.2 we explain the frameworks we use to assess different approaches to funding. We also explain the assessment criteria and discuss the types of competition categories that exist and how these map to elements of the NPA. We then consider the different roles the NPSO, third parties and vendors play across the lifecycle of funding. The prerequisites for successful funding forms our last consideration, where we draw upon findings from past product roll outs.

In the last section (Section 5.3) we apply these frameworks to NPA elements. This provides the basis for an analysis of the most viable funding options for those elements, and an outline of the 'deal levers' which can be used by the NPSO to enable the investment.

5.2 NPA Theories and Assessment Principles

We have developed a series of frameworks to help the NPSO with funding approaches investor selection, considering the nature of competition in payment systems. The NPSO will have a different role across the value chain depending on the nature of competition of the service provided.

Pre-requisites for the adoption of new payment services which improves the chances of a successful product roll out have been identified as well.

An overview of the assessment criteria which is based on the PSR's, Forum's and NPSO's objectives is presented to enable a more competitive, accessible, efficient and resilient UK payments industry.

5.2.1 Competition Categories

The nature of competition on the supply side of the UK's payments services reflects the characteristics and dynamics of our market. Competitive behaviour ranges across a spectrum depicted in Figure 5.1 which shows four competition categories of funding approaches.

At one end of the spectrum, there can be many firms 'in the market' supplying similar services. Towards the other end of the spectrum however, the scale and nature of more systemically critical services drives a concentration of suppliers, particularly in the Clearing and Settlement layers.

Typically, these are provided by a small number of suppliers with a few providing services concurrently, or at its extreme a single provider 'for the market' who may face competition over time on renewal of their contract with the purchaser. In the NPA, one of the roles of the NPSO is to procure such systemic services. It may also stimulate the market towards commercial self-sufficiency by having a 'market catalyst' effect on some payment services as outlined later in this section.

'Unaccredited' Competition

'Unaccredited' means that elements or activities in this category are not required to be accredited by the NPSO. They may be required to meet general regulatory expectations or standards set by other bodies however. In theory, this category holds the most scope for competition and innovation within the NPA and its ecosystem.

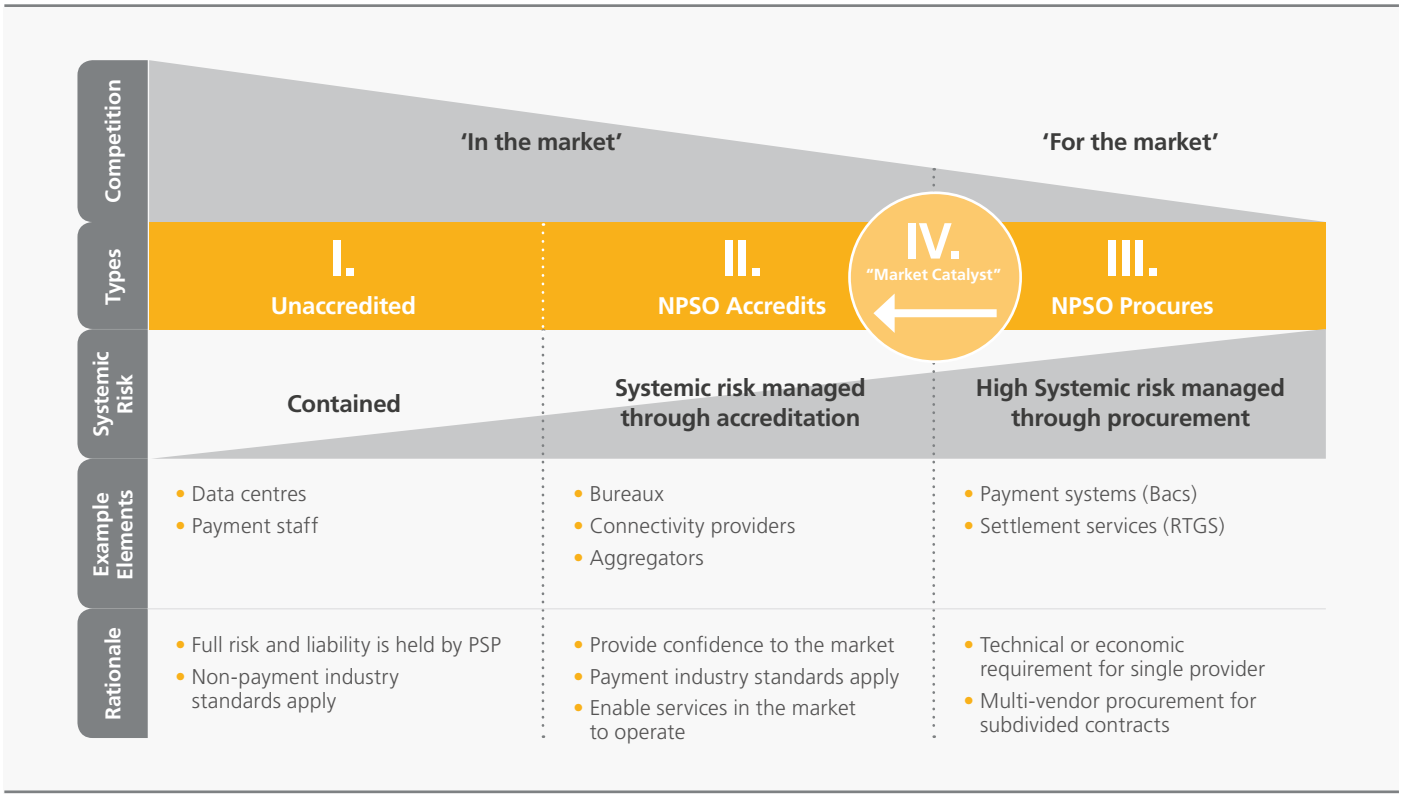
Examples of potential elements include data centres and staff members. The risk for these 'elements' is carried by the providers and PSP customers themselves.

'NPSO accredited' Competition

The Forum is committed to ensuring that competition and innovation is embedded within the overall make-up of the NPA. This consideration must however, be tempered by a fundamental commitment to system stability and resilience. Where there is a perceived risk to stability, security, a critical interoperability requirement, or need for ubiquity, the NPSO must set rules and standards which might have the effect of narrowing the potential source of supply.

The NPSO mitigates risk by technically accrediting providers and overseeing their application of the rules. Accreditation brings consistency of payments industry standards, protects the functioning of payment services and ensures confidence in the market. In this category there will be multiple providers competing to deliver solutions but to do so they must be accredited by the NPSO. Some examples of elements of the payments ecosystem which fall within this category are bureaux, connectivity providers and aggregators.

FIGURE 5.1 NPA COMPETITION CATEGORISATION



'NPSO procured' Competition

Elements posing high systemic risk that are fundamental to the overall payments landscape where there are technical or economic challenges with multiple, concurrent solutions, will fall within this competitive category. It is likely that elements within this category will be best served by a single provider. There may be instances however, where elements could be subdivided and provided by multiple vendors.

Current examples of services within this category include PSOs, as well as clearing and settlement services that enable connectivity with the Bank of England's RTGS service. Since these elements pose high systemic risk, their resilience and stability is paramount. In many cases this is likely to provide rationale for a fixed term, single provider. Substitutability however, is a key part of resilience and may give rise to the NPSO procuring multiple vendors delivering replicas of an element and competing for business.

The layered model of the NPA allows for the possibility of procuring parts of the system as individual elements rather than as single layers. This presents new potential opportunities to improve competition.

In the case of 'NPSO procured' elements operating on fixed term contracts however, competition risk may yet exist. There is a greater propensity for vendor lock-in and barriers to entry due to the standards applied to ensure resilience for systemically important elements. To mitigate this, a wide pool of vendors should be consulted during the initial phase and common standards should be set to enable vendors to compete at re-procurement. One example of a common international standard that will lead to a larger pool of interested bidders is the ISO 20022 standard.

'Market catalyst'

Where there is general recognition that addressing a detriment may bring benefits to the market, it may be appropriate for the NPSO to act as a 'market catalyst'. The NPSO's role will enable the interoperability and market contestability which drive competition and innovation.

'Market catalyst' models will be needed when supply-side players do not immediately see the commercial opportunities of participating in a new payments market. Vendors may be unwilling to enter the market since potential market adoption is unknown. Potential market entrants may be deterred by the risk of developing new solutions outweighing the benefits of exploring the potential of the market.

To prove a specific market solution, the NPSO could undertake a number of optional steps depending on the requirements. Initially, the NPSO could define the principles of the market solution by **setting standards**, rules and guidelines for the new service. Consumer protection frameworks and liability models are prime examples of where the NPSO could play a valuable role relieving the burden on market participants by determining market characteristics.

The NPSO can **stimulate the market** further through a range of direct and indirect activities. For instance, the NPSO could stimulate market participation indirectly by commissioning industry research and thought leadership.

A key example of this is the work FPS did with challenger banks to spur providers into developing the 'technical aggregators' new access model. The use of a sandbox environment can also lead to stimulation of the market. This would be an interesting proposition mostly for smaller FinTechs and vendors. We would expect the NPSO to fund this from its Research and Innovation (R&I) budget or if more substantial, by way of interested market participants or venture capital.

In all these cases, accreditation and proof of market would provide the foundations for increased interest from financial investors, as well as support for new services.

We elaborate further on the 'market catalyst' risks and mitigations in the Commercial Approach and Economic Models (C&E) supporting paper.[43]

FIGURE 5.2 "MARKET CATALYST" MODEL

Model types		Description
'Market Catalyst'		• Driven by end-user needs which are served by a specific service offering • Market participants currently do not envisage a positive business case therefore the NPSO will provide a proof of market
A	Setting standards	• NPSO defines rules and guidelines on how the new service should be operated • NPSO defines the consumer protection framework and liability models
B	Stimulate the market	• NPSO will commission research, thought leadership work or provide the industry with an environment within which to drive innovation (e.g. sandbox)

Question 5.1

Does our competition framework adequately capture the types of competition that may exist in payments?

Question 5.2

Do you agree with the NPA competition categories described? If not, please explain why.

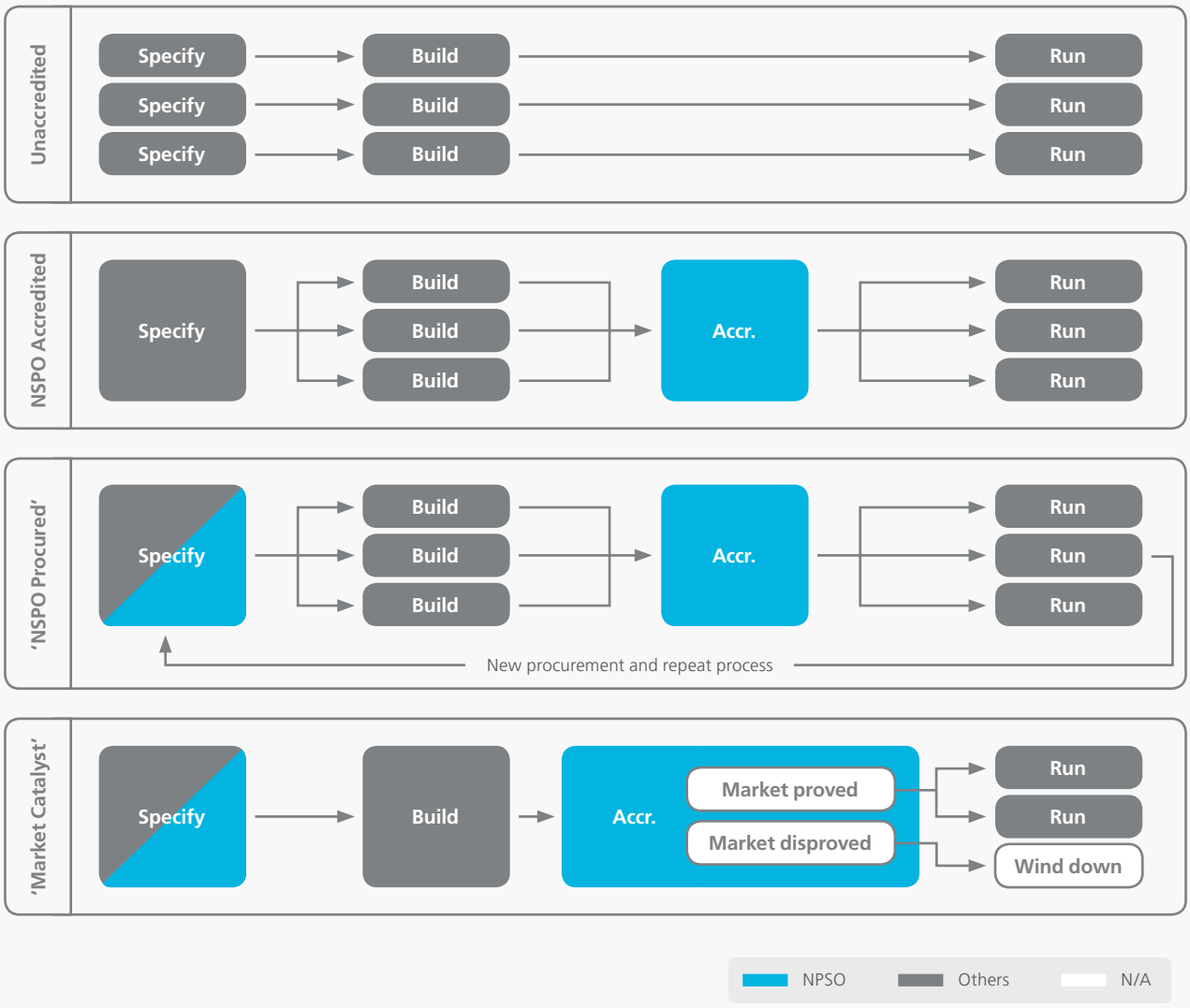
[43] https://implementation.paymentsforum.uk/consultation

5.2.2 NPSO and Third Party Roles in the Payments Lifecycle

In our discussions, we identified new and / or different roles for the NPSO and third parties across the four-stage payments lifecycle (specify, build, accredit, and run) in the NPA.

In all of the different lifecycles where it does have a role, the NPSO is always the accrediting body. As such, it is the enabling 'gateway' for any new payments products that require accreditation or procurement, no matter who requests the change. Furthermore, the NPSO never 'builds' a product but rather must procure or facilitate the procurement of a service. The roles are illustrated in Figure 5.3 per lifecycle stage and NPA competition category type.

FIGURE 5.3 PAYMENTS LIFECYCLE



Funding

In its report on the funding of the NPSO, the PSO Delivery Group identified different types of funding requirements. These included: initial set up of the NPSO, business as usual operating costs, research and innovation costs, reserve capital and development/ extraordinary funding.

Our analysis draws on the PSO DG's work and forms the basis of the funding rationale we use later.

During the **specify** stage, the NPSO's role is to design the rules and standards (except for elements within unaccredited competition to be served by the market alone). The NPSO will collaborate with vendors and others on how the solution should be built, aligning on technical specifications and regulatory requirements.

In the next stage, **build** costs represent the costs associated with developing a solution.

At the **accreditation** stage, vendors will pay for accreditation by the NPSO, granting them the opportunity to provide payment services.

Finally, within the **run** stage, operational costs are covered by the pricing mechanism chosen by the NPSO, including costs associated with operational enhancement and upgrades, capital recovery and sinking fund expenses.

Question 5.3

Does our framework capture the dynamic roles the NPSO may play in the market?

5.2.3 Pre-requisites for successful funding

This section provides a framework for pre-requisites to be considered for a successful roll out of payments solutions to the market.

The single-channel considerations, are geared towards solutions that rely solely on PSPs for market, consumer and end-user adoption (e.g. Paym). There are a number of enablers for each identified stage of the process which facilitate successful funding.

In comparison, the dual-channel model applies to solutions that are dependent on market participants (e.g. vendors, retailers) as well as PSPs' adoption and promotion (e.g. contactless payments). As such more enablers are required to successfully establish a product on the market. Further details on both models can be viewed in the C&E supporting document.[44]

After examining the cases of Paym, contactless payments and CASS, we found common themes which would contribute to the successful roll-out of market catalyst payment solutions:

1. **Promotion and adoption of the new service roll-out needs to be done synchronously by all payment market participants.** The proposition for all parties needs to be compelling, which may require stimulating investment by those working on each side of the market.
2. **Commitment and collaboration between industry participants is vital** to deliver the network effect needed for major industry change. Co-ordination is required when a new product is brought to market to ensure take up is as quick and efficient as possible.
3. **Recourse to further action is needed if there is limited adoption and promotion.** If uptake is lacking, where a solution is viable there should be alternative action such as adjusted pricing mechanisms or regulatory intervention.

We recommend the NPSO to carefully consider these pre-requisites when solutions are deployed.

[44] https://implementation.paymentsforum.uk/consultation

5.2.4 Assessment Criteria

The NPSO will determine the appropriate type of funding for different elements of the NPA. We outline some assessment criteria, which the NPSO could use to determine this.

TABLE 5.1 ASSESSMENT CRITERIA

Assessment Criteria	Definition
Systemic Risk	• Risk of failure of vendor solution and the impact it has on continued provision of payment services within the ecosystem. • State of the security and stability of the operations to provide a stable service.
Competition	• Number of competitors interested in the market and wanting to compete on price and quality. • Level of innovation that is driven by vendors to differentiate themselves. • Barriers to entry for other vendors.
Accessibility	• Level of accessibility for PSPs (large or small).
Efficiency	• Efficient delivery of the system and innovation to the end-users. • Corporate governance structures in place. • Reduced overheads and efficient operational structure. • Pricing impact for the end-user.
Financial Risk	• Financial risk (investment at risk) carried by the investor. • Size of investment required to Design, Build and Operate service. • Risk profile of the investment.
Intellectual Property	• Opportunity and restrictions in the usage of IP to develop other products or use the IP in other countries / sectors.

Systemic Risk

Systemic risk is the possibility of failure of one or more elements and the impact this may have on the environment as a whole. A key consideration for the NPSO is the extent to which an element may present risk to the system, how it is managed and the propensity of potential investors to cover the associated cost of managing it.

Competition

Increasing competition in both the infrastructure market and the PSP market are key objectives of the NPA. The NPSO must take into account the number of competitors in the market, as well as their interest in competing on price and quality. Barriers to enter a market should be considered in order to assess the complexity of competing in a new market for smaller players.

Access

Simplifying and increasing access to smaller PSPs and FinTechs is another key objective of the NPA. In light of this, the NPSO must consider the views of all relevant stakeholders and the motivations of potential investors.

Efficiency

Resilience of service is paramount, and it must be balanced by the efficiency of service provided. The NPSO must consider vendor pricing in relation to the stringency of Service Legal Agreements (SLAs) that the vendor commits to whilst appropriate corporate governance structures ensure effective service provision.

Financial Risk

The NPSO must consider the level of capital of various funding stakeholders. This entails a view of the size and risk profile of the investment.

Ownership of Intellectual Property

Intellectual property (IP) ownership represents our final assessment criterion because of its value. Historically infrastructure providers have been able to utilise their UK IP in other geographies.

Question 5.4

Are there any other important criteria that we should use to assess the funding options we have identified?

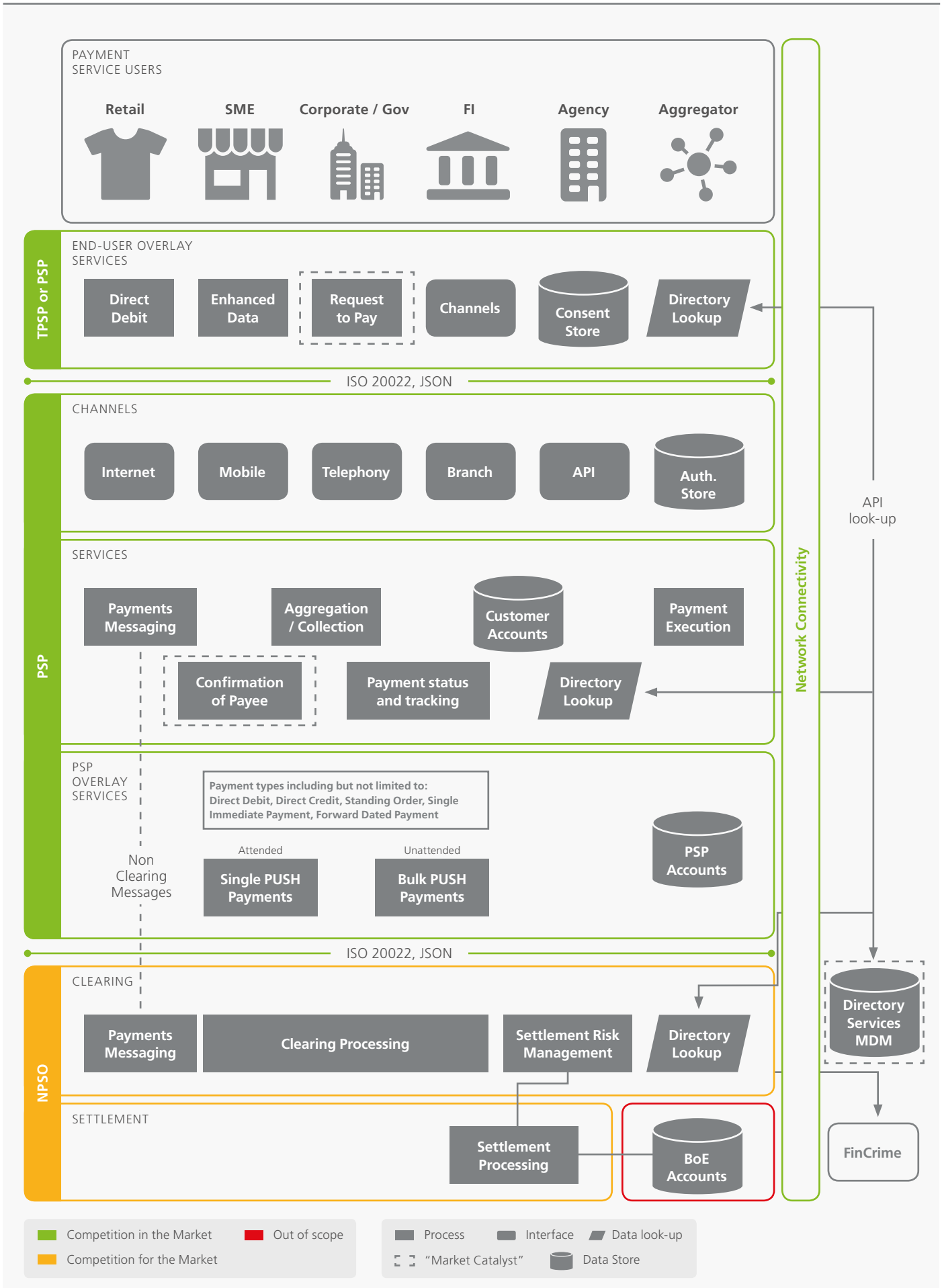
5.3 Commercial, Funding and Competition Assessment

This section seeks to provide a view on viable funding options by applying the assessment criteria and the NPA's competition framework.

5.3.1 Elements of the NPA

We have applied the NPA competition framework to the NPA architecture. 'NPSO procured' solutions sit at the bottom of Figure 5.4, followed by competition in the market. Key elements that may be categorised as 'market catalyst' at this stage are circled.

FIGURE 5.4 NPA COMPETITION CATEGORIES



5.3.2 Assessment of the NPA's Competition Categories

This section applies the assessment criteria we outlined in 5.2.4 to two types of competition categories we outlined in 5.2.1, 'NPSO procures' and 'market catalyst', in order to identify appropriate funding models. In addition we identified a number of risks and their 'deal levers'.

'NPSO procured' Considerations

We understand NPA elements falling within this category pose high **systemic risk.** Splitting the clearing and settlement contract into multi-vendor deployment could help mitigate the spread of systemic risk.

Since the resilience and stability of these elements is critical, the NPSO is limited in the levers it can use to alter the level of **competition** of this market category. Barriers to entry are high since the solutions may only be provisioned by a single vendor for some elements. Splitting clearing into individual elements or running procurement with multiple vendors, may have an impact on competition.

The NPSO must take **accessibility** for smaller PSPs and FinTechs into account. This entails ensuring that the cost of access is kept to an acceptable price range, without necessarily relying on aggregators or direct access PSPs. Pricing model innovation represents a potential 'deal lever', whereby tiered pricing could provide greater inclusivity for PSPs and FinTechs. The NPSO should be flexible in its approach to pricing, maximising market adoption while limiting detrimental forms of cross subsidisation.

We foresee that the procurement of new solution providers on a fixed contract basis may have a negative short-term impact on operational **efficiency** where the infrastructure provider has changed and PSPs are required to implement system changes. The NPSO can consider setting up penalty systems with SLAs to control operational efficiencies of the service. If this is done, the NPSO must ensure it has the monitoring capabilities to enforce the Service Level Agreements (SLAs).

We anticipate the **financial risk** for procured vendors to be low due to volume commitments from PSPs and the fact that these services are crucial to the functioning of the payments industry. Given that market solutions are likely to be large in scale, a limited number of vendors will possess the capital and capabilities to deliver these services. As such, the NPSO should consider allowing vendors to bid in consortia or work with financial investors to lower the risk of entering the market.

Vendors may have the potential to re-use **intellectual property** (IP) and sell services in other countries, especially if the IP developed is built on international standards. The NPSO could have a role in the control of future IP usage in the set-up of licensing agreements, whilst the inability to re-use IP may impact vendors' interest in participating in the bidding process.

'Market catalyst' Considerations

NPA elements falling within the 'market catalyst' model pose a medium to low **systemic risk** since the provision of these solutions is not viewed as critical to the functioning of the payments ecosystem. While elements within this category will be served competitively once the market has been proven, there is still some risk that established solutions might end up as 'for the market' solutions. As such, the NPSO could test solutions in its sandbox first on a small scale to enable multiple vendors to engage.

The 'market catalyst' model provides a key mechanism for the NPSO to increase **competition** within the market. Competition can be facilitated through consulting with multiple and diverse vendors to ensure the rules do not inadvertently favour one vendor. Commissioning industry research or the creation of sandbox environments should positively impact competition and innovation.

A large number of market participants should be consulted during the launching of new services or solutions to ensure **accessibility** for smaller PSPs is maintained. This ensures standards are achievable by a range of PSPs. And as noted above accessibility can be improved through thought leadership addressing key issues or testing new approaches in the sandbox.

The 'market catalyst' model is not driven by standard demand, supply and competition rules and might fall behind the market in terms of **efficiency.** Development of solutions and bringing them to the market are dependent on collaboration between vendors and the NPSO's funding reserves. Learnings from previous roll-outs detailed in the Section 5.2.3 will help mitigate this risk.

In comparison to 'NPSO procured' solutions, there is increased **financial risk** within the 'market catalyst' category due to the uncertainty of the market demand. Financial risk can be limited with a phased approach to investing to prove market demand with minimum required investment.

There is increased scope for the NPSO to retain **intellectual property** (IP), which may be beneficial in promoting competition, for 'market catalyst' solutions. The NPSO then has the option to set-up legal structures to retain IP and recover its initial investment if the market has been proven.

Question 5.5

Do you agree with our NPA competition assessment? If not, please explain why.

5.3.3 Commercial Considerations for End-User Solutions

To provide a view on the competitiveness and commercial approach to the proposed end-user solutions presented in this paper we have focused our attention on two solutions: Request to Pay and Assurance data – Confirmation of Payee (CoP). Remaining subcomponents of Assurance Data and Enhanced data are not discrete architectural elements and thus are not suited to this analysis. The real-time balance component lies entirely in the competitive domain of the PSPs and vendors.

Request to Pay

Several solutions already exist in the market that offer Request to Pay functionality (e.g. pay.me from Monzo and Receive on Pingit). These solutions however, lack interoperability, are non-standard, and cannot be used on all schemes. This has been one of the hindrances to Request to Pay being adopted and attaining ubiquity. The Forum is seeking to address the detriments identified and drive ubiquity by setting out a minimum standard that allows competitive market solutions that are interoperable, ubiquitous and easily recognised by end-users.

Initially we expect the NPSO to be involved in publishing the minimum standards for Request to Pay as well as proving demand in the market for this solution. This strongly aligns to our 'market catalyst' category. Once demand is established, it is assumed it will move into 'NPSO accredited' competition.

To ensure successful funding and product roll-out, we foresee three main parties being involved – the payee (corporate, utility company or individual), payer and a Request to Pay service provider (vendor, PSP or TPSP). The NPSO can draw upon the findings in the single-channel framework presented in the C&E supporting paper[45] in order to best catalyse Request to Pay.

To support Request to Pay the Forum has conducted numerous interviews with corporates, the outcome of which suggests that there could be demand among them to develop such a product and offer it to their customers. The design of Request to Pay has also been developed through working groups to ensure that potential problems that arise from, for instance, 'late payment' or 'non-payment' have been addressed within the current proposition.

Confirmation of Payee

Confirmation of Payee (CoP) can be classified as a 'market catalyst' solution with the intent to move to 'in the market'. It is crucial that the CoP solutions, which can be developed internally or offered by vendors, are interoperable between PSPs and comply with the same standards.

CoP creates positive benefits for end-users and market participants. The solution is largely dependent on universal acceptance among the PSPs and thus the NPSO should learn from the findings in the single-channel framework in the C&E supporting paper[46] (e.g. collaborative approach). Furthermore, market participants will be able to build on CoP to both innovate and address a major detriment identified in the current systems, including the fraud identified by Which?'s super-complaint.

Others

Both Payment status tracking and Enhanced data are capabilities which will be developed as inherent functions of the NPA on the underlying infrastructure. The delivery of actual services and innovation on top of this architecture will be dependent upon the PSPs.

Question 5.6

Do you agree with our assessment of the End-User Needs Solutions? If not, please explain why.

5.3.4 Funding Stakeholders

The NPSO has access to a diverse range of investors. We have identified four major stakeholder categories which are most likely to be interested in financing solutions within the NPA based on evidence in the payment industries in the UK and abroad:

- Vendors
- Financial investors
- Retail investors
- Other market participants

Question 5.7

Do you agree with our list of funding stakeholders? If not, please explain why.

The NPSO itself may also choose to fund initiatives. Further detail can be found in the Appendix.

[45] https://implementation.paymentsforum.uk/consultation
[46] https://implementation.paymentsforum.uk/consultation

5.3.5 Financial Instruments Viable for Funding the NPA

The NPSO has a number of financial instrument options available depending on the stage of solution maturity. There are three main ways to fund any NPSO efforts: self-fund with existing resources, raise external debt or equity investment from public or private markets.

To raise equity, we envisage that the NPSO would create a subsidiary that would sell equity to a financial or strategic investor, such as an investment fund. Equity raising is beneficial since it can be used across all lifecycle stages of a business even when there may not yet be positive cash flows. The NPSO should however, consider the overall cost of this financial instrument, as well as the level of control of equity stakeholders. Lining up financial investors across early (Venture Capital) as well as late (Private Equity or Pension funds) stages upfront can help limit the risk of delivery. This is aligned to the findings of the PSO DG report which described the sources of funding for the NPSO in further detail.

Debt can be raised from a bank (senior debt) or debt fund (unitranche or high yield bonds). This instrument would bear the advantage of limiting the influence of funding providers on the governance and operation of the service. Debt financing may not be appropriate for certain parts of the payments lifecycle but for more established products with a clear cash generative profile. Unitranche and high yield bonds providers may be more suitable than bank's senior debt to support the investment into future growth.
The NPSO should also consider the effect of debt financing and interest repayments on cash flows, anticipating any constraints.

Question 5.8

Are there other significant sources of funding or types of funding instruments the NSPO could secure that have not been described? If not, please explain why.

5.3.6 'Deal Levers'

The following section provides 'deal levers' against our assessment criteria, building upon the analysis of various investor types and financial instruments.

Each 'deal lever' gives a way of reducing potential risks relating to each of the criteria but may have an impact on other areas of the assessment criteria. For instance, it may be possible to use a deal lever to reduce systemic risk but in doing so decrease competition.

In order to mitigate the risks associated with **systemic risk,** the NPSO should ensure investors and service providers are credible and capable to deliver. The NPSO should only offer contractual arrangements which ensure vendors fulfil the NPSO's design and facilitate increased competition in the overlay market. Contractual arrangements should bear this in mind, and should ensure that financial investors are limited in their ability to create barriers to competition and innovation. Therefore the NPSO should have internal resources able to handle the evaluation of investors and vendors.

Vendors may have a **competitive** advantage in providing overlay services on the back of their 'for the market' contract. Constructing 'Chinese walls' between infrastructure and overlay services could be an option for the NPSO to mitigate this. Alternatively, the NPSO could consider prohibiting vendors from entering the overlay market for a short period to allow other providers to establish themselves.

The NPSO should ensure that vendor solutions will not limit **access** of other market participants, smaller PSPs and FinTechs. Increased consultation with smaller PSPs and FinTechs will be necessary to ensure any standards for access are suited to their needs.

To ensure **efficient** service delivery, the NPSO should consider governance structures which enable oversight of the service. This will require negotiations with investors and the NPSO will need additional internal resources to handle the workload. Alternatively, the NPSO can consider Joint-Venture (JV) structures where the vendor (service operator) is not restricted in its operations by the financial investor's interest in increasing investment returns. Financial risk per party can be split if investors bid in consortia or in hybrid models (e.g. cooperation with strategic or financial investors).

Lastly, the NPSO should consider licensing agreements that will ensure control over **intellectual property** and provide better control over the managed service. Strong restrictions on the usage of IP however might limit vendors' interest in providing a service and thus a balance between stakeholder interests has to be found. The NPSO should consider appropriate mechanisms to obtain the right skill set to monetise its value in other geographies or markets (if possible).

The NPSO can also consider bridging any knowledge gaps by contracting with vendors and external advisors, which brings with it a financial impact and dependencies. There may be instances where alternative hybrid models, such as joint ventures, may be the most appropriate option. This is most likely to occur if there is a requirement to diversify the risk of delivery amongst investors with different competencies.

In all cases, exit requirements for financial investors will need to be taken in to account.

TABLE 5.2 ILLUSTRATIVE 'DEAL LEVERS'

Assessment criteria	Indicative Deal levers
Systemic Risk	• Set-up contractual SLAs with penalty-pricing to ensure strong service delivery. • Split procurement contracts into smaller elements.
Competition	• Set-up 'Chinese walls' between infrastructure and overlay services provided by the same party. • Temporarily prohibit access to overlay services market for infrastructure providers. • Incorporate innovation as an evaluation factor for procurement of services.
Accessibility	• Set-up consultation channels with wider payments community to ensure open access. • Set standards, that investors will comply with, which will consider access to the market for all PSPs (small or big).
Efficiency	• Explore Joint Venture (JV) structures for procured services to grant efficient service delivery. • Set-up standards that will enable efficient service delivery by wider group of vendors. • Use governance structures that enable NPSO services oversight.
Financial Risk	• Volume guarantees set by users (PSPs) to limit investment risk. • Allow investors to form consortia or bid with financial or strategic investors backing. • Limit risk of future solution by building standards, customer research and vanilla products.
Intellectual Property	• Utilise licensing agreements to protect the NPSO IP ownership.

5.4 Conclusion

A spectrum of funding options that the NPSO can consider has been identified. The NPA represents an opportunity, not only for vendors, FinTechs and small PSPs, but also for financiers that can enter this dynamic market.

We believe there are four NPA competition categories that cover NPA components, two of which will be funded competitively by the market. For the other two, the 'NPSO procured' and 'market catalyst', the NPSO should explore alternative funding options.

End-user solutions presented in this paper have been designed to foster competition and deliver benefits to the wider payments ecosystem. It is assumed that both Confirmation of Payee and Request to Pay will move from 'market catalyst' to 'in the market' solutions once the market has been established.

We have identified four types of potential investor (financial investors, retail investors, vendors and market participants) in addition to the NPSO. The extent to which NPA elements will be of interest to potential investors depends on the amount of risk, investment size and investor capabilities.

The NPSO has a wide selection of funding options to choose from for the delivery of the NPA and the funding does not need to be rigid or overly concentrated.

5.5 Next Steps

The Forum will consider the responses to this consultation and amend its commercial approach accordingly before preparing its final paper to hand over to the New Payment System Operator at the end of 2017.

6.0 Improving Trust in Payments

6.1 About this section

Our Strategy proposed a set of seven solutions to engender user trust in safe and certain payments through collaboratively preventing financial crime. We committed to consult on two solutions, namely 'Payments Transaction Data Sharing and Data Analytics' and 'Trusted KYC Data Sharing' respectively. Appendix 8 provides an update on the other five solutions that we have progressed, including updates on handover by the Forum to other industry bodies who will carry implementation forwards.

We expect that these sections will be of particular interest to those with a role in the prevention of financial crime, including Payment Service Providers, trade bodies, solution vendors, regulators, law enforcement agencies and the government.

6.2 Payments Transaction Data Sharing and Data Analytics

6.2.1 Overview

Payments in the UK can be made using multiple payments mechanisms (e.g. Bacs, CHAPS and Faster Payments). These payments systems can be used by criminals to launder stolen or misappropriated money, masking the trail of funds and making its origin unclear. This laundered money can be used to fund terrorism or organised crime, or allow criminals to profit from fraud.

In our Strategy, we proposed a Payments Transaction Data Sharing and Data Analytics solution to help fight financial crime that occurs through the misuse of payments systems. The solution will enable visibility across different transactional data sources to create a rich data repository and analytical capability.

The objective of the solution is to detect and prevent current and future financial crime by creating an industry-wide capability to analyse end-to-end payment transaction data from all retail interbank payment mechanisms in conjunction with other relevant sources of diagnostic information. Examples of financial crime being targeted include: the identification of money mule accounts and the ability to return stolen money.

We progressed the solution in two ways: a tactical solution[47] and a strategic solution.

The tactical solution was handed over in early July to FPSL as a delivery body for implementation; this solution will transition into the NPSO later this year. The tactical solution will provide early benefit to aid the detection of money mule accounts, and pilot methods for funds repatriation. The tactical solution will run as an interim service, until the strategic solution is implemented.

This section of the consultation focuses on the strategic solution.

6.2.2 Solution Capabilities and Requirements

The strategic solution will consist of three core capabilities:

- Ability to acquire payments transactions and other contextual data from a wide range of sources.
- Ability to store several years' worth of this data in an accessible form.
- Ability to deliver advanced data analytics on the payments transactions and other data that is acquired.

The solution must meet these key requirements:

- Provide timely access to both detective and preventative analytical tools and information that enable measures to be taken by Payment Service Providers (PSPs), public bodies (i.e. central and local government), and law enforcement agencies to address identified incidents or trends.
- Be adaptable to new types of payment mechanisms.
- Be adaptable to new financial crime threats.
- Include all Account Servicing PSPs and all payment types to ensure sufficient coverage is available to enable full payment journeys analysis.
- Support a competitive market for the supply of tools, analytical insight and other relevant services for each of the core components.
- Have appropriate linkage to the New Payments Architecture (NPA) for the acquisition of payments transaction data.
- Provide significant additional detective and preventative capability compared to the tactical solution and be scalable in terms of volumes, types of transactions and financial crime threats.

What is a money mule account?

A money mule is a person who transfers money acquired illegally to either other transit accounts or the scam operator.

The use of multiple money mule accounts is designed to hide the true source and or purpose from PSPs and authorities, before they are ultimately transferred into goods or un-traceable funds.

A money mule account is either obtained using false identification, or control of a legitimate account is achieved by fraudsters with consent or through payment processing scams or hacking.

[47] For more information on the scope and handover of the tactical solution, please see the Payments Transaction Data Sharing and Data Analytics – Tactical Solution paper here: https://implementation.paymentsforum.uk/consultation

6.2.3 Solution Scope

The solution will cover all transactions made by any payment mechanism, to or from every customer account domiciled in the UK, covering a minimum time period of five years. The stored data must be available both to a central set of analytical tools and also to participants so they can access and carry out their own analysis.

The solution must be capable of processing all of the information held to either identify threats and trends, or to specifically look for transactions associated with a particular type or instance of financial crime. The analytical tools should:

- Be able to run at all times and provide results immediately on demand.
- Be capable of handling a wide range of criminal activity, ranging from third party payment fraud, beneficiary fraud and application fraud through to benefits fraud or terrorist financing.
- Be capable of predicting criminal activity based on patterns of behaviour, enable risk-based scenario modelling, as well as identifying impacted customers (such as fraud or scam victims).
- Have the capability to identify new typologies of criminal behaviour, and facilitate appropriate responses.
- Provide and support mechanisms to allow continuous feedback to participant organisations to help better understand financial crime activity, and so inform development of participants' internal policies and processes to counter financial crime.

Participants in the strategic solution are likely to include information providers (e.g. PSPs and payment schemes), information users (e.g. PSPs, Government, Law Enforcement and investigators) and service / solution providers (e.g. data storage and analytics). There should be no restrictions on participants within these categories, other than to safeguard against illegal or inappropriate use or ensure the safety and security of the data. Other valid participant groups may emerge over time. Therefore, the solution should not be limited to the original categories of participants.

Question 6.1

Do you agree with the outlined participant categories identified for the Payments Transaction Data Sharing and Data Analytics strategic solution? Are there other categories that should be considered for inclusion? Please explain your response.

Question 6.2

What is your opinion on the role non-payments industry participants should have as part of the Payments Transaction Data Sharing and Data Analytics strategic solution? (This could include Government, Law Enforcement, or others). If appropriate, please outline your views on the usage of the system, provision of data to the system, and legal considerations for participation.

6.2.4 Minimum Scope Requirements

The intention is for the strategic solution to be available within 2 to 3 years. Therefore, based on current payment mechanisms and storage / analytical technology, a realistic minimum scope for initial implementation of the strategic solution would include:

- Payments above a minimum value threshold based on transaction type, with the ability to reduce or remove this threshold over time.
- Payments made using the core UK domestic electronic schemes, card payments, international payments, internal bank payments and transactions (including future derivations of these payment types).
- At a minimum, payments made to or from personal current accounts and business current accounts, with an ability to add additional account types as required.
- Diagnostic and contextual information (e.g. known fraud or Suspicious Activity Report related information) based on availability and relevance.
- Data updated daily (holding information for the previous six months only).

Where data that exceeds these requirements is available, this should be included if practical. It is expected that the solution capability will expand beyond this minimum scope over time.

Whilst the objective is to cover as many payments systems as possible, it is recognised that some sources of data may not form part of the initial solution based on the complexity and costs of inclusion. Any transactional source that is not part of the initial solution runs the danger of financial crime migration (i.e. criminals may start to use those payment mechanisms to move money). These transaction sources may be subsequently used to hide the trail of funds, or allow laundered money to enter the UK payments market. As such, these must be fully risk assessed.

6.2.5 Links to other systems and financial crime initiatives

The development of the solution will consider the necessary interactions and links with other systems, transactional data sources and financial crime initiatives.

In particular, the appropriate linkage between the solution and the implementation of the NPA will be considered, and appropriate design decisions made to reflect this.

The solution may, over time, also link to other Forum financial crime initiatives and solutions, including Trusted KYC Data Sharing, Guidelines for Identity Verification, Authentication and Risk Assessment, and Financial Crime Data and Information Sharing.

Combining information from these different sources has the potential to provide huge benefits for the detection and prevention of financial crime, as well as improving process efficiencies for PSPs and consumers.

Whilst the links between solutions and existing systems should be carefully considered, the implementation of the solution should not be reliant on the implementation of other payments industry initiatives.

6.2.6 System Use Cases

The solution will support both on-demand interaction, where participants can get feedback from the system in near real-time, as well as longer running processes to develop deep analytical insight over large volumes of data.

On-demand interactions would involve participating organisations exchanging information with the solution in near real-time. This could involve matching account information against known watchlists prior to authorising a transaction, or more general transaction risk scoring.

Longer running batch processes will run over large sets of data with the ability to use advanced analytical techniques (machine learning, artificial intelligence etc.), to support intelligence building. Potential benefits include recognition of new financial crime trends by observing unusual patterns of behaviour, or the identification of potential fraud and scam victims where the pattern of financial crime behaviour is known.

The strategic solution will be able to combat a range of financial crime methods over and above the tactical solution (money mule account identification and funds repatriation), potentially spanning both private and public sector uses.

Some example use cases are outlined below. Whilst some solutions exist on the market that attempt to address these use cases, this collaborative solution would be uniquely placed to provide a comprehensive industry wide analysis with a full range of payments data. This would greatly enhance the value of such solutions, providing benefit for consumers, businesses and financial institutions as financial crime is detected and prevented with greater accuracy, efficiency, and speed.

Transaction Verification Services

Verification of payee identity and identification of abnormal account activity are just two examples of a large number of transaction verification problems faced by the payments community. The solution could be used to address these problems at an industry scale, and is closely aligned to the 'Assurance Data' NPA solution that tackles 'Confirmation of Payee' (Section 2.3.2). For example, analysis of the core transaction data could provide account name verification, allowing the system to verify that a payment is going to the intended recipient (which would contribute to addressing authorised push payment scams), thus reducing the chance of misdirection of payments and protecting against financial crime scam activities. The solution could also be used to combat a large variety of other transaction verification problems (e.g. identifying unauthorised transactions).

Fraud Victim Identification

Given a known pattern of fraud or scam activity, spanning multiple payments channels, analytical techniques could be used to identify potential consumer victims. Furthermore, at-risk customers could be identified and pre-warned of emerging financial crime threats prior to them being targeted or falling victim to crime. Combining different data sources in this way will enable proactive financial crime prevention.

Suspicious Activity Report (SAR) Investigation

The National Crime Agency (NCA) may be able to use the system to identify and investigate SARs. This capability may reduce the burden and cost on individual organisations for SAR reporting, improving efficiency and reducing cost within the industry. Access to a single, comprehensive view of high quality payments transaction data may allow for increased accuracy, identifying criminal activity that may otherwise have remained undetected when data is split between different systems.

Benefits Fraud Identification

By using appropriate contextual data in combination with transactional data, the solution could be used to identify cases of benefits fraud. This could be done at an individual level using information and techniques to model behaviours of an individual, or a household. This insight could be especially useful for government departments, mandated to seek out and tackle benefits fraud.

Question 6.3

Do you agree with the potential use cases outlined for the Payments Transaction Data Sharing and Data Analytics strategic solution? If not, please provide your reasoning. Please indicate if there are other potential uses for the system that should be considered.

6.2.7 Implementation Approach

This implementation approach is underpinned by key principles that will guide solution development and delivery:

- The first instance of new capability should be implemented by mid-2020 with a programme of enhancements and expansions planned for subsequent years.
- Regulators and other relevant bodies such as the Joint Money Laundering Intelligence Taskforce (JMLIT), Joint Fraud Taskforce (JFT), UK Finance and the Information Commissioners Office (ICO), should be fully engaged throughout the design / build / implement stages and be invited to participate and make use of the new capability.
- A tiered participation and pricing / funding arrangement must be available based on usage of, and contribution to the solution.
- The analysis of the data must be carried out under tightly controlled conditions by accredited entities using approved analytical tools and in compliance with data protection, information security and competition regulations.
- The learnings from the tactical solution should be incorporated into the strategic solution. It should not however be limited to the tactical solution's constraints, participants or suppliers.

The above principles can be reviewed and amended as part of the solution development but only under clear and independent governance.

Identification of and resolution of legal and regulatory constraints to the acquisition, analysis and usage of the data will need to be considered as part of detailed scoping and implementation planning. This may limit the scope of the solution capabilities.

Question 6.4

Do you agree with key principles we have outlined for the implementation of the Payments Transaction Data Sharing and Data Analytics strategic solution?

Question 6.5

Other than those already listed, what stakeholders should be consulted and engaged during the design and implementation of the Payments Transaction Data Sharing and Data Analytics strategic solution?

6.2.8 Indicative Implementation Timeline

The high-level workplan outlined in this document must take planned industry and existing regulatory developments into account.

Figure 6.1 shows the key stages and outcomes of solution implementation, together with indicative timescales. The proposed timelines for implementation are subject to further discussion during handover to the solution body; handover should complete by the end of 2017. The indicative implementation timelines foresee system design completed in 2018 using fully competitive Request For Information (RFI) and Request For Proposal (RFP) processes, system build and testing in 2019, with the first implementation live during 2020.

6.2.9 Transition from tactical solution to strategic solution

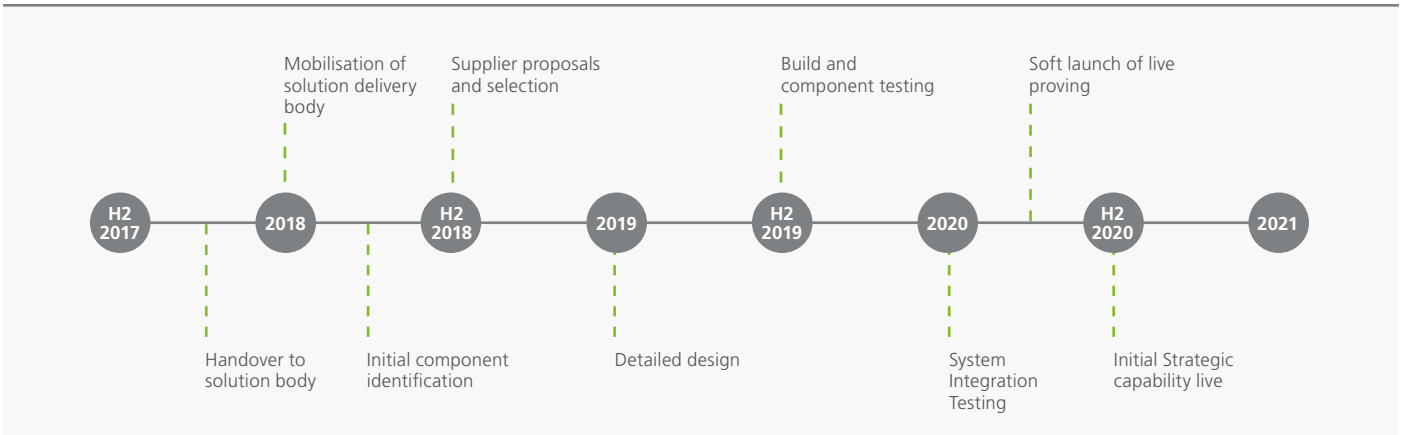
The transition from tactical to the strategic solution will be planned carefully. It will be important to ensure that there is minimal disruption to the service, and so to end-users; this may involve a phased transition, where both solutions are run in parallel for a short time.

The approach to the transition will be developed in conjunction with

Question 6.6

Do you agree with the high-level timeline for the Payments Transaction Data Sharing and Data Analytics strategic solution? If not, what timing would you suggest and why?

FIGURE 6.1 INDICTIVE IMPLEMENTATION TIMELINE



6.3 Trusted KYC Data Sharing

6.3.1 Overview

KYC (Know Your Customer) is the term commonly used to describe due diligence activity undertaken by financial and non-financial institutions when on-boarding a new customer. The purpose is to make sure that the customer is who they claim to be and that financial crime risk associated with that customer is understood and mitigated. It is repeated on a periodic basis throughout the relationship. For business customers in particular, the due diligence process can be complex, involving multiple lines of enquiry which hinders the identification of 'bad actors'.

What is a bad actor?

Bad actors are those individuals or organisations who intend to use the services of a PSP or Financial Institution to commit fraud or other financial crime.

Our Strategy proposed a solution for storing and sharing KYC data between PSPs and potentially other participants, focusing on business customers, enabling more efficient and effective AML and KYC checks. We have undertaken more research to confirm the viability of this solution, and have developed a data sharing framework which is expected to enable the development of a market for the provision of KYC services and a range of facilities supporting other business activities.

We recommend that SMEs (Small and Medium Enterprises) should be the initial focus of this framework. The main reasons for this decision are the materiality of SMEs to the UK economy, the limited number of third party or shared KYC solutions for SMEs, the high relative costs of KYC in this market segment and significant financial crime activity by bad actors within the SME segment.

The greater the number of participants utilising the exchanging mechanisms, the more often the data is refreshed, verified and updated with the SME customers' consent. Therefore, participants will have more efficient access to the most complete and highest quality data. The outcome will be increased opportunity to detect bad actors, whilst streamlining the KYC process between SMEs and PSPs. Participants will receive tangible benefits from the beginning, including reduced barriers for PSPs to enter the market and SMEs being able to more easily access new products and services as a result of more efficient due diligence processes.

In summary, the recommended data sharing framework will consist of the following components:

1. Baseline standards for sharing a core set of SME customer data, accepted within and beyond the payments industry, to support SME KYC processes.
2. A permanent governance body monitoring adherence to standards and rules, including responsibility to mitigate the risks of abuse, fraud, privacy and security issues.
3. A temporary testing environment aimed at encouraging the development of a market for value-added KYC services.

6.3.2 Problem Statements and Detriments

The banking and payments industries are currently undergoing a dramatic transformation as they embrace the digital revolution. Increased customer engagement and better experience, choice, competition, transparency, and new innovative services are some of the desired outcomes being driven in part by a technology revolution and in part by EU and UK government initiatives and policy.

The introduction of the General Data Protection Regulation (GDPR) in May 2018, together with industry-specific regulation including the second Payment Services Directive (PSD2) in Europe and the Competition and Markets Authority (CMA) remedies in the UK, mean that a tipping point has been reached which is compelling the industry to identify new ways to interact with their customers.

In particular, the CMA 'Retail Banking Market Investigation' report of November 2016 recommended a 2018 review by the Treasury with regards to secure data sharing for SMEs between PSPs and third parties, which allows them to manage their accounts with multiple providers.[48] These changes will potentially have a significant impact on the KYC processes of PSPs operating in the UK.

Since publishing our Strategy, we have reviewed the approach and agreed on the following detriments as focus areas for the proposed data sharing framework:

- **Inclusion of bad actors:** Obtaining sufficient KYC information to identify bad actors requires the use of multiple external data sources and systems during on-boarding and ongoing due diligence. Incomplete, in-accurate or out-of-date SME customer data hinders the detection of bad actors.
- **Poor customer experience for good actors:** Limited data sharing among the PSPs and other sectors such as utilities and telecommunication providers lead to significant duplication of effort if a customer moves to another provider or extends their products.
- **Barrier for small PSPs:** Privileged access to SME data can be viewed as a barrier for small and new entrants, narrowing access and weakening competition.
- **Inefficiency in the SME KYC process:** Customer identification processes can be complex, protracted, and expensive, despite not being a key competitive differentiator for PSPs and providers in other sectors.
- **Lack of trust:** The fear of fraudulent actors potentially being able to penetrate the digital environment and get access to customer data leads to an erosion of trust in society.

[48] 'Retail Banking Market Investigation' report, CMA, 9 August 2016, pages 621 - 625.

6.3.3 Data Sharing Framework

We have conducted research into the UK payments market, concentrating on SME-focused PSPs and financial service providers. Most of them have their own commercial constraints and requirements for KYC services so it is unlikely that a 'one-size fits all' KYC shared service utility with a central repository could be successfully built and used to meet the heterogeneous market needs.

Instead, we recommend the establishment of a data sharing framework (see Figure 6.2) to provide a method of sharing a core set of SME customer data between organisations acting as data providers where the customer already has an account (e.g. a bank or insurance company) and other organisations who use that data with the customer's consent (data consumers).

The framework will consist of a set of standards for the sharing and exchanging of a core set of SME customer data overseen by a governance body, and supported by a temporary testing environment. It is our view that the lack of industry-wide standards, rules and governance has limited the market adoption of data sharing solutions in the past. It is expected that the data sharing framework will resolve this and lead to a range of competitive value-added KYC services using the evolving data sharing capability.

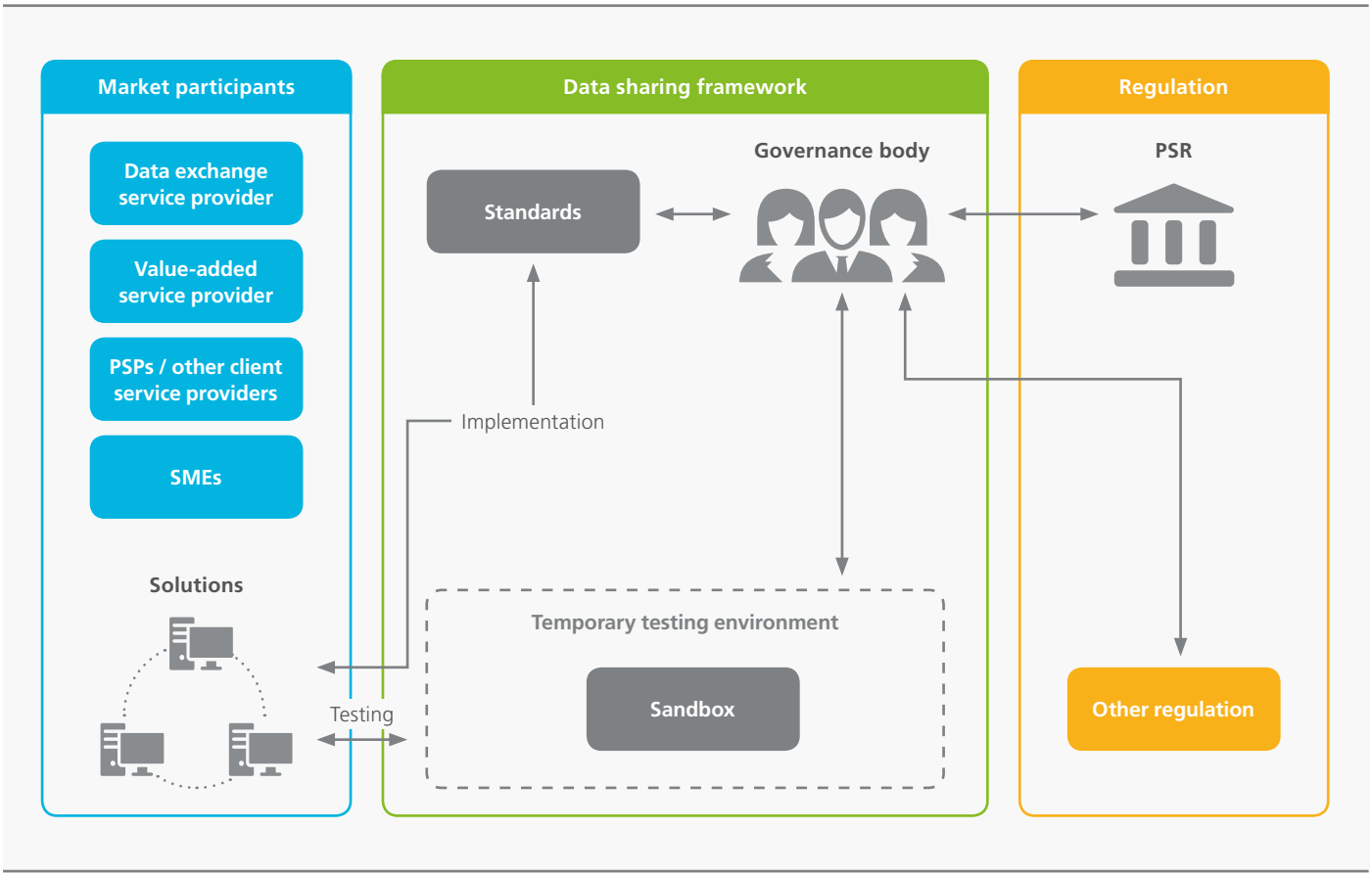
Data sharing is intended to be on a point-to-point basis between PSPs, or via data exchange service providers which offer a single point of connectivity between data providers and consumers.

Data will only be shared with the customers' consent. For example, an insurance company (data consumer) can only receive customer data from a bank (data provider) about a customer (data owner), with that customer's consent. In this example, the insurer could also purchase services from a data analytics company (KYC service provider) to further enhance and validate the data being shared. The whole network and the wider public will benefit from improved (i.e. corrected, verified and timely) customer information through updates during each interaction. The results will include improved customer experience, reduced KYC operational costs and increased ability to identify bad actors and reduce financial crime.

The data sharing framework is expected to enable the development of a market for the provision of KYC services as well as a wider range of services supporting other business activities. Data exchange service providers will be able to participate by complying with the standards set by the governance body. Value-added service providers will be able to test their KYC services against the specific needs of individual PSPs and client service providers in the temporary testing environment.

This will increase the transparency of different processes and standards employed by individual PSPs and client service providers, fostering a more competitive and innovative market for the provision of third party services.

FIGURE 6.2 SCHEMATIC PICTURE OF DATA SHARING FRAMEWORK



As a result, there will be a wide variety of participants interacting through the data exchange environment:

- **Data exchange service providers:** Vendors offering data exchange services to the whole range of participants within the environment.
- **Value-added service providers:** Vendors offering additional value-adding services, including services across the whole KYC value chain to PSPs and other financial institutions.
- **PSPs and other client service providers:** Financial institutions and other industry participants outside financial services that will exchange data through the open data sharing environment.
- **SMEs:** Customers of the financial institutions which will own the data and consent for the sharing of their private information, relating to both the business and its key individuals.

Given the diverse nature of payment providers, it is important that the costs to PSPs and client service providers are affordable, in particular, to those operating at smaller scale. The data sharing framework supports this by avoiding the need for PSPs and client service providers to adopt a standardised set of KYC processes, and therefore bear the cost of convergence. The framework also encourages competition and therefore a more diverse and innovative range of services in all areas. This prevents any individual institution from dominating one particular part of the ecosystem, and therefore avoids the risk of anti-competitive behaviour.

The proposed data sharing framework would deliver the following advantages:

- **Open:** Accessible to institutions and vendors of different sizes that wish to participate.
- **Governed:** Participants register and agree to conform with the standards set by the governance body.
- **Accessible:** Using API-based technology that is secure, re-usable and scalable.
- **Customisable:** PSPs and client service providers will benefit from access to a wider range of services and solutions (depending on their needs and financial limitations) and the ability to offer their own services to third parties.

Question 6.7

Do you agree with the establishment of the recommended framework for the sharing and exchanging of a core set of SME customer data overseen by a governance body? If not, please explain your reasoning.

Question 6.8

We are keen to get your input on the benefits provided by the framework.

a. Do you agree that the focus on sharing a core set of SME customer data is beneficial for the KYC processes in your organisation? If not, please explain your reasoning.

b. Which other business activities could be supported by / benefit from the described sharing and exchanging a core set of SME customer data?

6.3.4 Data Sharing Standards

The definition of mutually agreed data sharing standards and accompanying oversight from a governance body are required to increase trust among the participants and maintain the interoperability between the exchanges of data through the environment. Each PSP will continue to perform their own due diligence over data received through the sharing mechanisms; however, they will receive the most up-to-date data more efficiently, and with the explicit consent of the SME customer. It is important to note that in the absence of the provision of confirmation services, data is being exchanged on a non-reliance basis.

High levels of trust associated with compliance with the standards are required to secure higher investment from a greater number of solutions and drive faster adoption by PSPs. Similarly, a common brand or 'kite mark' confirming compliance with the standards is expected to increase the likelihood that SMEs will provide consent on the use of their customer data through the exchange mechanisms.

We envisage two scenarios for the sharing of data between PSPs and other client service providers through a network: Peer-to-peer data exchange; and exchange of data through data exchange service providers which offer connectivity, removing the need for individual PSPs and client service providers to build their own point-to-point networks.

The standards will be developed by the governance body to accommodate both scenarios and all network participants will need to conform to the specified rules. The scope will evolve incrementally as the solution offerings expand and new regulatory requirements emerge (e.g. extensions to the data model and additional security requirements). The baseline standards defined will cover the following topics:

- **Sharing capabilities and interoperability:** Defining the sharing mechanisms between the data provider and the data consumer, e.g. consent process and cooperation recommendations to ensure that both provider and consumer contribute data.
- **Data model:** Defining the data model building upon some components of 'The standard information set' developed by CMA, including completeness requirements and data access rights. A minimum set of fields will be defined that ensures flexibility for different KYC processes and regulatory requirements.

We recognise that many of these topics are already being addressed for the purposes of Open Banking and PSD2. The governance body will draw on the progress made in each of these areas. Further details of the standards scoping and governance oversight can be found in the supporting materials accompanying this document.[49]

Other standards related to sharing data are available (such as OAuth 2.0 and the Open ID Connect protocols), but are not specifically designed for use in association with KYC services. The proposed KYC Data Sharing standards are complementary to these and it is anticipated that all standards will develop over time to meet the needs of the evolving market place.

Question 6.9

Do you agree that the topics covered by the standards will provide sufficient guidance in order to implement the data sharing framework without being too prescriptive? Are there additional topics you believe should be included?

6.3.5 Governance Body

The governance body must ensure that the standards evolve on an ongoing basis to cover the needs of the whole range of participants. It will supervise the authentication process ('kite marking') for participants that are compliant against the defined data sharing standards, and will have the authority to revoke the certification of participants that no longer meet them.

Overall responsibilities of the governance body will include the following activities:

- **Define the standards** on the sharing and exchange of a core set of SME customer data through the environment.
- **Evolve the standards** to meet the needs of the whole range of participants (SMEs, PSPs and KYC service providers).
- **Enforce compliance** of the defined data exchange standards.
- **Encourage participation and usage by PSPs and SMEs** in the data sharing environment.

Question 6.10

To engender trust in the sharing and exchanging of a core set of SME customer data, are there other responsibilities you would expect the governance body to have oversight over?

Question 6.11

In your view, do any existing bodies (industry or other), already perform this oversight role? If not, is there an existing body you believe should perform this role, or would you expect a new body to be established?

6.3.6 Temporary Testing Environment

The objective of the temporary testing environment is for an early adopter community of PSPs, service providers and technical providers to exchange data in a safe environment, in order to test and fine tune the interoperability between the different methods used to exchange data.

The temporary testing environment will support the development of the process to certify all participants against the data exchange standards. Importantly, the temporary testing environment will also provide an environment for third party KYC service providers (Section 6.3.7) to position, market and refine their value-adding service offerings. The temporary testing environment provides a mechanism to aggregate and manage the demand for KYC services from the PSPs and other service providers. It can help to identify the needs, specify the services and required standards of delivery and monitor volumes.

At the same time, it can help to aggregate buying and communication power, e.g. in the event that two separate PSPs are looking for the same KYC service. The temporary testing environment also offers a single interface for suppliers looking to sell their services and define service terms like quality, price and set-up fees. It makes it easier for PSPs and client service providers to buy services, and for KYC service providers to sell them.

The environment will help to improve market competition and is expected to lead to development of a range of solutions resolving shared industry problems, particularly ones driven by upcoming regulatory change such as GDPR and PSD2. Multiple exchange providers and peer-to-peer networks can coexist in the temporary testing environment and allow third party service providers to use the established data foundations to demonstrate value-added services to potential PSP customers.

The temporary testing environment will have the following features:

- It will allow the testing of the standards designed for the exchange of customer data.
- It will provide an environment for KYC service providers to test and demonstrate their offerings to Financial Institutions using the provided data sharing environment.
- It will be flexible enough to test future requirements within the KYC end-to-end value chain including data validation, customer screening and other functionalities.

Question 6.12

Do you think a temporary testing environment as described is the right approach? If not, please explain your reasoning.

Question 6.13

Are there any other key features you would expect in the temporary testing environment?

[49] The Trusted KYC Data Sharing - Standards Scope and Governance Oversight document can be found at the following link: https://implementation.paymentsforum.uk/consultation

6.3.7 Value-Added Service Providers

The focus of the data sharing framework is to provide a data sharing environment as described in the section above. A range of potential business propositions have been identified that could leverage the exchanging capability provided by the environment to offer additional services to PSPs, and so drive adoption of the service (see Figure 6.3). These have been grouped into three broad categories:

1. KYC service providers
2. Confirmation service providers
3. User authentication services / data passports

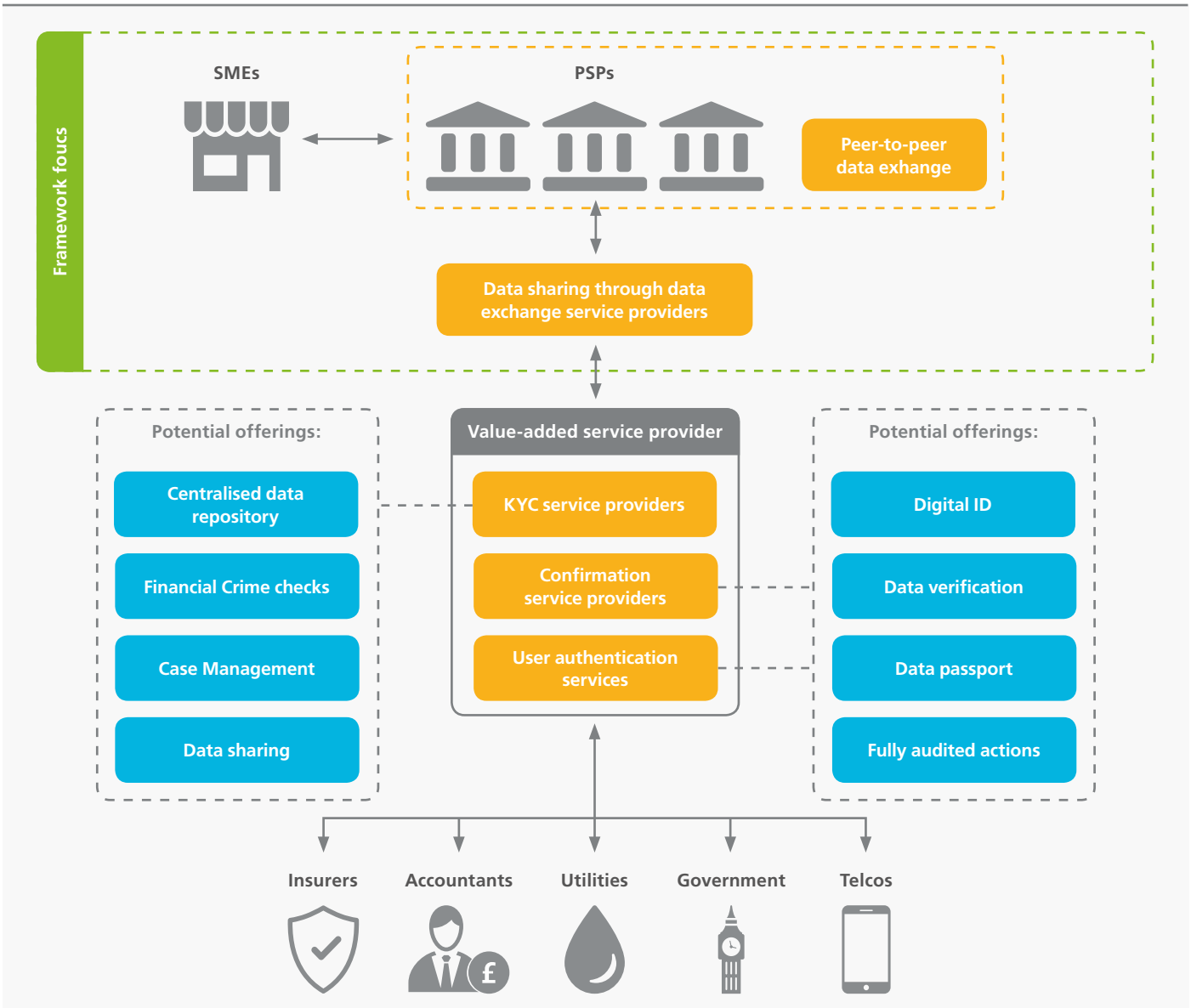
The data sharing framework is inclusive and further business models could be integrated at a later stage.

KYC Service Providers

A wide range of KYC and data sharing services are offered by providers including KYC utilities. PSPs can either subscribe to services from different providers, use a KYC utility, or rely on their own in-house processes. Examples include centralised data storage, data collection, classification, cleaning and processing. KYC services are offered across the due-diligence value chain, including financial crime checks, client risk classification and workflow management.

A KYC utility is a central repository that stores the data and documents required to support the PSPs KYC procedures. Once the SME data has been entered into a utility, member PSPs can access and leverage the information for their own individual KYC requirements. Centralising the collection of customer information into a common repository that's accessible by participating PSPs eliminates duplicative KYC activities across the industry. This can increase standardisation of KYC quality and compliance.

FIGURE 6.3 OVERVIEW OF BUSINESS MODELS ENABLED BY THE DATA SHARING FRAMEWORK



Confirmation Service Providers / Digital ID

Confirmation services include identity provision, attribute provision and data verification. They differ from the services outlined above in that they include a transfer of liability between the relying party and the confirmation service provider.

Identity schemes - sometimes called 'identity proofing' - are the most well-known form of confirmation service, and are often implemented at a national level to confirm the identity of an individual. Several government identify schemes have been implemented to date, such as GOV.UK Verify in the UK. The schemes undertake the due diligence necessary to link a digital identity (for example an email address) with a physical or legal entity (i.e. the citizen who uses that address).

User Authentication Services / Data Passports

User authentication is another important aspect of the security and integrity of KYC data sharing. User authentication is the process through which service providers check that the digital identity seeking access to their services has the authority to do so. This is usually done through the exchange of credentials (user name / password) and the use of secrets or keys.

A data passport is the most prominent example of these services. Customers can give their consent to an institution to access and use the data that is already linked to the data passport. As well as providing user authentication and consent at the point of transaction, a data passport could also be accessed directly, giving the customer an opportunity to review their digital footprint, add links to data held by other institutions that they engage with as customers, and update their data.

Question 6.14

Do you agree that value-added service providers would benefit from the data sharing environment enabled by the framework?

6.3.8 Data Consumers and Data Providers

The data sharing environment will provide benefits to both data consumers and providers among participant PSPs and other client service providers. In most cases, the participants will act both as data consumer and data provider, thus extending the range of benefits received from sharing data within the environment.

This environment will only be successful if network participants are willing to share their core set of SME customer data with other PSPs and client service providers. While data consumers will directly profit from receiving the data, there is currently limited regulation requiring data providers (in most cases larger PSPs) to share their valuable customer data. The sections below illustrate the requirements and advantages for both net consumers and net providers.

Benefits for Net Data Providers

Financial institutions holding most of the customer data (entities with large customer databases) will receive a great number of requests from other institutions and service providers to share customer information with them. Upcoming regulation might require them to share and exchange their core set of SME customer data in the future. Under GDPR, these larger financial institutions are required to provide customers access to their own data, and to ensure that it is portable to third parties. Our recommended solution supports the implementation of these personal data rights. The solution also enables them to prepare for a review of data sharing by HM Treasury in 2018, as specified in the final CMA report highlighted in Section 6.3.2.

There are also several business opportunities and advantages for net data providers. They will be able to provide an enhanced customer experience by offering easier access to products and services from other sectors like telecommunication companies and utilities providers. Furthermore, these institutions are well positioned to compete in the market for value-adding services, potentially enabling them to partly recover the cost of their existing KYC processes, for example:

- Utilising their trusted brand to offer user authentication services like data passport models.
- Providing confirmation and other data services to other client service providers.

Benefits for Net Data Consumers

Net data consumers will receive direct benefits from the exchange of the data through the environment. The received core set of SME customer data from other entities reduces the operational work required to obtain the data and supporting evidence and will lead to lower cost and a faster on-boarding process. This enables them to provide a better customer experience and potentially increased revenues due to increased customer interest.

Through access to value-added services these institutions may also identify mechanisms to improve the quality and accuracy of their customer due diligence processes and / or perform it more efficiently. Sharing this data in the network will continuously ensure data is up-to-date, complete and accurate.

Question 6.15

Are the arguments put forward compelling enough to encourage net data providers to engage? If not, please provide examples of what else would be required to make them participate.

Question 6.16

Do you see other advantages or challenges for net data consumers that were not listed above? Please explain your answer.

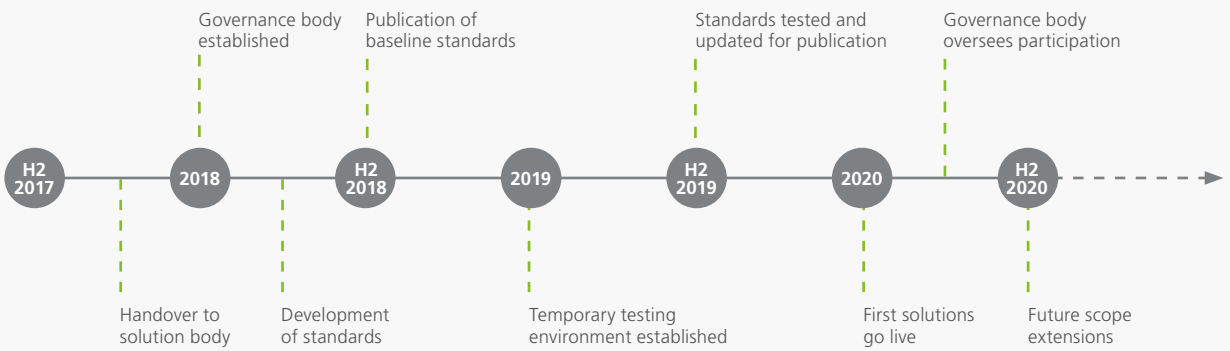
6.3.9 Proposed Implementation Approach

We recommend the data sharing framework to be handed over to an agreed industry body or organisation by the end of 2017. The body needs to establish necessary governance, define standards, and specify the mechanisms to establish the temporary testing environment. The range of solutions and participants of the data sharing environment will develop over time, increasing the benefits and subsequently mitigating more detriments.

Figure 6.4 shows the key stages and outcomes of solution implementation, together with indicative timescales. They need to be confirmed by the body identified to carried forward implementation, and further elaborated into a detailed plan.

Further details of the key stages and outcomes as well as the evolving benefits provided by the data sharing environment can be found in the supporting materials accompanying this document.[50]

FIGURE 6.4 HIGH LEVEL TIMELINE – IMPROVING TRUST IN PAYMENTS



Question 6.17

Do you agree with the high-level implementation timeline for the Trusted KYC Data Sharing solution? If not, what timing would you suggest and why?

Question 6.18

Are there other initiatives with a similar focus that should be considered in order to deliver the Trusted KYC Data Sharing solution?

6.4 Next Steps

We have assessed the next stages of activity required to ensure a successful handover, by the end of 2017, of the remaining financial crime solutions to appropriate organisations, capable of progressing the solutions to implementation. We will define a handover process with a detailed timeline which will take into consideration the consultation responses to the Payments Transaction Data Sharing and Data Analytics, and Trusted KYC Data Sharing solutions.

Further detailed analysis will be required following the outcome of the Liability Models for Indirect Access questionnaire (the full questionnaires can be accessed here.[51]); a recommendation report will be developed and socialised to a wide payments community prior to handing over the solution to an appropriate body capable of implementing the recommendations. For further details of our work on the Liability Models for Indirect Access solution please see Appendix 8.

[50] The Trusted KYC Data Sharing - Framework Implementation document can be found at the following link: https://implementation.paymentsforum.uk/consultation
[51] Link to Forum website to access questionnaires: https://implementation.paymentsforum.uk/access-account-services-questionnaires

7.0
Next Steps

About this section

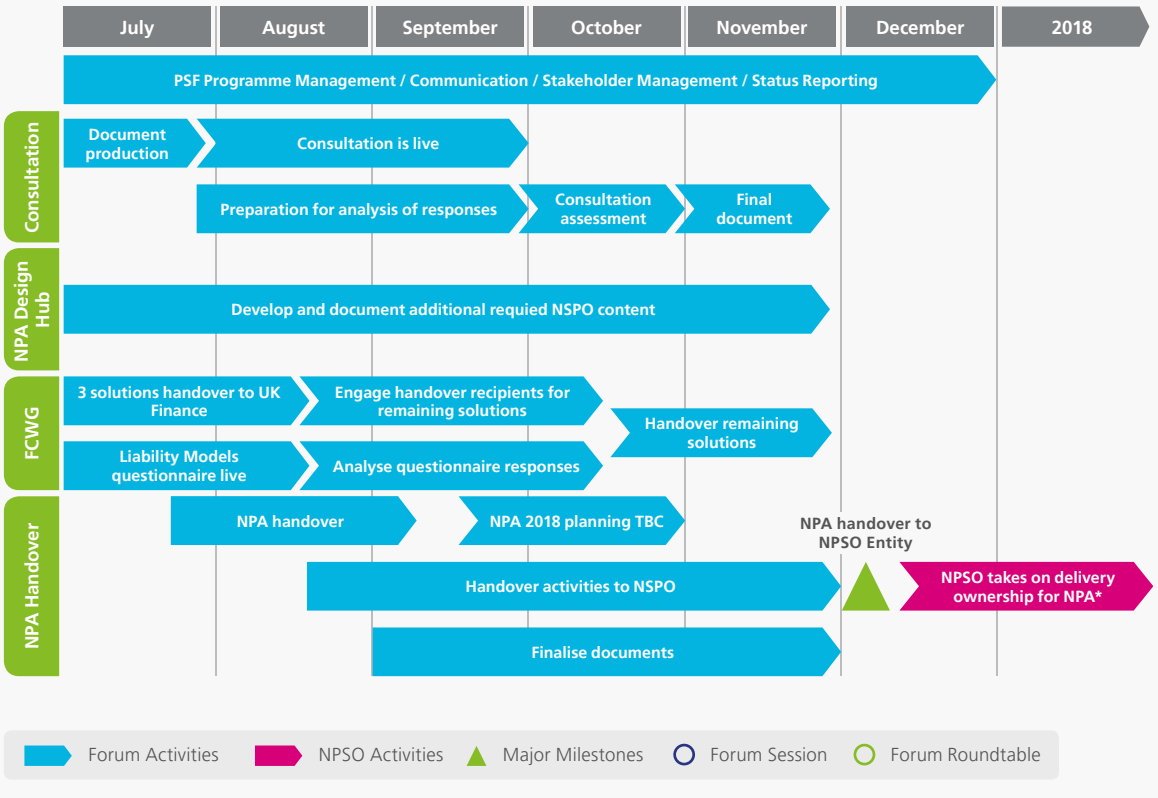
In this section we outline the Forum's activities for the remainder of the year post the publication of this consultation document.

Most importantly, we will be collating the responses received from stakeholders. Your responses to this consultation will be used to help shape the Forum's decision on the high-level blueprint for the future NPA and Financial Crime solutions.

Following the consultation, the next stage of NPA development and implementation will be taken up by the NPSO. Furthermore, all Financial Crime solutions will be handed over to appropriate organisations to continue implementation; this process has been completed, is in progress, or planned for Q4 2017 depending on the solution.

Activities are summarised in Figure 7.1 below, with further details in subsequent sections.

FIGURE 7.1 HIGH-LEVEL PLAN OF ACTIVITIES POST PUBLICATION OF THE CONSULTATION DOCUMENT



* Including competitive procurement of any central infrastructure.

7.1 Consultation Process

The consultation period starts with the formal issuance of this document on the 28th of July and will close on the 22nd of September.

The consultation process will:

- **Provide transparency** of the Forum's work on the NPA and Financial Crime solutions to the Payments Community.
- **Solicit input and confirmation** from an audience representative of all participants in the payments ecosystem.

Consultation responses will be used to finalise our documents for handover by the end of 2017.

In parallel to the consultation process, we will:

- Prepare to analyse consultation responses.
- Continue to develop NPA design materials.
- Continue planning for the NPA handover to the NPSO.
- Continue stakeholder engagement for the Payments Transaction Data Sharing and Data Analytics, and the Trusted KYC Data Sharing solutions, to support the consultation process.
- Continue to deliver against our plan for the Liability Models for Indirect Access solution as the questionnaires close on 18th August.
- Engage the appropriate handover entities for the remaining Financial Crime solutions to ensure effective handover in Q4 2017.

7.2 NPA next steps

The NPA high-level blueprint and associated material will be handed over to the NPSO in December 2017. Further handover planning will commence following the start of the consultation, including engagement with NPSO DG / IG to schedule handover activities. This will include proposed timelines for the activities of the NPSO following handover.

Aside from analysing consultation feedback, producing the consultation report, and preparing for handover to the NPSO, the activities of each NPA workstream are outlined below:

TABLE 7.1 NPA HANDOVER ACTIVITY SUMMARY

Workstream	Next Steps
NPA Design and Transition	• Further analysis of how Open Banking APIs and capabilities can be used to support the delivery of the NPA. • Additional analysis of areas of the NPA to aid handover to the NPSO. Potential areas include the API delivery plan and development of the requirements for the directory, consent and authorisation stores.
Collaborative Requirements and Rules for the End-User Needs solutions	• Analysis of liability and risks for the three EUN Solutions. • Analysis of data protection and privacy regulations across the EUN Solutions especially as pertain to GDPR.
Implementation Plan	• Further assessment of a detailed timeline taking consultation responses into consideration (including further commentary on principles and assumptions, as well as options for Bacs direct debit and credit solutions). • Definition of high-level risks and a review of mitigating factors in collaboration with industry participants. • Continued identification of synergies between the NPA and industry initiatives.
Cost Benefit Analysis of the NPA	• Updating CBA materials as required based on any changes to NPA design elements resulting from analysis of consultation responses.
NPA Commercial Approach and Economic Models	• Update documentation to reflect the responses to consultation, aligning with changes to elements of the NPA design as appropriate.

7.3 Financial Crime solutions next steps

In the rest of 2017, we will look to conclude the handover of our Financial Crime solutions to appropriate organisations to continue implementation. Of the seven Financial Crime solutions, four have already either completed or are completing formal handover. More details on these activities can be found in Appendix 8.

In addition, the following three solutions will look to complete handover in Q4 of 2017:

- Payments Transaction Data Sharing and Data Analytics is expected to handover to the NPSO.
- Trusted KYC Data Sharing will handover to an appropriate industry body or organisation (to be identified).
- Liability Models for Indirect Access will handover to an appropriate organisation, the identification of which may depend on the responses received to our questionnaires.

Table 7.2 outlines the activities for these solutions in the rest of 2017:

TABLE 7.2 FINANCIAL CRIME SOLUTIONS HANDOVER ACTIVITY SUMMARY

Workstream	Next Steps
Payments Transaction Data Sharing and Data Analytics	• Further stakeholder engagement to support the consultation process. • Analysis of consultation findings and development of consultation report. • Finalisation of solution deliverables, reflecting the responses received from consultation. • Engagement with the NPSO to define, agree and complete a formal handover process.
Trusted KYC Data Sharing	• Further stakeholder engagement to support the consultation process. • Analysis of consultation findings and development of a consultation report. • Finalisation of solution deliverables, reflecting the responses received from consultation. • Identification of an appropriate industry body or organisation to own the solution following handover from the Forum. • Definition, agreement and completion of the handover process.
Liability Models for Indirect Access	• Analysis of responses received to the published questionnaires. • Production of questionnaire report to set out key findings. • Identification of an appropriate handover organisation based on the responses from the questionnaires, and definition of the handover process. • Finalisation of solution deliverables to support handover.

8.0 Appendices

8.1 Appendix 1 – Summary of the Ongoing Solution Ownership

TABLE 8.1.1 ONGOING SOLUTION OWNERSHIP

Solution	Ownership
Request to Pay	We have progressed these solution alongside the design of the NPA. More information can be found in Section 2 of this document.
Assurance Data	
Enhanced Data	
Guidelines for Identity Verification, Authentication and Risk Assessment	We have progressed these solutions as set out in the Strategy prior to being handed over to appropriate industry bodies to carry forward. More detail can be found in Section 6 of this document.
Payment Transaction Data Sharing & Data Analytics	
Financial Crime Intelligence Sharing	
Trusted KYC Data Sharing	
Enhancement of Sanctions Data Quality	
Customer Awareness & Education	
Access to Sort Codes	This solution has already been implemented by BPSL.
Accessible Settlement Account Options	The BoE's development of this solution has been taken into consideration where appropriate.
Aggregator Access	As per the Strategy, this solution is being implemented by the PSOs.
Common PSO Participation Model and Rules	As per the Strategy, this solution is being progressed by the Interbank System Operators Coordination Committee (ISOCC).
Establishing a Single Entity	As per the Strategy, this is being progressed by the PSO DG.
Moving the UK to a Common Message Standard	Included in the design of the New Payments Architecture as a key requirement.
Indirect Access Liability Models	This solution has been progress as part of the Financial Crime Working Group.
Simplified Payments Platform	This has been progressed within design of the New Payments Architecture.

8.2 Appendix 2 – Alignment of the NPA to Industry Initiatives

8.2.1 Payment Services Directive 2 (PSD2)

PSD2 is proposed as a way to respond to the changes in the payments landscape and to promote improvements and innovation in payment services across Europe. PSD2 includes proposals to:

- Level the playing field for Payment Service Providers (PSPs), including new players.
- Ensure a high-level of consumer protection and payments security.
- Encourage lower prices for payments.
- Facilitate the emergence of common technical standards and interoperability.

The NPA is fully aligned with PSD2 and each layer of the architecture has been established to work within and support the PSD2 framework. This includes areas of the NPA design, such as payment initiation, which includes the new PSP definitions and security standards.

8.2.2 Open Banking

Open Banking provides a standard and framework for how bank data should be created, shared and used. Specifically, it provides standards for 'open APIs' that will facilitate transactions governed by PSD2 data sharing requests. It is recommended that the NPA adopts these APIs as they meet (or will meet) the needs of the NPA and could reduce the need for additional development by the organisations offering services within the different layers of the NPA.

It is also recommended that consideration is given to adopting Open Banking directory services once it is clear how it will support all the potential users of the directory (and not just the CMA9 PSPs). An assessment of the Open Banking directory service indicates that it can meet the requirements of the different roles and layers within the NPA, such as supporting the delivery of the key functions of participant registration, identity access management and security authentication. Should it be required however, the NPA would not preclude the use of a third party provided alternative for the supply of the directory services capability.

8.2.3 General Data Protection Regulation (GDPR)

GDPR impacts all organisations that process European Union citizen's personal data and aims to encourage organisations to construct a data protection strategy with privacy at the core. Key features of GDPR include the pseudonymisation of customer data whether in transit or at rest and that the customer's details are the property of the customer.

The design of the NPA should not inhibit the NPSO's ability to build a GDPR compliant system and would enable their governance role to ensure the participants within the layers of the NPA can also be compliant with both the GDPR technical security, customer rights to data and privacy requirements.

8.2.4 Fourth Money Laundering Directive (4MLD)

The Fourth Money Laundering Directive prevents the use of the financial system for the purposes of money laundering or terrorist financing. Much of the directive points to procedural changes outside of the NPA, however the NPA's support of enhanced data and payment status capabilities could be used (if so directed by applicable laws) to provide valuable information in the campaign against money laundering and associated illicit activities. Along with the other regulatory requirements, it is suggested that this area will require further consideration as the NPA is specified, procured and delivered.

8.2.5 Real Time Gross Settlement (RTGS)

The Bank of England has mandated the use of the revised RTGS service to settle payments in the UK. The NPA architecture has been designed with this settlement service at its core and will work with the BoE to be fully compliant with the requirements for interfacing with the renewed RTGS. It is worth noting that the transition to the NPA is dependent upon having mechanisms within RTGS to settle in central bank money.

8.3 Appendix 3 – NPA Key Use Case Scenarios

8.3.1 Direct Debit

Direct Debits is a product offered by BPSL that allows organisations to collect payments from their customer's account once a mandate has been authorised by the customer and lodged with their bank. Organisations that use the existing Bacs Direct Debit payment system will still require the ability to automatically collect a payment from their customer's bank account.

Under the new payments architecture, Direct Debit payments will be made via a push payment model which makes the delivery of a Direct Debit payment consistent with other payment types such as Direct Credits, Single Immediate Payments (SIP) and Standing Order Payments (SOP).

The clearing and settlement system will receive a Direct Debit file that has been authorised by the payer's Payment Service Provider (PSP) and sent to a single receiving PSP. A single debit and credit amount (the sum of all payments in the file) will be used for settlement risk and settlement processing.

In addition, the Direct Debit payment product comes with a guarantee that ensures an immediate money back guarantee from the customer's PSP in the event of an error in collection, advance notice if the date or amount changes and the right to cancel at any time. The NPA framework intends to support these aspects of the Direct Debit customer proposition, along with the necessary reporting requirements provided to PSUs today.

Organisations are expected to continue producing a bulk collections file as they do today. Under the NPA framework, the organisation will require the role of a Third Party Payment Service Provider (TPSP) to authorise a mandate and process the bulk collections file. The TPSP will be registered to provide Direct Debit services as per existing Direct Debit regulations. The TPSP role could be provided by the payee's bank (PSP), an existing Bacs software solution provider, a new payment provider or the organisation themselves. It will be the TPSP's responsibility for submitting the bulk collection file to each of the payer's PSP to ensure payments are made by the collection due date. Organisations that currently submit a bulk collection file directly into the Bacs central infrastructure will now require the role of a TPSP to process their file. The TPSP has an opportunity to minimise the impact on the organisation when migrating to the NPA. For example, whilst the bulk collections file will be required to be produced in the new ISO 20022 file format, the organisation could continue to create the file in their existing file format and allow the TPSP to convert the file into the ISO 20022 format. In addition, the organisation could continue to create the bulk collections file three days earlier than the due date (as per the existing Bacs Direct Debit scheme) and the TPSP would ensure that the payment file is held and submitted for collection on the actual due date.

Given that cleared funds are submitted into the clearing and settlement system, the current unpaid Direct Debit process is simplified using the NPA framework. Payments that could not be applied to the individual's account on the due date will be rejected and reported to the organisation on the same day the payment was due to be taken. The organisation is able to respond more quickly to the failed payment rather than wait for two further days as per the existing Bacs Direct Debit scheme.

Direct Debit Example Use Case

The following example summarises the Direct Debit process. It includes the requirement to set-up and authorise a mandate (Steps 1 to 3) and to collect the Direct Debit payment (Steps 4 to 10). Further details of the Direct Debit process within the NPA are included in the NPA Design and Transition Supporting Document.

It should be noted that there could be more than one way to process a Direct Debit payment and the steps described below offers one potential approach.

Step 1
A request for payment is initiated by the payee and a mandate is set-up prior to the first collection taking place.

Step 2 and 3
A request for a mandate is sent to the payer's PSP for authorisation.

Step 4
Based on the payer's authorisation, the payee's PSP initiates the payment as a push payment.

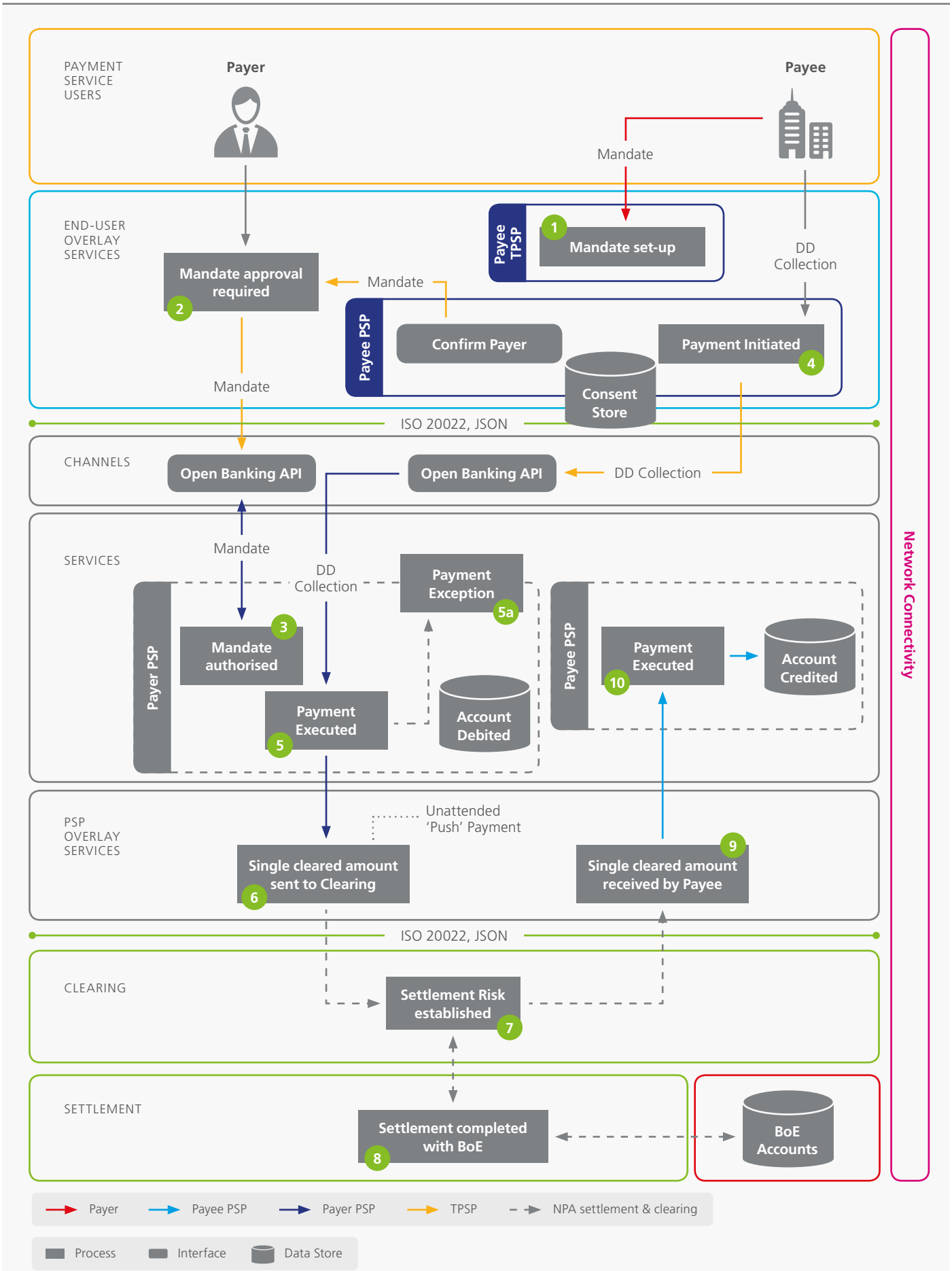
Step 5
The payee's PSP disaggregates the bulk collection file and sends a file to each payer's PSP to debit the individual's account on the due date.

Step 5a
Unpaid payments are notified to the payee's PSP on the due date.

Step 6 to 9
A single bulk value for the cleared funds is submitted by each PSP to the clearing and settlement system. Note: the clearing process for bulk payments is consistent with clearing for Single Immediate payments.

Step 10
The payee's account is credited with funds by the payee PSP.

FIGURE 8.3.1 DIRECT DEBIT EXAMPLE



8.3.2 Cheque Payment

It is expected that customers are still likely to require the ability to make a payment via cheque. As shown through the example below, the NPA framework can support cheque based payments that use the Image Clearing System (ICS).

The steps listed along with the diagram below illustrate how an ICS based payment could potentially be supported using the NPA framework. In this example the customer is assumed to physically present a cheque in a PSP's branch. In this case, the PSP would assume the role of the TPSP in order to initiate the request for a cheque payment.

Other channels such as bulk and intelligent deposit machines can be used to submit an ICS payment including the customer capturing the image of the cheque and sending it directly themselves to their TPSP for processing.

Step 1 and 2
The customer (payee) presents a cheque at a physical branch to be deposited into their account. The branch scans the cheque and sends the details to the payer's TPSP.

Step 3
The payer's TPSP validates the cheque details e.g. duplicates, fraud or high value.

Step 4a to 4d
If it is a high value cheque the payment may require the payer to authorise the cheque before processing it. This authorisation process is consistent with a suggested process used to set-up Standing Orders.

Steps 5 and 6 (including 6a and 6b)
The cheque payment is initiated by the payer's payment initiation TPSP and the payer's account is debited. Where the payment cannot be executed, the payee's TPSP is notified via the paid/not paid message.

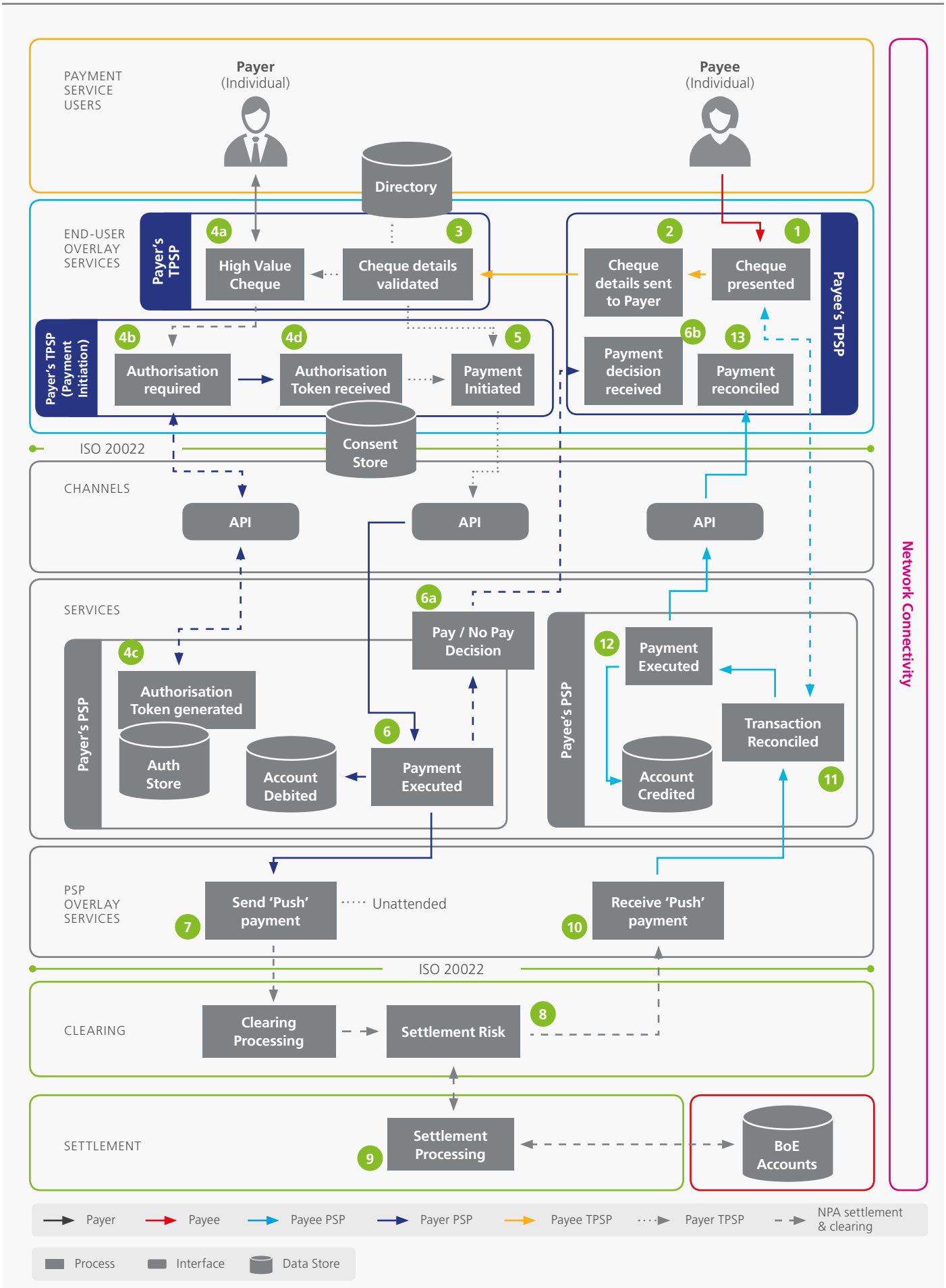
Step 7 and 8
Cleared funds are 'pushed' to the clearing and settlement service and a settlement obligation is created between each PSP.

Step 9 and 10
The clearing and settlement service initiates settlement with the Bank of England and payment details are sent to the payee's PSP.

Step 11 and 12
The payment is reconciled against the cheque received from the payee's TPSP and the payee is credited with the amount.

Step 13
Finally the payee TPSP's reconciliation process ensures that the payment has been cleared.

FIGURE 8.3.2 CHEQUE PAYMENT EXAMPLE



8.3.3 Direct Submission

There are approximately 45,000 organisations that directly submit payments to BPSL in the UK today. The NPA will be able to support direct submissions and the following diagram shows one way in which this could be achieved, along with the roles within the NPA framework that are required to fulfil a direct submission. With the eventual sun-setting of the Bacs scheme, a directly submitting organisation (such as a large corporate) will still be able to submit payments into clearing and settlement but they will need to ensure that the payments are routed to the correct recipient PSP. The routing of payments will be carried out by the role of the TPSP who could be an existing Bacs software solutions provider, a new payment provider or the organisation itself. PSPs are likely to assume the role as a TPSP without further licensing requirements.

The following scenario highlights the role of a TPSP processing a Direct Credit file for a direct submission.

Step 1 and 2
The payer creates a bulk Credit file and submits the file to the TPSP.

Step 2a and 2b
The TPSP initiates the Payment Assurance process (Step 2a) and confirmation details of the payee are received (Step 2b) prior to the TPSP submitting the bulk Credit file to the payer's PSP.

Step 3
The payer's account is debited.

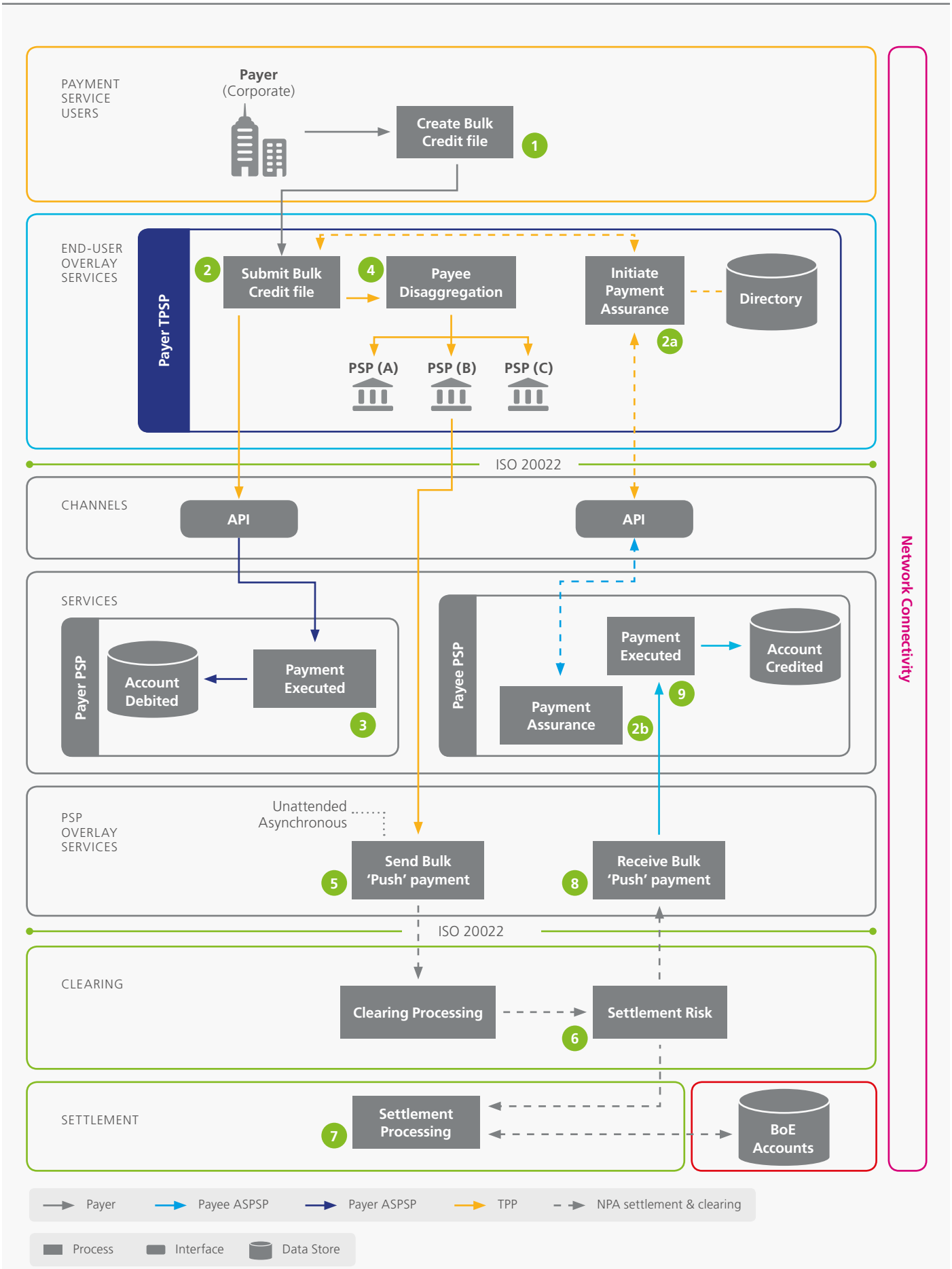
Steps 4
The TPSP disaggregates the bulk Credit file into separate files intended for each of the payee's PSPs.

Step 5 and 6
Cleared funds are 'pushed' to the Clearing and Settlement service and a settlement obligation is created between each PSP.

Step 7 and 8
The Clearing and Settlement service initiates settlement with the Bank of England (Step 7) and payment details are sent to each of the individual's PSPs (Step 8).

Step 9
The payee is credited with their payment.

FIGURE 8.3.3 DIRECT SUBMISSION



8.4 Appendix 4 – How will the NPA support the three End-User Solutions?

8.4.1 How will the NPA support Request to Pay?

The NPA will provide the architectural framework on which Request to Pay will be implemented as an overlay service. Common standards through APIs and messaging will be in place to ensure interoperability.

The Figure 8.4.1 provides an example[52] of a utility company requesting a bill payment from one of its customers. The payer chooses to make an electronic payment over the NPA through their TPSP.

In this example, the main steps involved are:

Step 1
The payee's billing system would initiate a Request to Pay (RtP) and pass this on with the appropriate information to the RtP Service provider.

Step 2
The payee's RtP provider generates a 'Request to Pay' instruction. The necessary data is populated. Recipient, Description, Amount, Reference ID etc. The provider would also look up the payer's RtP address from a directory.

Step 3
The payee's RtP provider sends the RtP to the payer's RtP provider.

Step 4
Upon receipt of the RtP, the payer would respond (Pay all, Partial pay, Request Contact etc.). The response would be sent back to the payee's RtP provider.

Step 5
If payer intends to make a payment (Full or Partial), a payment process would be initiated via their TPSP, who may also be their PSP.

Step 6
The payer's TPSP authenticates the payer and initiates the payment.

Step 7
The payer's PSP authorises the transaction.

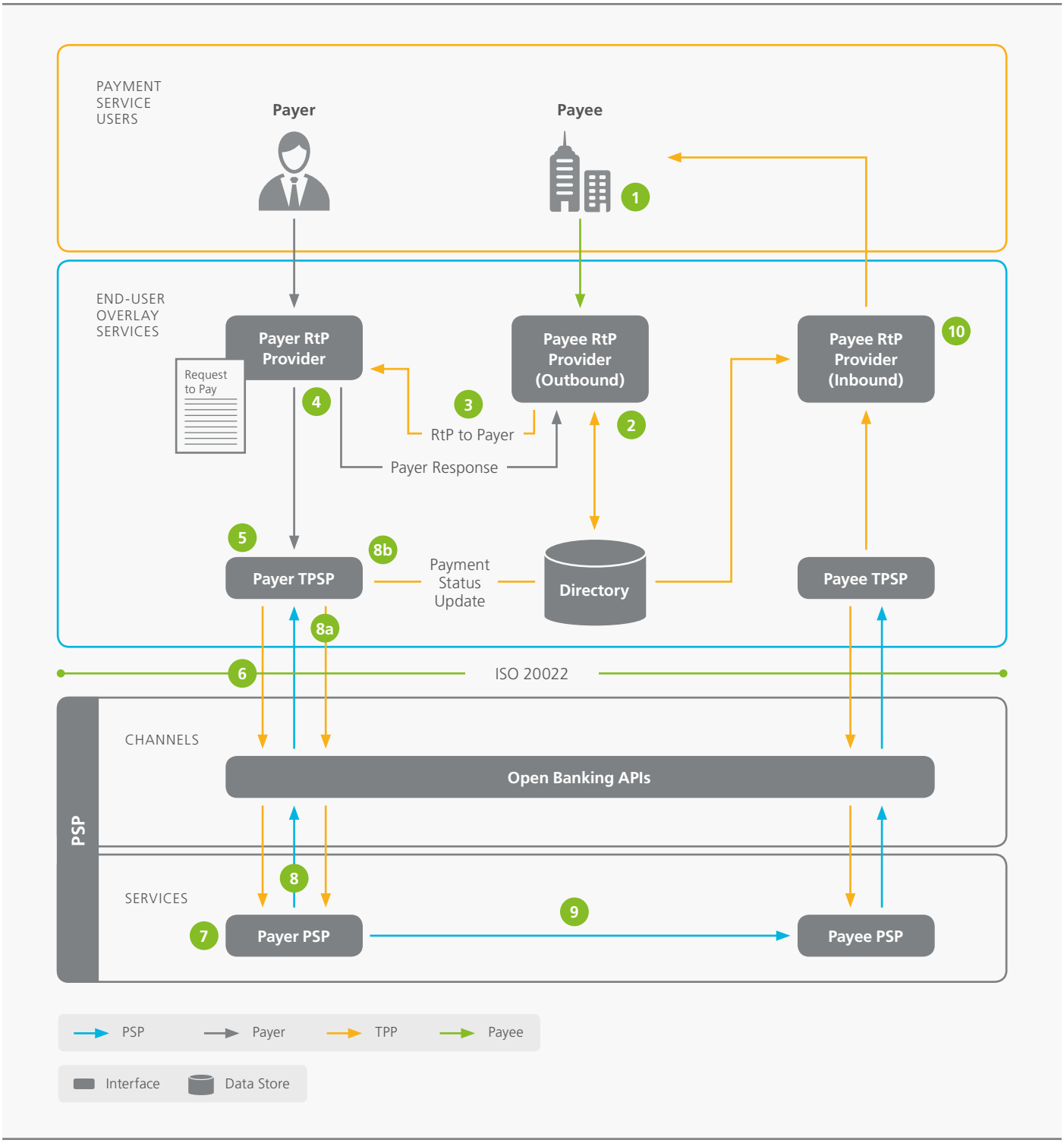
Step 8
The payer's TPSP receives the payment authorisation (via a token) from the payer's PSP and initiates payment (Step 8a). The payee would also be updated on the payment initiation outcome. (Step 8b).

Step 9
Funds are transferred to the payee's PSP.

Step 10
The payee's RtP provider updates the request status and passes this on to the payee.

[52] Please note that the following is just one example, and therefore, not the only way Request to Pay could be deployed on the NPA.

FIGURE 8.4.1 REQUEST TO PAY IN THE NPA



8.4.2 How will the NPA support Confirmation of Payee?

The NPA will be designed to provide an architectural framework, set of standards and APIs that will enable Confirmation of Payee (CoP) providers to interoperate.[53]

It is considered essential that all PSPs participating in CoP provide a near real-time CoP response to registered PSPs requesting payee information.

The figure below illustrates an example[54] where the payer is making a first time payment to a new payee with their bank account details that were received via a text. The payer wants to be sure that the details he received are correct and that the account actually belongs to the payee when he makes the payment. The payer is making an electronic payment over the NPA.

In this example, the main steps involved are:

Step 1
The payer provides the payee's account details.

Step 2
The payer's PSP looks up these details in a directory to determine the payee's PSP. The payer's PSP is then able to determine the correct API end point.

Step 3
The payer's PSP makes a Confirmation of Payee request to the payee's PSP CoP service through an API call.

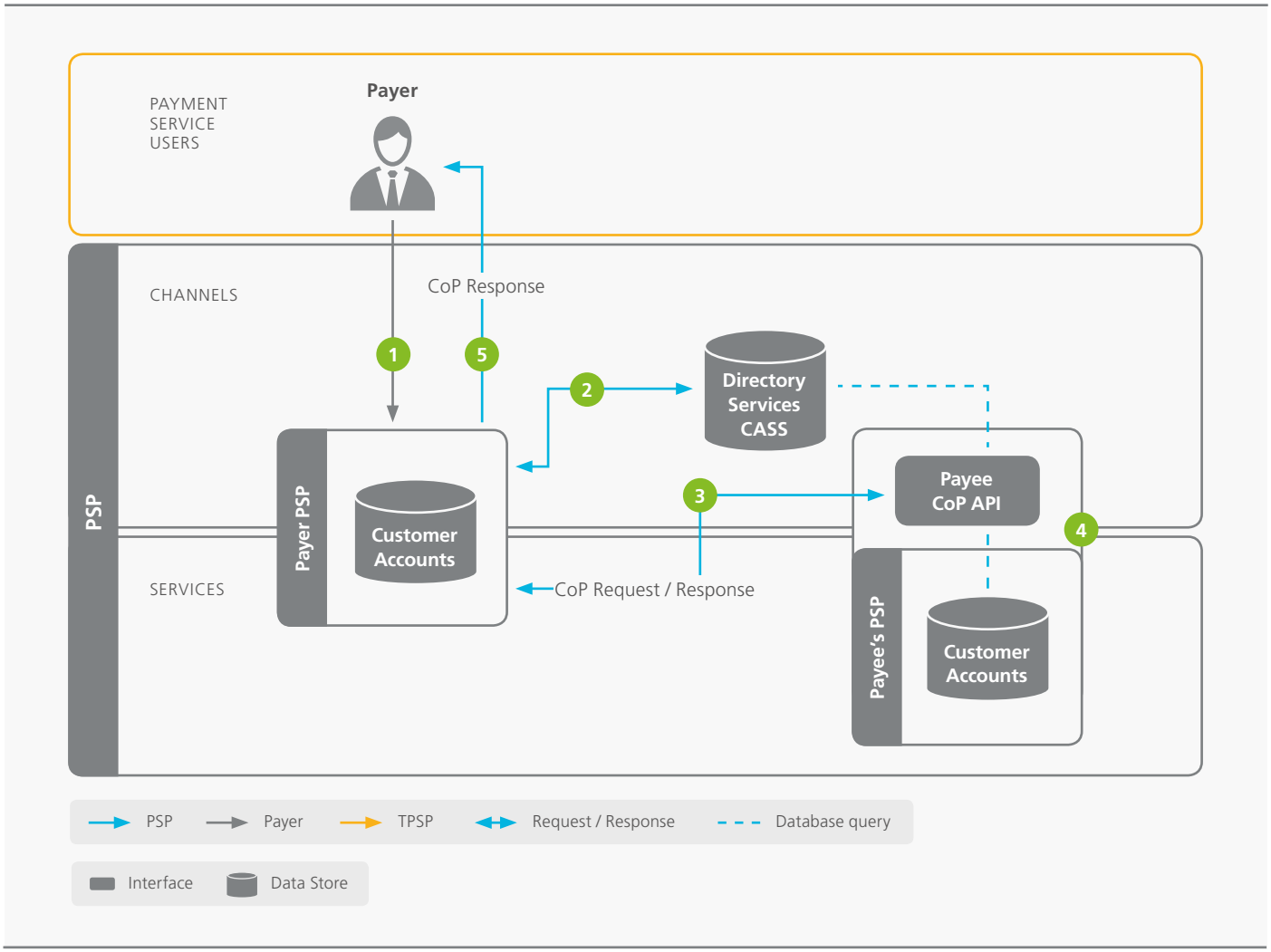
Step 4
The payee's PSP upon receipt of the CoP request, looks up the payee's details in its customer account store (Step 4a). The payee's PSP returns the CoP response back to the payer's PSP (Step 4b).

Step 5
The payer is presented with the response by their PSP. The user makes a decision based on the information provided.

[53] We support the work of PayM to deliver a 'Confirmation of Payee' capability on the current architecture, and we recognise the potential of this activity to inform the final design of the overall Assurance Data Solution in the NPA.

[54] Please note that the following is just one example (and therefore not the only way possible) of how Confirmation of Payee could work over NPA.

FIGURE 8.4.2 CONFIRMATION OF PAYEE IN THE NPA



8.4.3 How will the NPA support Payment status and tracking?

NPA will support two types of push payments: attended and unattended push payments. It will support provision of payment status messages to a customer's PSP / TPSP throughout the payments lifecycle.

Single immediate payments have the advantage of being processed in near real time resulting in immediate feedback. For unattended payments, status messages are not provided in real-time.[55]

The figure on the previous page illustrates a Single Immediate Payment.

In this example, the main steps involved are:

Step 1
Payment is initiated via Open Banking APIs through the payer's TPSP.

Step 2
The payer's PSP executes the payment request and payer's account is debited. Where the payment cannot be executed, a payment exception message will be returned to payer (Step 3a).

Step 3
The payer's PSP sends the payment details to the clearing and settlement service using a push payment and receives back an acknowledgement.

Step 4
The clearing and settlement risk management checks the PSP's risk position and creates a settlement obligation. The clearing and settlement service initiates settlement with the Bank of England (BoE).

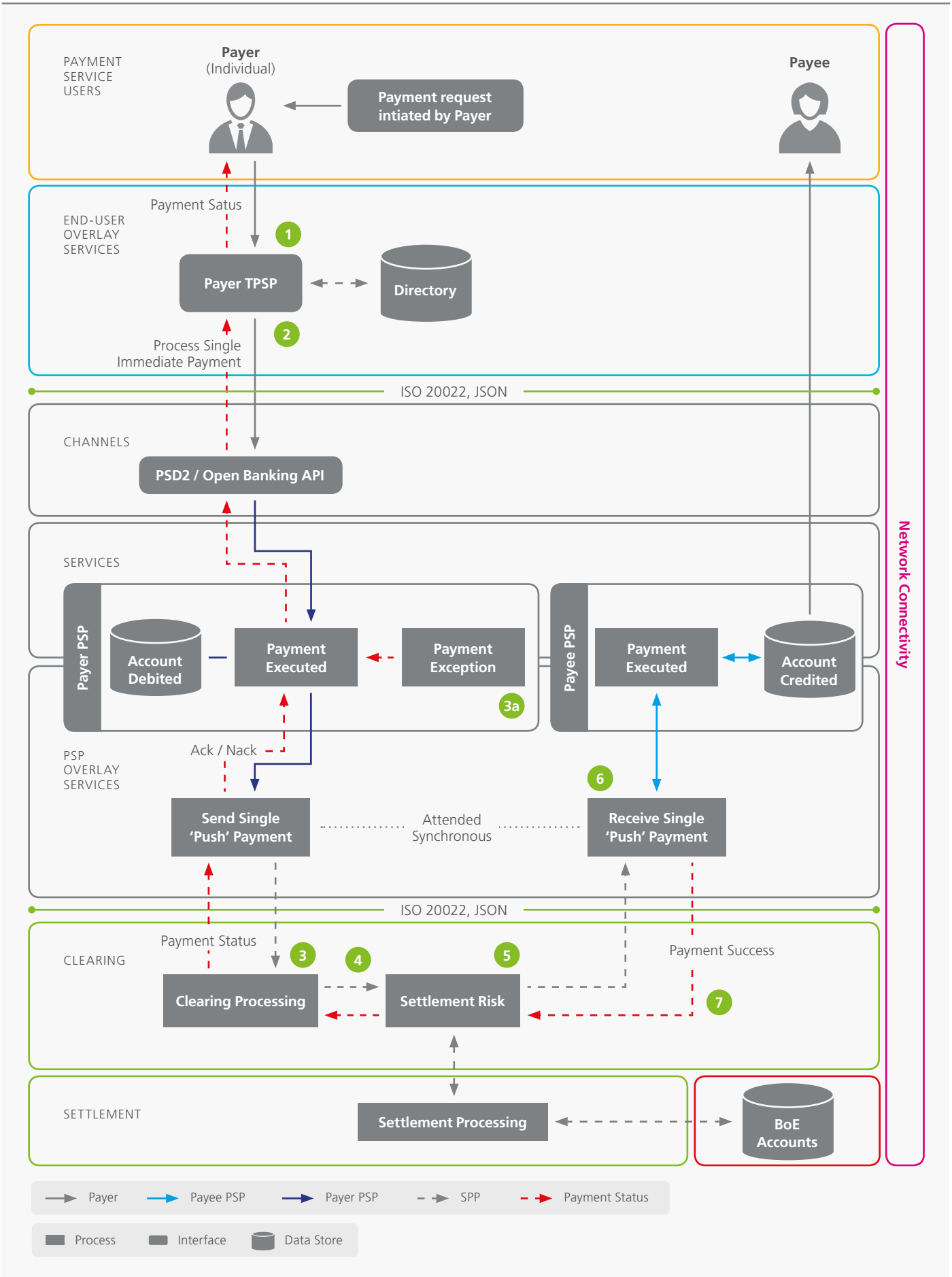
Step 5
The clearing and settlement service sends the cleared settlement payment details to the payee's PSP and simultaneously confirms the payment status. The payee's PSP, checks the account status and credits the payee's account.

Step 6
The payee's PSP confirms payment credited and provides the payment success status to the payer's PSP.

Step 7
The payer will be notified that the payment has been completed successfully via their TPSP.

[55] In the case of 2nd tier accounts the payer will be notified immediately once the payment is received in the collecting account. They will receive notification once the payment has been forwarded. This type of payment is expected to represent a fraction of the overall payments volume going through NPA.

FIGURE 8.4.3 PAYMENT STATUS AND TRACKING IN THE NPA



8.4.4 How will the NPA support Enhanced Data?

The New Payment Architecture will 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. This a key assumption in the delivery of Enhanced Data in the New Payments Architecture.

In this example implementation, the remittance information is stored external to the NPA.

TPSPs are expected to offer the storage service with each Enhanced Data item being identifiable in the external cloud through a unique identifier. The Payment message will contain the identifier (e.g. GUID, Document Ref, Token, and external cloud identifier) which will provide the link to the reference information stored externally. The directory will securely hold routing data allowing routing of the data from one point to the other.

Open Banking APIs will provide the interface through which this data is loaded or retrieved.

The main steps involved are:

Step 1
The payer's Enhanced Data TPSP receives payment instructions and Enhanced Data Unique Identifier from the payer.

Step 2
The payer's TPSP stores the Enhanced Data items and sends the payment instruction including the Enhanced Data Unique Identifier to the payer's payment initiation TPSP.

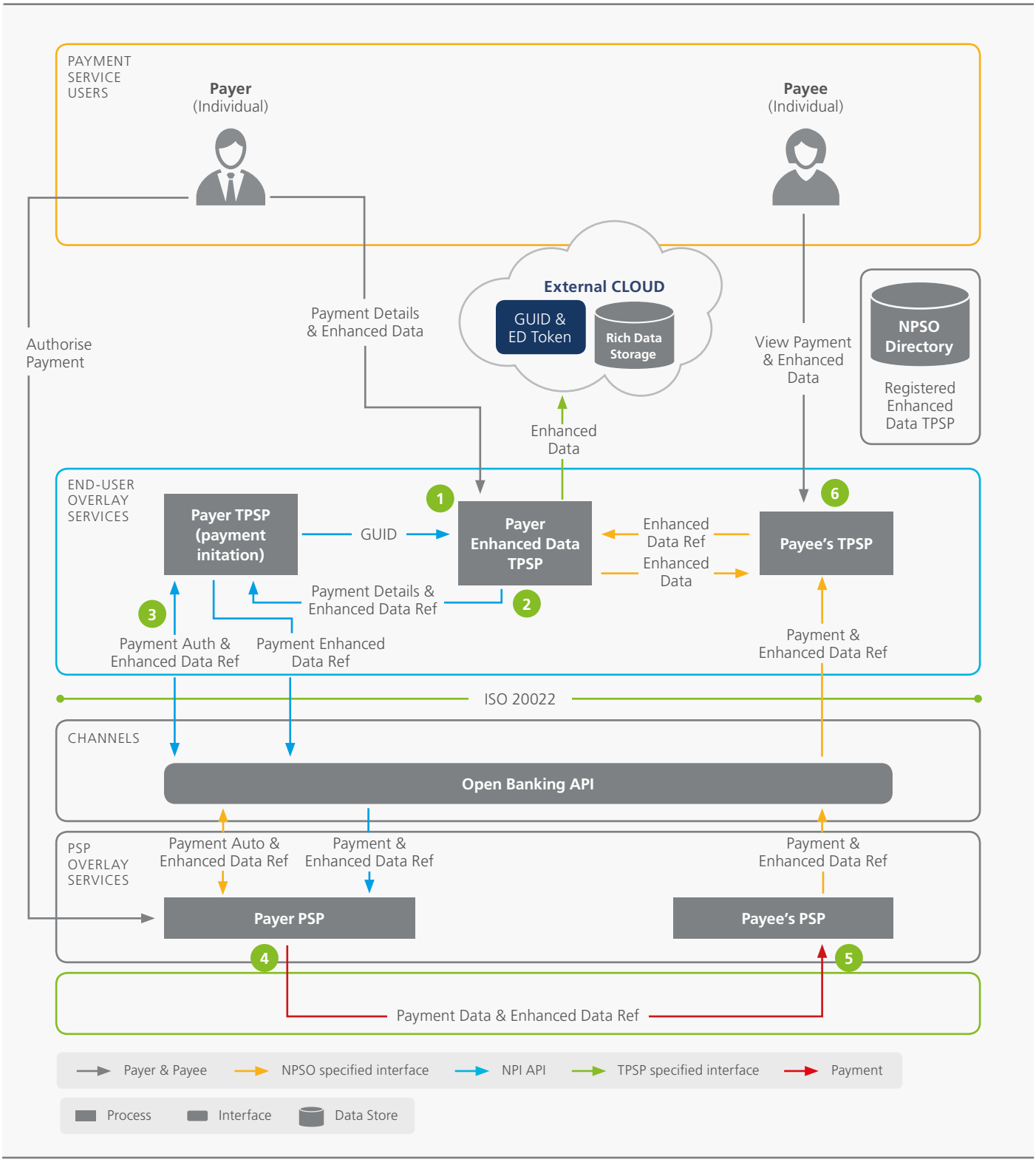
Step 3
The payer's TPSP (payment initiation) sends the payment details (including the Enhanced Data Unique Identifier details) to the payer's PSP.

Step 4
The payer's PSP creates and sends the payment (with the Enhanced Data Unique Identifier details) for clearing and settlement.

Step 5
The payee's PSP receives the cleared payment (with the Enhanced Data Unique Identifier details) and sends them to the payee's TPSP.

Step 6
The payee accesses the cleared payment and Enhanced Data via their TPSP, which looks up the location of the payer's Enhanced Data TPSP from the directory and retrieves the Enhanced Data.

FIGURE 8.4.4 ENHANCED DATA IN THE NPA



8.5 Appendix 5 – Implementation Plan and Transition States

8.5.1 Transition State and Period 1 – Single Payments Implementation

TABLE 8.5.1 TRANSITION STATE AND PERIOD 1

Overview: Transition Timeline for Period 1 – Q1 2021 to end Q2 2022	
All PSPs are capable of receiving Single Immediate Payments (SIPs): • Phase 1: Sending of new SIPs (phased). • Phase 2: Sending forward-dated payments.	
Prerequisites	
• Faster Payments, Bacs and ICS will be settling via the new RTGS. • The NPA clearing and settlement layers and prerequisite components for SIPs will be in place. • All PSPs will have obtained accreditation from the NPSO and will be ready to receive SIPs. • Overlay service providers (e.g. Confirmation of Payee / Request to Pay) have obtained accreditation from NPSO and solutions are in place.	
Payment Type	**Migration Status**
FPS	• SIPs begin migration to NPA including deferred payments e.g. standing orders and future dated payments.
Bacs	• No migration yet.
ICS	• No migration yet.
User Group	**Benefits / Changes**
Consumers	• When sending payments will be able to confirm payee, find out intended time of receipt and confirm receipt (Assurance data). • Will see more information when receiving payments and be able to include more information when sending (Enhanced data). • Greater flexibility when paying bills (Request to Pay).
Corporates	• SIPs. • Confirmation of Payee will save time and money by reducing misdirected payments and liability risks (Assurance Data). • Confirmation of receipt gives greater visibility (Assurance Data). • More efficient reconciliation (Enhanced Data).
Government	• SIPs. • Confirmation of Payee will save time and money by reducing misdirected payments and liability risks (Assurance Data). • Confirmation of receipt gives greater visibility (Assurance Data). • More efficient reconciliation (Enhanced Data).
PSPs	• Have obtained NPSO accreditation. • Be able to receive NPA SIPs from Day 1. • Begin sending SIPs via NPA. • Roll out enhancements to their own propositions to support the NPA end-user benefits.

8.5.2 Transition State and Period 2 – Bulk Payments Implementation

During Transition State 1, which covers SIPs, there may be a need to support a basic payment routing capability within the PSP's payment gateways to start the migration of sending payments in a managed way via the NPA. Since the NPA will require a larger set of data to deliver new end-user services than is supported by this solution, we propose that this transition solution option does not remains a core function of the NPA. It is expected that any routing capability would be provided by PSPs or other market led solutions.

TABLE 8.5.2 TRANSITION STATE AND PERIOD 2

Overview: Transition Timeline for Period 2 – Q3 2021 to end Q4 2022	
All PSPs are capable of receiving bulk payments: • Phase 1: Sending of bulk credit payments implemented (phased). • Phase 2: Sending payments with a persistent mandate (Direct Debits) – this will continue as an overlay service.	
Prerequisites	
• Components for bulk payment functionality (Bacs Direct Credits & Debits, Bacs Direct Submission and Faster Payments Direct Corporate Access) will need to be available. • All PSPs must be ready to be able to receive bulk payments.	
Payment Type	**Migration Status**
FPS	• DCA migration begins; SIP migration continues.
Bacs	• Direct Debit and Direct Credit migration; Direct Submitters also migrate.
ICS	• No migration yet.
User Group	**Benefits / Changes**
Consumers	• Will see more information when receiving business to consumer payments.
Corporates	Bulk payments: • Confirmation of Payee will save time and money by reducing misdirected payments and liability risks (Assurance Data). • Confirmation of receipt gives greater visibility (Assurance Data). • More efficient reconciliation (Enhanced Data). • Direct submitters will need to make changes to enable the migration to NPA. • Improved cash flow through faster clearing for bulk payments.
Government	Bulk payments: • Confirmation of Payee will save time & money by reducing misdirected payments and liability risks (Assurance Data). • Confirmation of receipt gives greater visibility (Assurance Data). • More efficient reconciliation (Enhanced Data). • Will need to make changes to enable the migration to NPA.
PSPs	• All PSPs must be able to receive bulk payments. • Bacs volumes will migrate. • FPS migration will complete during this period enabling the close down of legacy FPS systems.

In Transition State 2, corporates, PSPs and government departments who submit work directly will be required to migrate to NPA. Under the proposed approach, the direct submitters will not be required to change their existing file format. These files will be sent to a third party processor (similar to sending them via Bacstel IP or DCA) who will complete the pre-processing for example, disaggregating the file, changing the format to ISO 20022 etc., before submitting the file to the NPA for Direct Credits or to the Payers TPSP for Direct Debits.

The direct submitters have the opportunity to adopt the ISO 20022 file format in order to provide additional information, i.e. Enhanced Data that is not supported in the current file format. Adoption of the ISO 20022 file format could be implemented at any time during or after the transition period. Similarly, there is no requirement to change the existing Direct Debit mandates during the transition period. Adopting a new Direct Debit Mandate approach for Payer verification could be implemented at any time during or after the transition period.

8.5.4 Transition State and Period 3 – Image Clearing Implementation

TABLE 8.5.3 TRANSITION STATE AND PERIOD 3

Overview: Transition Timeline for Period 3 – Q1 2024 to end Q4 2024	
All PSPs are capable of receiving: • Phase 1: Processing of credits (Bank Giro Credits). • Phase 2: Processing of cheques.	
Prerequisites	
• Components will be in place for Image Clearing. • All Paying PSPs will need to be able support NPA image clearing.	
Payment Type	**Migration Status**
FPS	• FPS migration now complete.
Bacs	• Bacs migration now complete.
ICS	• ICS migration begins.
User Group	**Benefits / Changes**
Consumers	• No additional expected benefits or changes outside the prevailing proposition.
Corporates	• No additional expected benefits or changes outside the prevailing proposition.
Government	• No additional expected benefits or changes outside the prevailing proposition.
PSPs	• Migration of ICS volume leading to the wider NPA cost benefits.

8.5.4 Transition State and Period 4 – Close down

Transition Timeline for Period 4: Q2 2022 to end Q4 2024

By the end of Transition Period 4 all legacy volume will have migrated to the NPA and legacy infrastructure will have been closed down. All users will be able to receive the full benefits of NPA from this point.

8.6 Appendix 6 – Cost Benefit Analysis

8.6.1 Methodology and Approach

Approach Overview

The CBA framework has been developed based on the perspective of five groups of participants in the payment process. These participants include: end-users (i.e. consumers, businesses and government), PSPs, Payment System Operators (PSOs), Infrastructure Providers and Aggregators.

Our approach to the CBA modelling involved:

- Estimating the current costs of the interbank payments system i.e. FPS, ICS and Bacs.
- Estimating the costs and benefits of the NPA.
- Estimating the costs and benefits of the overlay services.
- Estimating the parallel running costs.
- Estimating the costs and benefits of the alternative minimum upgrade.

Modelling Parameters

Social Time Preference Rate:

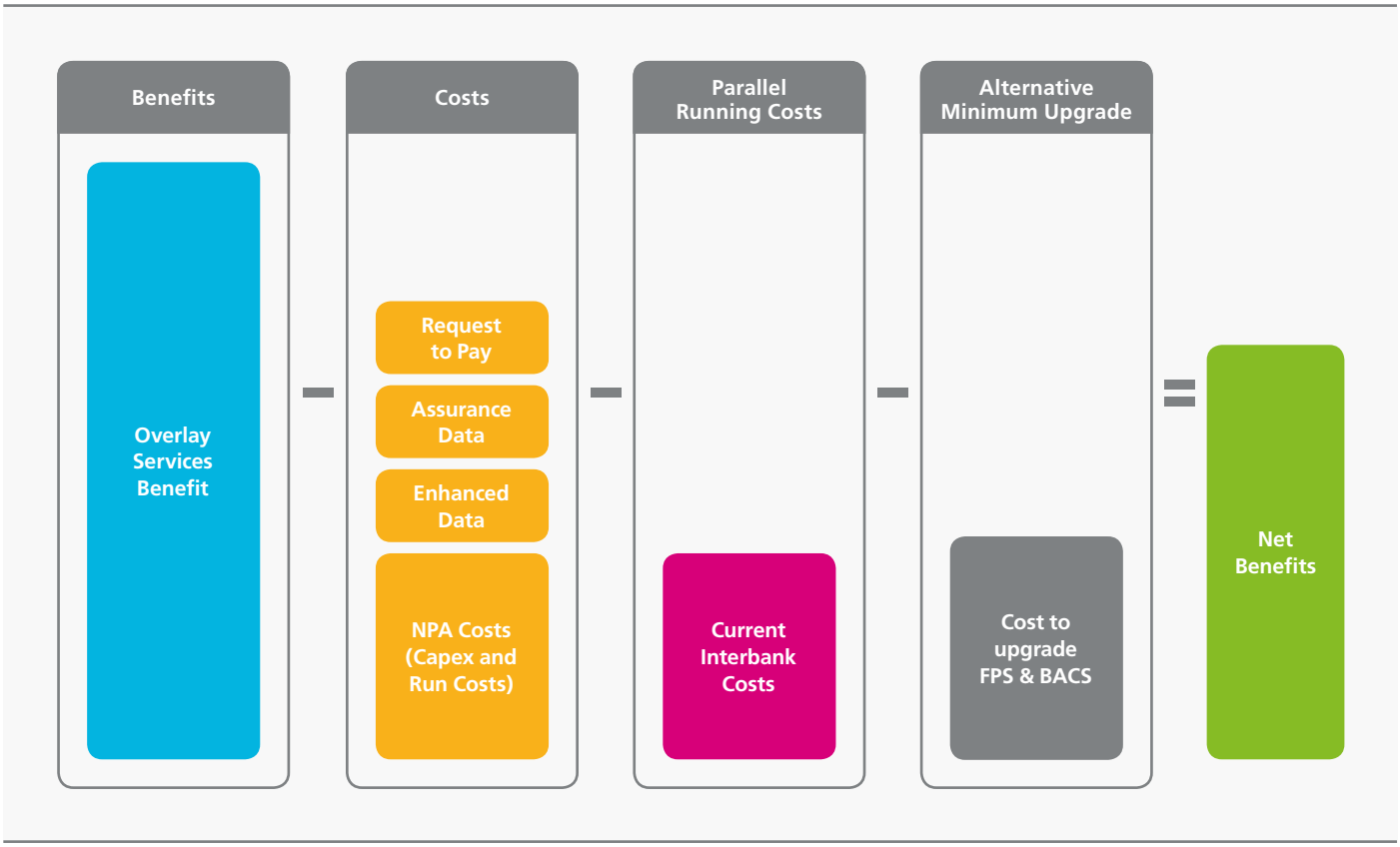
Social Time Preference is defined as the value society attaches to present, as opposed to future, consumption. The Social Time Preference Rate (STPR) is a rate used for discounting future benefits and costs, and is based on comparisons of utility across different points in time or different generations.[56]

The HM Treasury Green book recommends that a 3.5% STPR be used as the standard real discount rate.

Inflation:

In this CBA, we have ignored the impact of inflation because the prediction of future prices introduces unnecessary uncertainty into the analysis. This conforms to best practice guidelines as set out in the HM Treasury Green Book where it stipulates that benefits and costs should be expressed at today's price level.

FIGURE 8.6.1 CBA OVERVIEW



[56] The Green Book – Appraisal and Evaluation in Central Government.

Supporting Information

Our analysis builds on evidence in the work undertaken stratgey and is based from the findings of two main evidence gathering processes: desk based research and a stakeholder engagement programme across the payments industry.

We invited the following types of stakeholders for discussions: PSPs of all sizes; Payment Service Users (PSUs), including large and small corporates and public sector organisations; PSOs; infrastructure providers and aggregators and; FinTech companies.

Analysis

The main purpose of the CBA is to use the cash flow forecasts attributable to the NPA to calculate suitable net return indicators i.e. the Net Present Value (NPV). We have used the incremental Discounted Cash Flow (DCF) approach. This implies an assumption that only cash inflows and outflows are considered.

8.6.2 NPA Benefit Narratives and Estimates

Benefits 1-7 set out below are derived from the steps in the Request to Pay and Enhanced Data end-to-end journeys (refer to Section 2.2 and 2.4 respectively for a detailed illustration of the end-to-end journeys). Benefit 8 refers to the Confirmation of Payee end-to-end journey (refer to Section 2.3).

Benefit 1: Auto-reconciliation could reduce payees' manual and invoice reconciliation costs.

The capability to add more characters or information in a remittance message provides possibilities for e-invoicing to expand.

Currently, due to the limited number of characters that can travel with a payment message, most remittance information must travel separately from the basic payment details, e.g., via accompanying post or email, thereby requiring a costly manual intervention to process and reconcile payments.

E-invoicing enables businesses to automate their invoice reconciliation processes. We use the 5.5 billion electronic individual C2B and B2B payments made annually[57] as a proxy for the annual number of invoices that could benefit from the implementation of auto-reconciliation solutions.

As with other benefits, we exclude small and microbusinesses due to assumption that their operations are not large enough in scale to invest in the solutions required to realise this benefit. These businesses generate 33% of annual UK business turnover.

It is currently estimated to cost SMEs £2.90 and large businesses £1.58[58] per unit to manually reconcile invoices sent separately from the payment message. This cost is assumed to reduce by 40% if auto reconciliation solutions are adopted by medium and large businesses. This 40% reduction estimate is the average of estimates in the relevant literature we have reviewed.[59]

We estimate that over a ten-year implementation period, the take-up of this solution by businesses would be up to 30%, i.e. up to 30% of the volume of relevant electronic payments would allow the use of auto-reconciliation solutions.

Consequently, these businesses could save between £3.7 billion and £4.5 billion in discounted invoice reconciliation costs over the period 2019-2031.

Benefit 2: The solution would help reduce losses associated with invoice fraud.

According to research by Tungsten Network quoted by Experian[60], SMEs are losing more than £9 billion in invoice fraud every year. As automated credit represents 17% of the volume of payments made annually in the UK, we assume the same proportion of invoice fraud is addressable through Confirmation of Payee, i.e. £1.5 billion annually.

Subject to efficient KYC processes, each consumer using Confirmation of Payee when making an electronic payment could reduce the risk of invoice fraud affecting him / her by up to 100%.

We estimate that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of the value of relevant C2B, B2B and C2C electronic payments.

Overall, according to estimates of this study this benefit could generate cumulative discounted savings between £1.3 billion and £1.6 billion in reduced invoice fraud during the period 2019-2031.

Benefit 3: The solution would reduce average unit cost of producing and sending invoices for businesses.

The replacement of paper invoices by electronic invoices is already underway. Request to Pay should help accelerate this process, thereby driving down the cost of producing and sending paper invoices.

18.9 billion[61] non-cash B2B and C2B payments were made in the UK in 2014 and we take this number as a proxy for the number of relevant invoices produced annually in the UK. As with other benefits, we exclude small and microbusinesses due to assumption that their operations are not large enough in scale to invest in the solutions required to realise this benefit. Therefore only 67% of these invoices, i.e. 12.7 billion, are considered.

The cost of producing and sending an invoice is estimated to be £0.26 for a large business and £0.85 for a small business.[62] As large businesses represent 53% of UK turnover and medium businesses 14%, the average cost for producing and sending an invoice for the relevant businesses is £0.38 per unit.

[57] The total of C2B and B2B electronic payments (excluding cash, cheques, debit and credit cards) is 5.5bn. The total annual number of non-cash C2B and B2B payments is 18.9bn. Source: Payments UK, 2015.
[58] Source: Accenture, the Economics of Request for Payment, 2017.
[59] Sources: AP Automation Survey, Institute of Financial Operations, 2015 and The True Cost of Invoicing and Payments, 2002, Fidesic Corp. These studies forecast respective 37% and 43% cost reductions due to automated invoice reconciliation.
[60] http://www.experian.co.uk/blogs/latest-thinking/smes-losing-9bn-invoice-fraud/
[61] Source: Payments UK.
[62] Accenture, The Economics of Request for Payment, 2017.

Studies have shown that using Request to Pay as a form of electronic invoice could reduce this cost by 21%.[63]

We estimate that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of medium and large business invoices will be subject to the use of this solution.

Our analysis shows that adoption of Request to Pay could generate discounted cost savings due to a replacement of paper invoices of between £850 million and £1 billion during the period considered.

Benefit 4: Improvement in liquidity and subsequent reduction in financing costs.

The use of Request to Pay could help medium and large business payees improve liquidity via quicker debt collection with the potential impact of a reduction in financing costs.

Adoption of Request to Pay could reduce the current lead time in interacting with business customers. The assumption of this study is that customers who receive automated, instantaneous electronic requests rather than non-electronic requests are likely to settle debts quicker. Improvement in debt recovery will help liquidity (via a reduction in debtor days). As a result, businesses should see improvement in their liquidity and this will decrease the need for them to rely on credit facilities.

Average debtor days for UK businesses was estimated at 52 days in 2016. Total late payment debt owed to businesses represented £31 billion.[64] In order to be conservative, we exclude small and micro businesses from this analysis hence only 67% of this debt is considered, which represents £21 billion. The assumed interest rate for a credit facility is 5% over the base rate, i.e. 5.25%.

This analysis assumes that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of business transactions carried out by medium and large businesses will be subject to the use of this solution.

If Request to Pay reduces average debtors' days by around 5% i.e. 2.6 days, this would mean businesses could save between £550 million and £670 million in discounted financing costs during the period 2019-2031.

Benefit 5: Request to Pay is cheaper for businesses than re-presentation of a failed Direct Debit ('DD').

A Request to Pay can be triggered after the failure of a DD (due to insufficient funds on the account or cancellation by the payer). Currently, the first step taken by payees is to re-present the DD to the payer. This costly re-presentation process (a sample of utilities estimate this at £15 to £20 per failed transaction) could be replaced by Request to Pay notifications, that could cost up to 75% less.[65]

1.8% of Direct Debit transactions fail annually.[66] Excluding those that can be attributed to micro- and small businesses, we assume there are 47 million addressable Direct Debit representations annually.[67]

We estimate that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of Direct Debit failures would be handled with automated Requests to Pay.

Our study shows that these discounted cost savings could reach between £460 million and £560 million in the period considered.

Benefit 6: The solution would help reduce the losses to payers associated with misdirected payments.

The total value of misdirected payments was estimated at around £2.5 billion,[68] 20% of which is never recovered,[69] which would represent a net loss of £500 million to customer or business payers who have made these errors when sending electronic payments.

The adoption of Confirmation of Payee would reduce the risk of misdirected payments, as the payer would be able to check automatically whether the account that is about to be credited is the right one, thereby reducing losses associated with these errors.

We estimate that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of the value of relevant C2B, B2B, and C2C electronic payments would be subjected to a Confirmation of Payee and hence these payments are unlikely to be misdirected.

Based on these assumptions, this benefit could generate between £420 million and £515 million in discounted reduced losses to payers during the period 2019-2031.

Benefit 7: Request to Pay will make late payment processing for customers cheaper for businesses.

Total late payment debt owed to businesses represented £31bn[70] in 2014. We assume that total late payment debt potentially impacted by Request to Pay would represent £21bn.[71]

The current late payment chasing process for customers generally involves phone calls and letters. Sometimes, businesses have to pass the late payment cases to debt recovery agencies or factor certain invoices at a discount for cash.

Overall, Request to Pay could be cheaper (per case) than the current process as it would primarily rely on automated electronic interactions between payer and payee rather than the more expensive non-electronic means (a utility company estimates that one single reminder letter costs £0.38 and this may not even reach the customer who may have moved out).

[63] Accenture, The Economics of Request for Payment, 2017.

[64] Bacs research.

[65] Current chasing cost per late £1 is £0.35 (source: http://www.business-money.com/announcements/late-payments-costing-smes-billions). Excluding assumed debt collection agencies costs (£700 million turnover in 2009, source: Experian), this cost is £0.31. We then assume that replacing the current typical chasing process by two business text messages for any late £1 would amount to £0.07, i.e. a 77.4% saving (rounded downwards to 75%).

[66] Source: Bacs.

[67] There are 3.9 billion Direct Debit transactions annually. 33% of them are excluded from the analysis as they are associated with micro- and small businesses' activity.

[68] £2.5bn lost annually in misdirected payments and average FPS payment of £820. Source: Payments UK, quoted by the Daily Telegraph http://www.telegraph.co.uk/finance personalfinance/bank-accounts/11798573/The-pitfall-lurking-in-your-online-banking-that-sets-up-strangers-as-approved-payees.html

[69] Based on estimates provided by banking stakeholders.

[70] Including debt owed to micro- and small businesses who represent 33% of UK turnover and are being excluded from this analysis due to cost implications.

[71] Excluding the assumed share of debt owed to small and micro-businesses and debt associated with DD failures (which is the object of benefit 4). £22bn worth of regular payments were made by Direct Debit in 2014. Assuming a 1.8% DD failure rate, we therefore exclude a further c. £396 million of late payment debt from the scope of our analysis.

We estimate that up to 246 million[72] late debt reminders send by post each year could be sent through electronic means instead. As a result, depending on adoption, businesses could therefore save on administrative costs to chase late payments.

We estimate that over a ten-year implementation period, the take-up of this solution by businesses (particularly utility companies) will be up to 18%, i.e. up to 18% of medium and large companies' invoices will be subject to the use of this solution.

According to estimates of this study, these businesses could save between £80 million and £100 million in discounted payment processing costs during the period 2019-2031.

Benefit 8: The use of Confirmation of Payee by payers would help reduce the number of misdirected payments and thereby reduce their administrative costs to PSPs.

We have estimated there were 3 million instances of misdirected payments annually,[73] at an average handling cost of £17.50 per incident for PSPs.[74]

The adoption of Confirmation of Payee would reduce the risk of misdirected payments, as the payer would be able to check automatically whether the account he is about to send money to is the right one. The number of such incidents handled by PSPs would therefore be reduced.

We estimate that over a ten-year period, the take-up of this solution by end-users will be up to 18%, i.e. up to 18% of the value of relevant C2B, B2B, and C2C electronic payments would be subjected to a Confirmation of Payee.

Based on these assumptions, this benefit could generate between £45 million and £55 million in saved administrative costs for PSPs during the period 2019-2031.

8.6.3 Estimating the Benefits of Bacs, FPS and ICS

We have conservatively assumed the benefit of the Bacs, FPS and ICS services are equal to the current operating costs of these services. This is based on the assumption that Bacs, FPS and ICS as they are currently being run, generate benefits that are equal to the costs that participants in the current UK payments system pay to run them. We have replicated this assumption for the alternative minimum upgrade benefits.

Calculation

Annual run costs per annum are £480m. Therefore aggregating the discounted annual figure across the relevant period will produce an estimate of the benefits of the current interbank payment systems infrastructure (FPS, Bacs, ICS) as per our assumptions.

8.6.4 Comparison of the NPA to the Aternative Minimum Upgrade

TABLE 8.6.1 NPA AND ALTERNATIVE MINIMUM UPGRADE COMPARISON

Overlay Service	NPA	Alternative Minimum Upgrade
	Discounted (2019-2031)	Discounted (2019-2031)
Existing FPS / Bacs / ICS Benefits (assumption)	£4.04bn – £4.94bn	£4.04bn – £4.96bn
Overlay Services Benefits	£7.41bn – £9.06bn	N/A
Total Benefits	**£11.45bn – £14bn**	**£4.04bn – £4.94bn**
Total Costs (excluding EUN)[75]	£4.47bn – £5.47bn	£4.28bn – £5.23bn
Overlay Services Costs	£0.93bn – £1.13bn	N/A
Total Costs (including EUN)	£5.40bn – £6.60bn	£4.28bn – £5.23bn
Net Benefits	**£6.05bn – £7.40bn**	**(£0.24bn) – (£0.29bn)**

[72] Of the £20.5bn non-DD late debt owed to medium and large businesses, debt attributable to C2B invoices is estimated to be £9.8 billion annually, which we divide by the average monthly consumer utility bill (£41, source: https://www.ovoenergy.com/guides/energy-guides/the-average-gas-bill-average-electricity-bill-compared.html, back-calculated based on the annual energy bill). Non-DD late debt attributable to B2B invoices is estimated to be £10.6 billion, which we divide by the average business utility bill (£2,528, http://www.businessenergy.com/electricity). Overall this leads to a potentially addressable sample of late payment reminders of 246 million annually.

[73] £2.5bn lost annually in misdirected payments and average FPS payment of £820. Source: Payments UK, quoted by the Daily Telegraph http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/11798573/The-pitfall-lurking-in-your-online-banking-that-sets-up-strangers-as-approved-payees.html.

[74] Information provided by one of our PSP stakeholders.

[75] While the costs for the NPA and the alternative minimum upgrade look similar, there are a number of differences in the components that make up the costs. These include, efficiency savings associated with merging schemes, differences in the assumptions regarding parallel running costs and differences in assumptions regarding non central infrastructure costs.

8.6.5 Adoption assumptions for overlay services

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

TABLE 8.6.2 LEVEL OF ADOPTION ASSUMPTIONS BY END-USERS FOR EUN SOLUTIONS

Services	Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9	Y10
Request to Pay	3.1%	3.8%	4.6%	5.6%	6.8%	8.3%	10.1%	12.3%	15.0%	18.3%
Assurance Data	3.1%	3.8%	4.6%	5.6%	6.8%	8.3%	10.1%	12.3%	15.0%	18.3%
Enhanced Data	5.0%	6.1%	7.4%	9.0%	11.0%	13.4%	16.3%	19.9%	24.2%	31.0%

8.7 Appendix 7 – NPA Commercial Approach and Economic Models

8.7.1 Current State: Payments Landscape and Funding Arrangements

The current UK payments architecture consists of PSOs operating services used by PSPs, aggregators and end-users. The three PSOs within scope to be consolidated in the NPSO represent a variety of different governance models, operating structures and funding arrangements.

Bacs Payment Schemes Ltd (BPSL), Faster Payments Scheme Limited (FPSL) and Cheque and Credit Clearing Company Ltd (C&CCCL) operate on a not-for-profit basis by setting prices / tariffs to participants to cover their annual operating and development costs.

In the past, the PSOs have been funded directly by PSPs through upfront funding calls to finance the initial design and build stages or by vendor financing.

Currently, the three PSOs depend on their participants for funding through a combination of transaction-based fees and, for some PSOs, calls on members. Calculation of the relevant fees for each participant / member varies and depends on a few factors, such as volume and profile of transactions.

Central infrastructure providers are the main suppliers to the PSOs. The PSOs act as single procurers on behalf of their participants to source core services from infrastructure providers.

The system and services procured by the PSOs typically involves high fixed costs for set-up which must be recovered over a certain time period. Therefore, usage volumes need to be guaranteed in advance so that the commercial risk for the vendor is contained.

The balance between the cost, risk and technology capability associated with the provision of these services is a key consideration of the framework outlined in this paper. They constitute some of the 'deal levers' which can be used to increase competition, accessibility and efficiency in the market.

8.7.2 Current State: International Sector Comparison

The payments industry is changing globally and multiple countries including the UK are responding to new user needs and technology changes.

For many years clearing and settlement services have been delivered via central shared infrastructures – typically one single system for each type of payment services. In spite of technological developments in distributed systems, this generally remains the case today. Singapore's real time payments service and planned new payments services in Canada, USA and Australia are maintaining this approach. Even in the limited markets that permit multiple provision (e.g. SEPA), market forces have tended to deliver single solutions, i.e. SCT and SCT Inst cross-border solutions from EBA Clearing.

However, consistent with the NPA, others are starting to focus on fostering competition in overlay services e.g. The Australian New Payments Platform.

8.7.3 Funding Stakeholders

Vendors

Vendors enter into a managed-service contractual agreement with the NPSO to design, build and operate a service according to upfront agreed SLAs and rules in a vendor finance model.

Vendors are motivated by the prospect of entering into a financing agreement granting strategic access to the UK payments market, and gaining market share over competitors.

Vendors can fund the proposition over its full lifecycle from inception to its fully scaled state. Therefore, we expect vendors to take a longer-term view as to the pay-back period and overall return due to their potentially lower cost of capital than for example, financial investors.

The NPSO may consider that vendor financing for central infrastructure elements is suitable only for large players since others may lack the capital and skills to deliver large scale solutions. Smaller vendors will be encouraged to participate in the NPA and may bid in consortia to deliver larger scale solutions. The 'sandbox' may provide a useful environment within which to incubate new vendors.

A risk the NPSO faces with vendor financing is that vendors may reuse existing technology rather than providing best in class solutions once they have won the contract. The NPSO must consider appropriate arrangements to mitigate these issues, such as SLAs. Should the NPSO wish to take more ownership of the NPA's intellectual property this could have an impact on vendor financing.

Financial Investors

Financial investors can finance the creation of a market solution directly for the NPSO or for vendor(s). We anticipate their investment motivations to be driven mainly by maximising value from their investment. They are mostly interested in the prospect of business growth, with an ultimate objective of provisioning a sound business model to maximise value upon exit in a timeline of three to seven years. They will place emphasis upon the strength of the management team, achievability of the business plan and associated risks to deliver their required returns.

There are varying appetites for financial risk depending on the stage of the investment lifecycle and the type of investor. Table 8.7.1 details the investment size differences between investor type, their return requirements and maturity of businesses they invest into. Early stage and venture capital (VC) investors are most likely to finance the design and build stage.

Private equity and infrastructure investors are more likely to invest in established businesses that generate positive cash flows. Due to a perceived lower risk they look to invest larger amounts of money for a longer period of time.

On the other hand, debt funds have different risk appetite and investment requirements than equity investors. Debt investors are looking for a fixed return and are unable to take equity risk. Therefore, they only consider investing into established cash flow generative and repeat revenue businesses.

The NPSO should consider the exit process when provisioning investment from financial investors. For example, sale processes must be run as wide auctions to ensure no preferential follow-on treatment is granted through investor choice.

Furthermore, the public perception of private capital and the potential large returns achieved should also be considered. The relationship between financial investors and the vendors providing solutions should be clearly defined with the NPSO's objectives in mind.

TABLE 8.7.1 ILLUSTRATIVE INVESTOR PROFILES

Investor Type		Bussiness Stage	Rates of Returns	Invest. Term	Approx. Quantum
Early Stage		Start-up, seed, early development	50-70%	1-3 years	Up to £5m
Venture Capital		Growth and expansion	40-60%	5-10 years	£5m to £10m
Private Equity		Established, scaling, cash generative	20-30%	3-5 years	From £20m to over £1bn
Infrastructure		Fully scaled, cash generative	10-15%	10-20 years	From £500m
Debt	Senior Debt	Fully scaled, cash generative	3-5%	3-5 years	Up to £25m
	Unitranche		5-8%	5-6 years	£25m+
	Mezzanine		10-15%	3-5 years	£10m+

Retail investors (Crowdfunding)

Another funding source is crowdfunding which has been gaining strong traction in recent years across various sectors. People invest through crowdfunding platforms to test new products, identify new investments and be at the forefront of innovation.

The benefit of using crowdfunding is the opportunity to either raise funds against equity or pre-pay for a product delivered in future. Crowdfunding, unlike other funding sources, provides a fundraising campaign targeted at end-users (customers).

Crowdfunding requires strong in-house marketing and public relations capability in order to build a successful campaign. Due to the customer-centricity, overlay services might be more suitable for funding than non-customer centric solutions, e.g. clearing.

Other Market Participants

Since the NPA will work to benefit the broader payments ecosystem and stakeholder community, the PSO DG report suggests that there may be instances when market participants (such as PSPs, FinTechs, industry bodies etc.) propose beneficial changes to the solutions or design. In these cases, the market participant(s) would fund the NPSO effort to amend the standards and deliver change.

The risk in this model is that incumbent market participants are more likely to be in a position to propose and pay for changes which are advantageous to them. In this case, the NPSO would have to ensure that any proposed alterations would not work to the detriment of other market participants by limiting competition or access to payment services and systems. These kinds of funding arrangements must not be used to negotiate changes to make the governance structure less independent.

NPSO

The NPSO could invest in developing an element from its R&I budget. There may be instances where the NPSO may choose to fund certain NPA elements beyond the R&I development threshold which would require an additional funding source.

In this case, the NPSO secures finance and offers a build and operate contract to a vendor. It may therefore need skill sets to enable this.

The NPSO should be aware of the risks of the funding of 'NPSO procured' solutions and avoid instances where it would act as a driver of a monopolist market. It must not stifle competition or innovation in overlay services.

8.8 Appendix 8 – Financial Crime Solutions Update

8.8.1 Overview

Five of our Financial Crime solutions are progressing to handover and therefore have not been included in this Consultation document. For completeness, this section provides an update on these solutions:

- **Liability Models for Indirect Access:** Following our work on Simplified Access in 2016 we identified the need for more information from the payments community. We have developed two questionnaires that have been distributed to different stakeholders in the payments community to understand the range of views across the industry on risk liability between indirect Payment Service Providers (PSPs) and the banks / FIs who provide them with account services and access to payment systems.
- **Guidelines for Identity Verification, Authentication and Risk Assessment:** We have carried forward the position outlined in our Strategy to develop the design and implementation of comprehensive identity-related risk management guidelines for PSPs.
- **Customer Education and Awareness:** A current state analysis of customer education and awareness initiatives for financial crime has been carried out and the Forum's view is that the industry should strongly support and engage in the current programme. The Forum requested that particular consideration be given to the fast-changing nature of some fraud types, and that the industry seek to collaborate extensively to be more cost effective in educating society.
- **Financial Crime Data and Information Sharing:** Formerly the Financial Crime Intelligence Sharing solution, we have further developed our position on enhancing the sharing of financial crime data and information both within the payments community and with law enforcement agencies.
- **Enhancement of Sanctions Data Quality:** An action has progressed with HM Treasury identifying measures that could be used to enhance current sanctions list entries.

The activities of each solution are outlined in further detail below.[76]

8.8.2 Liability Models for Indirect Access

Our Strategy highlighted the need for greater clarity regarding financial crime risk liability between indirect PSPs and the banks / FIs who provide them with account services and access to payment systems.

We aim to gather a broad cross section of views on the issues faced by indirect PSPs to obtain bank account services and access to payment systems via providers (generally banks). We are now seeking to collect the views of the industry through targeted questionnaires.

We issued our questionnaires on 3rd July 2017 with responses due by 18th August 2017, and will collate the responses into a report during Q4 2017. The full questionnaires can be accessed here.[77] The solution will then be handed over in Q4 2017 to take the appropriate next steps as highlighted in the produced report. The appropriate handover organisation will be determined based on the responses to the questionnaire and the nature of the required next steps.

8.8.3 Guidelines for Identity Verification, Authentication and Risk Assessment

Our Strategy highlighted the need for guidelines for identity verification and management of Payment Service Users (PSUs). During 2017, we created a detailed scope document, outlining the content for the proposed guidelines, and how this ties in with the current state of UK legislation with regard to identification and verification of PSUs.

We completed our work on this solution during June 2017, creating deliverables that will be the basis of the development of the Guidelines. We are looking to conclude a formal handover in mid-August 2017 to an industry body, who will take the solution to completion by commissioning the new guidelines, and overseeing the testing, validation and refinement of the guidelines. A first draft of the guidelines should be produced by the end of 2017, with the guidelines ready for publication in by the end of June 2018.

8.8.4 Customer Education and Awareness

Our Strategy endorsed the current industry initiative for customer education and awareness on financial crime and fraud. We recommend that the payments industry should strongly support and engage in the current programme, and that particular consideration be given to the fast-changing nature of some fraud types, and that the payments industry seek to collaborate extensively to be more cost effective in educating society.

On 31st March 2017, the ownership of this solution handed over to FFA UK, to continue to raise customer awareness and help prevent more customers falling victim to financial crime. FFA UK must report on their progress on a quarterly basis during 2017.

8.8.5 Financial Crime Data and Information Sharing

The 'Financial Crime Intelligence Sharing' solution to deter and prevent criminal activity in payments systems and to reduce some of the friction affecting good consumers, as set out in our Strategy, has been reviewed and refined, resulting in a clearer focus and description of 'Financial Crime Data and Information Sharing'.

The solution handover to an industry body is being progressed in July 2017, who will carry it forward as part of detailed analysis and planning for activity over the next two years to: create a more effective model and roadmap for financial crime data and information sharing, building on the successful existing fraud data sharing model; examine options and help establish a stronger industry capacity and capability on financial crime data and information; and work with the government to develop a more effective legal framework on data and information sharing for the purpose of detecting and preventing all types of financial crime.

[76] A set of the deliverables produced by the financial crime solution workstreams have been included as supporting materials, and can be found at the following link: https://implementation.paymentsforum.uk/consultation

[77] Link to Forum website to access questionnaires: https://implementation.paymentsforum.uk/access-account-services-questionnaires

8.8.6 Enhancement of Sanctions Data Quality

Our Strategy highlighted the advantage that can be gained from higher quality identifiers for sanctions list entries. Enhancing the quality of the sanctions list entries would lead to fewer false positive matches against genuine customers, and a greater chance of identifying bad actors. During 2017, we met with HMT to identify steps to progress the case for enhanced data quality for sanctions list entries.

This solution is being handed over to an industry body in July 2017, who will take the solution to forwards by liaising between Government and the payments industry. The industry body will work with HMT and the payments community during 2017 to outline a clear set of examples where the quality of sanctions list entries is causing detriments to organisations, and identify a clear set of next steps of remedial action as appropriate. It will also look for any opportunities for linkage to the New Payments Architecture programme.

8.9 Appendix 9 – Composition of the Forum

The Forum currently consists of a Chair which is independent of the payments industry and 22 members appointed jointly by the PSR and the Forum Chair.

1. Ruth Evans – Chair
2. Alan Smith – Head of Payments and Banking Services, Post Office (Member until 1 March 2017)
3. Becky Clements – Head of Industry Engagement and Payment Change, Metro Bank
4. Brendan Peilow – Crown Representative, Banking and Payments, Cabinet Office
5. Carl Pheasey – Head of Policy, Money Advice Service (MAS)
6. Carlos Sanchez – CEO, Orwell Group
7. Faith Reynolds – Member, Financial Services
8. James Emmett – Chief Operating Officer, HSBC
9. Katherine Horrell – Group Treasurer, Centrica
10. Marion King – Group Director of Payments, The Royal Bank of Scotland (RBS)
11. Mark Lyonette – Chief Executive, ABCUL
12. Michael Maier – Deputy CEO, Fidor AG
13. Mike Smith – Commercial Director, Raphaels Bank
14. Neil Lover – Head of Payments and Financial Crime, Coventry Building Society
15. Neil Rowan – Head of Enterprise Billing and Global Sourcing, BT
16. Otto Benz – Director of Strategic Payments, Virgin Money
17. Paul Horlock – Director of Payments, Nationwide
18. Philip McHugh – Chief Executive, Barclaycard Business Solutions (Member until 1 March 2017)
19. Russell Saunders – Managing Director, Global Payments, Lloyds Banking Group
20. Ruth Wandhöfer – Global Head for Regulatory and Market Strategy, Citi Bank
21. Sian Williams – Director of the Financial Health Exchange, Toynbee Hall
22. Steven Cooper – Chief Executive Officer, Barclaycard Business Solutions
23. Thaer Sabri – Chief Executive, Electronic Money Association
24. Tony Shaw – Head of Treasury, Cash and Banking, Tesco

8.10 Appendix 10 – Acknowledgements

After publication of its Strategy in November 2016, the Forum committed to seeking the input of a wide range of stakeholders within the payments industry. The purpose of engaging stakeholders was to provide input and support the development of this Consultation Paper.

The Forum is grateful to the parties below for their time and input:

Accenture
ACI Worldwide
Advanced Payment Solutions
Age UK
AllPay
The Association of British Credit Unions Ltd (ABCUL)
Association of UK Payment Institutions
Bacs Payment Schemes Limited
Bank of England
Barclays Bank
BCS Consulting
Bottomline Technologies
Bovill UK
British Bankers' Association
British Gas
British Retail Consortium
BT Group Plc
Building Societies Association
Centrica
CGI
CHAPS Co
Charteris Consulting
Cheque and Credit Clearing Company
Cabinet Office
Citibank
Clarion Housing Group
ClearBank
Clydesdale Bank
Competition and Markets Authority
Cognizant Worldwide
The Consumer Panel
Consumers International
Coventry Building Society
Dovetail Systems
Driver and Vehicle Licensing Agency
Department for Work and Pensions Group
Electronic Money Association
Equens Worldwide
Experian Ltd
EY LLP
Factern
Faster Payments Scheme Limited
Financial Conduct Authority
Fidor AG
FIS Global
Financial Fraud Action UK
Flawless Money Limited
Handelsbanken
HM Revenue & Customs
HM Treasury
HSBC
Information Commissioner's Office
Innovate UK
Ipagoo
Joint Money Laundering Intelligence Taskforce (JMLIT)
LJPTech
Lloyds Banking Group
London Chamber of Commerce and Industry
Metro Bank
Mk2 Consulting
Mobile Payments Service Company Limited (Paym)
The Money Advice Service
Nationwide Building Society
National Federation of Self Employed & Small Businesses Limited (FSB)
Nets A/S
NS&I
Open Banking Implementation Entity
Orwell Group Holding Limited
Payment Systems Regulator
Payments UK
Paysafe
Prudential Regulation Authority
QuidCycle
Raphaels Bank
The Royal Bank of Scotland Group
Santander UK
SETL Development Limited
Starling Bank
SWIFT
techUK
Tesco PLC
Thomson Reuters
Toynbee Hall
Transport for London
TSB Bank PLC
Tusmor Limited
UK Finance
University of Greenwich
Virgin Money
VocaLink
Yorkshire Building Society

8.11 Appendix 11 – Glossary

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.

Account Identifier: Combination of numeric, alphabetical or alphanumeric characters used to uniquely identify an account.

Account Information Service: An online service to provide consolidated information on one or more payment accounts held by the Payment Service User with another Payment Service Provider or with more than one Payment Service Provider, and includes such a service whether information is provided.

Account Information Service Provider (AISP): A payment service provider which provides account information services.

Aggregation / Collection: A function that collects funds for a customer's account and updates their account with the aggregated value.

Aggregator: An organisation that provides one or more PSPs with technical access to one or more payment systems.

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.

Attended Payment: A payment where the payer who initiated the payment is physically awaiting a response. This will typically be a Single Immediate Payment.

Auth Store: A data store that holds the payer's authorisation code that is tied to a specific transaction.

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 without direct contact with the customer.

Bacs Payment Schemes Ltd (BPSL): The operator of the Bacs payment system.

Bacs Payment Services (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).

Bacstel IP: One of three communication channels used to connect to the BPSL infrastructure. This is typically used by indirect PSPs and corporates with smaller transaction volumes.

Bank of England (BoE): The central bank of the UK. It runs the RTGS service used for settlement in central bank money and is the prudential supervisor of some types of PSPs as well as payment systems with an objective of protecting and enhancing financial stability.

Bulk Payment: Provides the ability to make multiple debit payments in one transaction.

Bureau: An organisation that sends payments to Bacs on behalf of another organisation.

Central bank money: Is the technical term used to refer to money that can only be created by a central bank.

Channel: An interface through which communication can be made.

CHAPS: The sterling same-day system that is used for high-value / wholesale payments as well as for other time-critical lower-value payments.

CHAPS Co: The CHAPS Clearing Company Limited, a private sector entity which is responsible for the day-to-day management of CHAPS.

Cheque & Credit Clearing (C&CC): Payment system 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.

Cheque & Credit Clearing Company Ltd (C&CCCL): Operator of the Cheque & Credit Clearing payment scheme.

Clearing: A process in which two main functions may be performed: (a) the exchange of a payment instrument or relevant payment information between the payer's and the payee's financial institutions, and (b) the calculation of claims for settlement. The outcome of this process is a fully processed payment transaction from payer to payee, as well as a valid claim by the payee's institution during the clearing process.

Competition and Markets Authority (CMA): The CMA is a non-ministerial department of the UK government that promotes competition for the benefit of consumers, both within and outside the UK.

Confirmation of Payee (CoP): A capability which will provide a payer with assurance that the account to which they are making the payment belongs to the intended payee.

Consent Store: A database which holds customers' consents to allow a TPSP to facilitate payment initiation.

Consumer: A person who buys goods or services for their own use.

Corporate: Relating to a large company.

Credit card transaction: A card-based payment transaction where the amount of the transaction is debited in full or in part at a pre agreed specific calendar month date to the payer, in line with a prearranged credit facility, with or without interest.

Crowdfunding: People invest through crowdfunding platforms to test new products, identify new investments and be at the forefront of innovation.

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 by the PSP.

Debit card: A card enabling its holders to make purchases and / or withdraw cash and have these transactions directly and immediately charged to their accounts, whether these are held with the card issuer or not.

Debit card transaction: A card-based payment transaction, including those with prepaid cards that is not a credit card transaction.

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 (DD): 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 PSP or to the payer's own PSP.

Directory Look-Up: A function which obtains reference data from the master database (e.g. sort code, bank, overlay level EISCD reference data, CASS account transfers and customer reference data, PSP and TPSP endpoints, roles and certificates). These are necessary to make and route payments.

Discounted Cash Flow (DCF): A valuation method used to estimate the attractiveness of an investment opportunity.

End-user: Person or organisation that actually uses a product.

End-User Needs (EUN): The functionality of payments infrastructure required for consumers, businesses and Government identified by the Strategy. These are listed as greater control, greater assurance, enhanced data, as well as a reduction in financial crime.

Extended Industry Sort Code Directory (EISCD): A downloadable database containing information about all banks and building societies that are connected to the UK clearing systems. These include BPSL, FPSL, CHAPS Sterling and Cheque and Credit Clearing.

Faster Payments Service (FPS): The scheme used for real-time payments including standing orders.

Faster Payments Scheme Limited (FPSL): Operator of the FPS payment system.

Financial Conduct Authority (FCA): A regulatory body for financial services industry in the UK. Its role includes protecting consumers, keeping the industry stable, and promoting healthy competition between financial service providers.

Financial Fraud Action UK (FFA UK): Financial Fraud Action UK (FFA UK) is the name the financial services industry uses to coordinate its fraud prevention activities.

FinTech: Financial Technology companies that provide services and technology to institutions and consumers.

Forward Dated Payment: A payment set-up to be processed on a date in the future.

General Data Protection Regulations (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Parliament, the Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It was published in the Official Journal of the EU on 4 May 2016. It will apply from 25 May 2018.

Governing body: A group of people who formulate the policy and direct the affairs of an institution in partnership with the managers, especially on a voluntary or part-time basis.

Her Majesty's Treasury (HMT or the Treasury): The British government department responsible for developing and executing the government's public finance policy and economic policy.

High-Value Payment System: A payment system designed mainly for large value, high priority, but lower volume, payments to be made between participants with immediate settlement finality.

High Yield debt: Also referred to as junk bonds, High Yield debt is a debt instrument which carries a higher risk of default and typically pay a higher yields.

Image Clearing System (ICS): The proposed new method revolutionising how cheques are cleared in the UK. The cheques will be cleared using a digital image of the cheque rather than via the current paper-based clearing system where the actual paper cheque is transported around the country to be cleared.

Individual Savings Account (ISA): A class of retail investment arrangements available to residents of the United Kingdom, qualifying for favourable tax status.

Information Commissioner's Office (ICO): The UK's independent body set-up to uphold information rights.

Intellectual Property (IP): Intangible property that is the result of creativity, such as patents, copyrights, etc.

ISO 20022: An international standard for the development of financial messages which ICS will be the first UK payment scheme to adopt.

JavaScript Object Notation (JSON): An open standard file format used for data interchange.

Joint Fraud Taskforce (JFT): The Joint Fraud Taskforce is made up of key representatives from government, law enforcement and the banking sector and has been set-up to tackle fraud.

Joint Money Laundering Intelligence Taskforce (JMLIT): JMLIT has been developed in partnership with the financial sector to combat high end money laundering. Its website is: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

Joint Venture (JV): Is a business entity created by two or more parties. Parties tend to provide capital, resources, know-how and IP into JV vehicles.

Know your customer (KYC): KYC is the process of a business, identifying and verifying the identity of its clients.

Market participant: A Participant is an entity that has a payments service relationship with the NPSO. It can include settlement Participants, direct Participants, indirect Participants, service Participants, third party providers and aggregators.

Net Sender Cap (NSC): A control mechanism to limit the credit exposure each participant brings to the system.

Net Present Value (NPV): The value in the present of a sum of money, in contrast to some future value it will have when it has been invested at compound interest.

New Payments Architecture (NPA): The NPA Design Hub has been established by the Forum to progress the detailed design of the New Payments Architecture ahead of the handover to the New Payment System Operator (NPSO) by the end of 2017.

New Payment System Operator (NPSO): The new PSO which will be made up of BPSL, C&CCCL and FPSL.

OAuth 2.0: A specification that defines a delegation protocol that is used for conveying authorisation decisions across a network of web-enabled applications and APIs.

Open Banking: PSD2 sets out the regulatory regime that lays the foundations for open banking, by giving registered/authorised third party providers a 'right' to access a consumers account. As part of the implementation of this, Open Banking are designing API Standards to create a more effective system for connecting third party service providers and financial institutions.

Open ID Connect protocols: OpenID Connect allows clients of all types, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.

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.

Paym: A service that enables payments to be made using a proxy such as a mobile phone number to a bank account. Paym is run by the Mobile Payments Service Company Limited (MPSCo), a company limited by guarantee. The Paym service is offered directly to customers by Payment Service Providers that are participants in MPSCo.

Payment Assurance: A function that confirms the payee's and payer's identity as well as the status of a payment.

Payment Execution: Processes the payment at the payee's or the payer's PSP account and manages payment execution.

Payment gateway: A service that facilitates a payment transaction by transferring information between the buyer and the seller.

Payment Initiation Service (PIS): A service to initiate a payment order at the request of the Payment Service User with respect to a payment account held at another Payment Service Provider.

Payment Initiation Service Provider (PISP): A Payment Service Provider which provides Payment Initiation Services.

Payment Institution: A legal person that has been granted authorisation by the FCA in accordance with Article 11 (PSD2) to provide and execute payment services.

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 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 Service User (PSU): A person when making use of a payment service in the capacity of payer, payee, or both.

Payment Accounts: An account held in the name of one or more Payment Service Users which is used for the execution of payment transactions.

Payments Messaging: A communication channel that facilitates the exchange of non-clearing messages (e.g. reports and adjustments) between the PSP and the clearing function.

Payment Services Directive (EU Directive on Payment Services): Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC of 13 November 2007, published in the Official Journal of the EU on 5 December 2007.

Payment Services Directive 2 (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.

Payments 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 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 System Operator Delivery Group (PSO DG): Delivery Group set-up by the BoE and the PSR to manage the consolidation of the three retail PSOs; Bacs, C&CCC and FPS.

Payment Systems Regulator (PSR): The economic regulator of payment systems in the United Kingdom. The PSR aims to promote competition, innovation and interests of end-users of payment systems.

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.

Ponzi scheme: a form of fraud in which belief in the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by later investors.

Private Equity fund (PE): Is a general partnership formed with the intent to invest equity into companies.

Proceeds of Crime Act 2002 (POCA): is an Act of the Parliament of the United Kingdom which provides for the confiscation or civil recovery of the proceeds from crime and contains the principal money laundering legislation in the UK.

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.

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.

Real-Time Gross Settlement (RTGS): The accounting arrangements established for the settlement in real-time of sterling payments across settlement accounts maintained in the Bank of England system.

Request to Pay (RtP): A flexible payment and bill management service concept that offers payers more control over bill payments that is initiated by the payee.

Research and Innovation (R&I): Budget defined by the PSO DG which stands for research and development of new solutions.

Sandbox: The regulatory sandbox allows businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers.

Secure Hash Algorithm 2 (SHA-2): A set of cryptographic hash functions designed by the United States National Security Agency (NSA). The cryptographic hash functions are mathematical operations run on digital data; by comparing the computed 'hash' (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity.

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.

Service user: Service users are defined under Financial Services (Banking Reform) Act 2013 as 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.

Settlement: The process by which a valid claim from the payee's institution is discharged by means of a payment from the payer's institution to the payee's institution. Specifically, the steps in the settlement process are: (a) collection and integrity check of the claims to be settled, (b) ensuring the availability of funds for settlement, (c) settling the claims between the financial institutions, and (d) logging and communication of settlement to the parties concerned.

Simplified Payments Platform (SPP): Relates to only the clearing and settlement functions within the NPA.

Single Euro Payments Area (SEPA): SEPA is a payment-integration initiative of the European Union with the objective to simplify bank transfers denominated in Euro. As of 2015, SEPA consists of the 28 member states of the European Union, the four member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco and San Marino. The project's aim is to improve the efficiency of cross-border payments and turn the fragmented national markets for euro payments into a single domestic one.

Single Immediate Payment (SIP): A payment set-up to be paid straight away.

Small and Medium sized Enterprises (SMEs): Any business with fewer than 250 employees

Standing Order (SO): A payment for a fixed amount to be paid regularly to the same beneficiary.

Standing Order Payments (SOP): an instruction to a bank by an account holder to make regular fixed payments to a particular person or organisation.

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.

Social Time Preference Rate (STPR): A rate used for discounting future benefits and costs, and is based on comparisons of utility across different points in time or different generations

Suspicious Activity Report (SAR): A report made by a financial institution about suspicious or potentially suspicious activity.

Telephony: A channel where customers can access services via a telephone

Unattended payment: Payments which are typically bulk payments with responses not being real-time.

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.

Unitrache debt: Is a debt instrument that combines senior and subordinated debt in one instrument.

Vendor: A technology provider of payment services. Those that offer clearing and settlement services are also referred to as infrastructure providers.

Venture capital fund (VC): Is a form of general partnership which invests into early stage corporations with a higher risk profile.

Which?: Brand name used by Consumers' Association, UK's registered charity, to promote informed consumer choice in the purchase of products and services.