Payments Community Roundtables

2/3 May 2017

Objectives for today

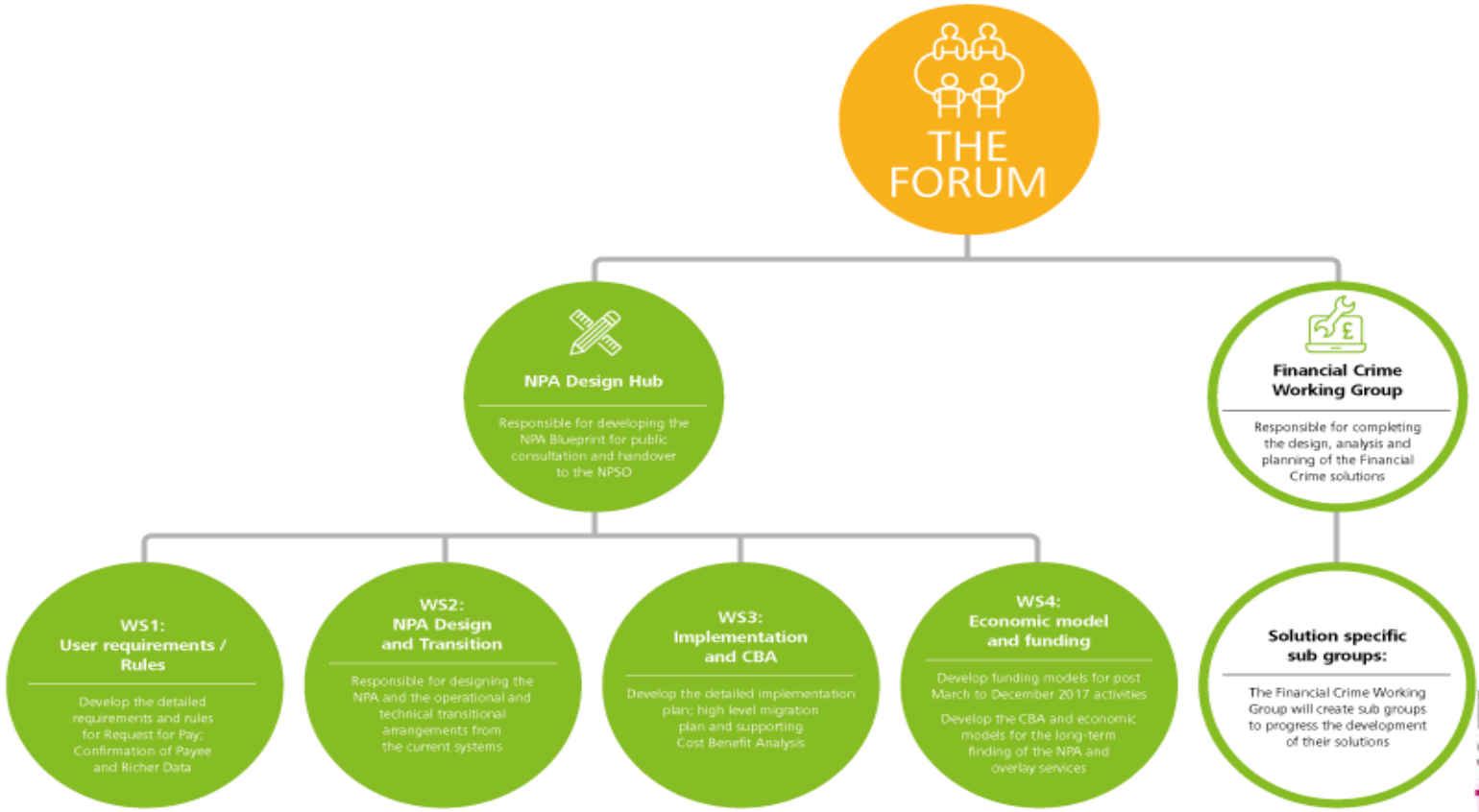
- Provide an update of the Forum's work to date
- Give an opportunity to offer feedback
- Opportunities for engagement

payments strategy forum

The Forum Year Two

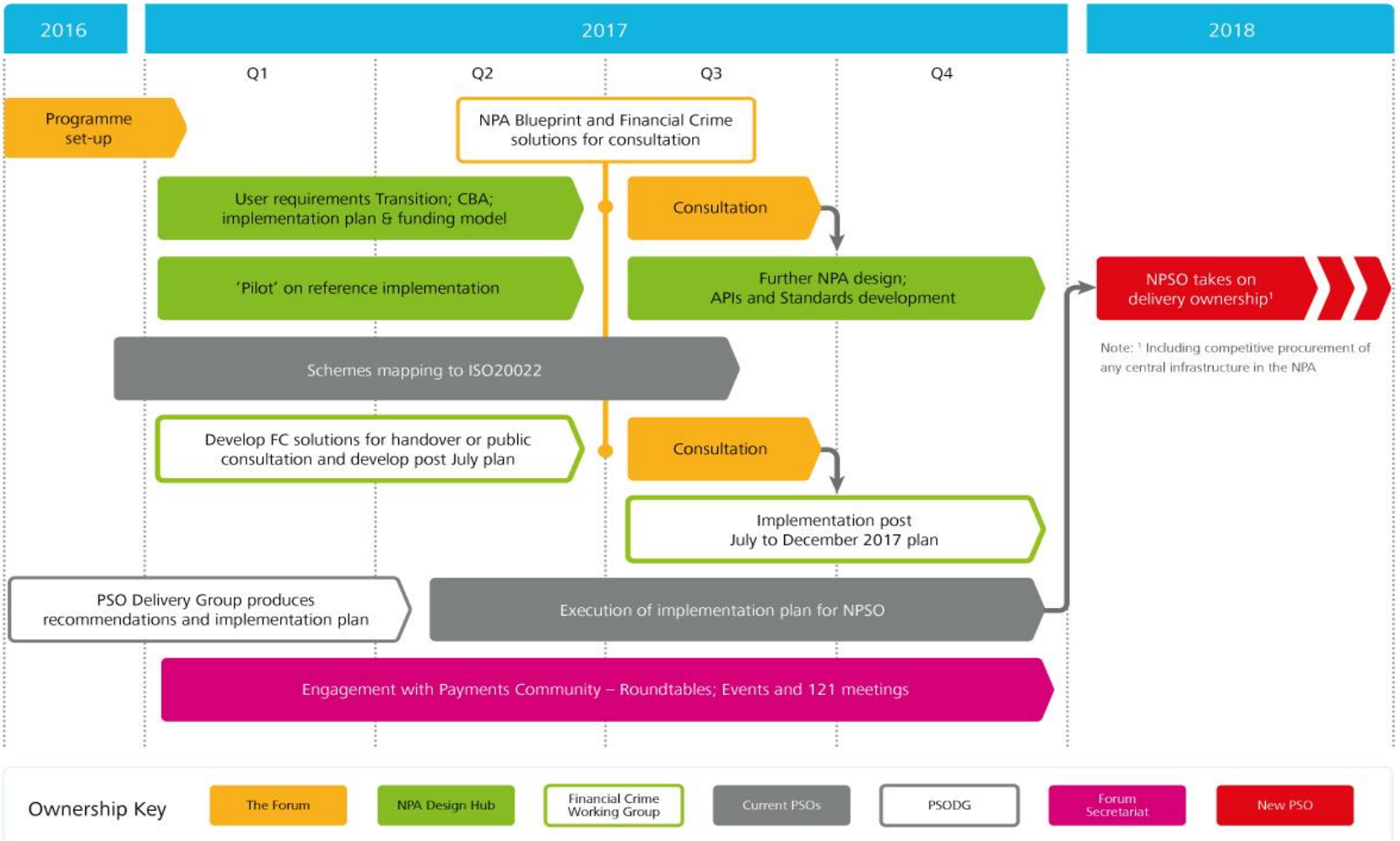
The Forum's Strategy was a starting point; successful implementation will require continued commitment to collaboration between payments industry participants and careful coordination across a number of industry initiatives.

A new working structure has been established to progress the design and delivery of the Forum's Strategy in 2017.



payments strategy forum

2017 High- Level Plan



payments strategy forum

payments strategy forum

NPA Design Hub

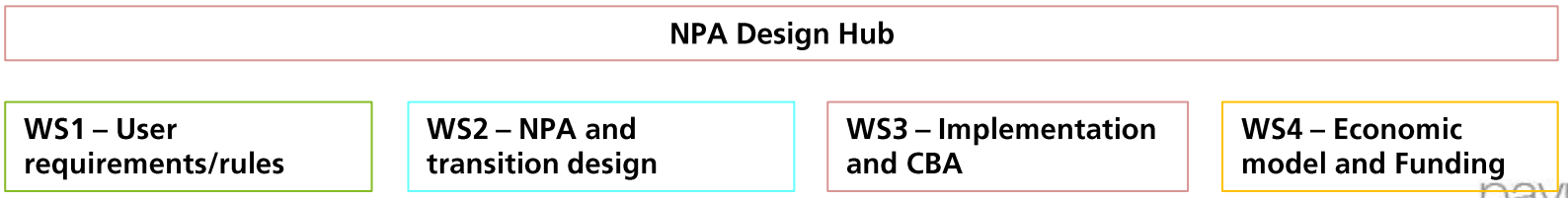
NPA Design Hub

The NPA Design Hub (the Hub) is gathering evidence and supports the Forum's next phase of work in relation to the NPA set out in the Strategy. The Hub has created a work plan based on the high level dates, and coordinates and oversees its work streams (WS), driving their delivery and reporting to the Forum. The Design Hub will document its draft NPA "blueprint" for public consultation by July 2017.

The Forum will finalise its design work and implementation planning, and handover to the New Payment System Operator (NPSO) at the end of 2017. This will include addressing feedback from the public consultation; further design / definition on the above areas, and additional work on API development and standards definition.

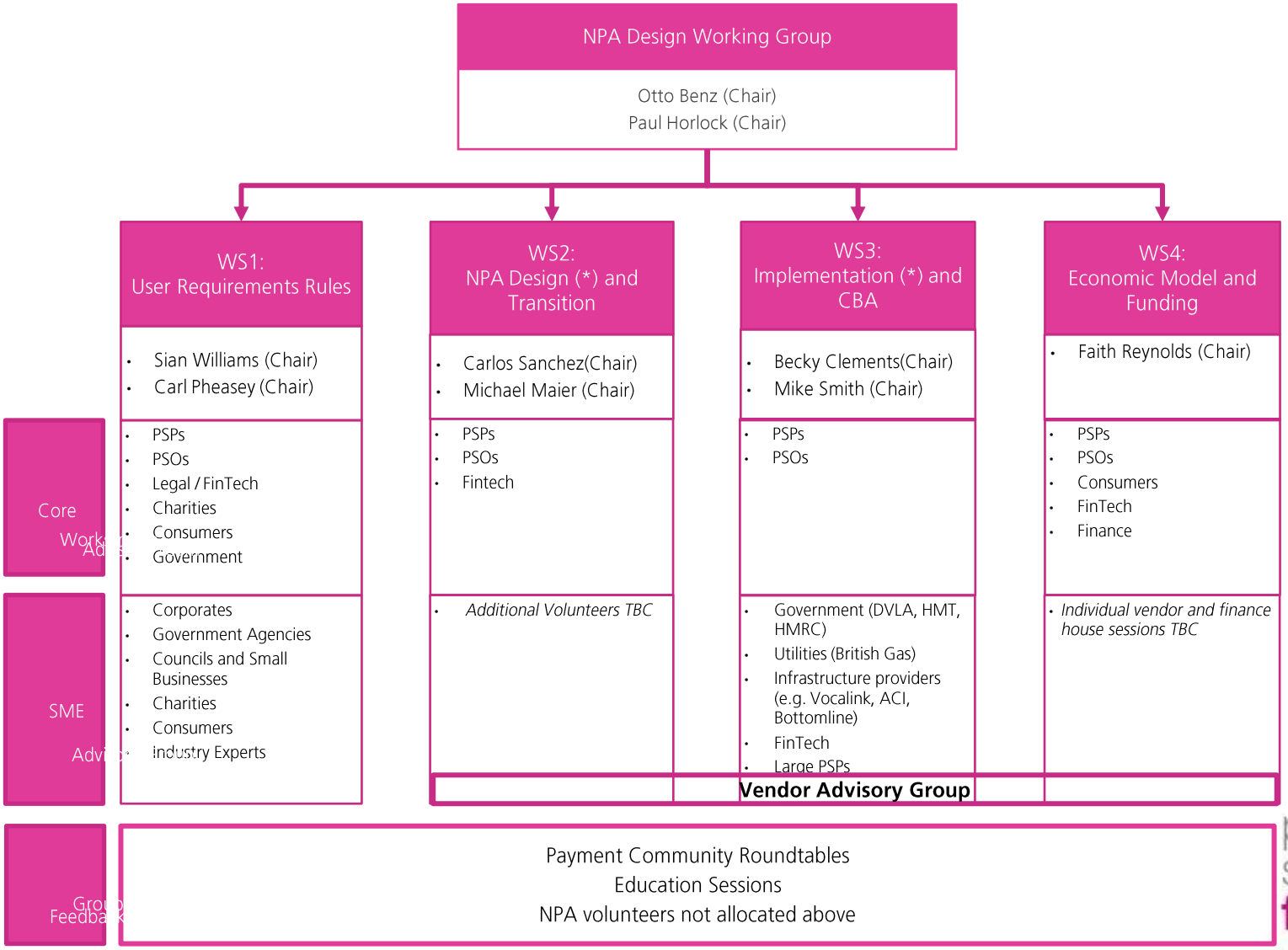
In designing the "Blueprint" and its implementation plan, the Design Hub will take into account all relevant industry initiatives, including:

- The PSR market review into the ownership and competitiveness of infrastructure provision
- The Bank of England's strategic review of RTGS
- The CMA's open banking remedies
- The implementation of PSD2



payments strategy forum

Stakeholder structure of the NPA Design Hub



(*) The Bank of England will be kept informed of the WS2 and WS3 Implementation work but are not part of the Advisory, nor are acting in an official observer capacity.

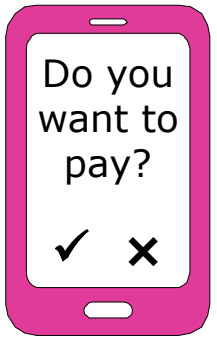
payments strategy forum

payments strategy forum

WS01 – User Rules and Requirements

The 3 End-User Solutions Proposed in the Forum's Strategy

1. Request to Pay



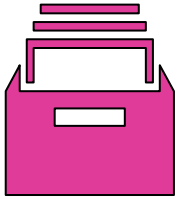
For a majority of end users, current push pull payments work well. However, for an increasing share of the market they are **not flexible enough to meet their needs** especially driven by changing labour arrangements where more and more people/businesses are on increasingly variable income and trading receipt patterns.

2. Assurance Data

At present **end users making a payment are subject to uncertainty at various points in the payment journey.** They are not able to determine for certain the identity of the recipient and thereafter the status of the payment-Receipt as well as any events mid flight.

A recent "Which? Super complaint" to the PSR on safeguards related to push payments highlights some of these vulnerabilities

3. Enhanced Data



Traditionally a payment carries a limited set of data (Amount, Date, Identity of Origin). This is supplemented by a companion document sent via alternative means usually paper based. Receipts, invoices, tax certificates etc. **This inability to add data creates problems with providing sufficient data for reconciliation, adding additional data required for other solutions such as Request to Pay and Assurance Data etc.**

payments strategy forum

WS1 Stakeholder structure

WS1:Leadership - Sian Williams (Chair), Carl Pheasey (Chair)

Core Workstream Advisory Team (Weekly)

Corporates	Government	Councils	Small Business	Charity
Fintech	PSPs	Consumers	PSOs	Industry Experts

SME Advisory Group (Workshops)

Corporates	Government	Councils	Small Business	Charity
Fintech	PSPs	Consumers	PSOs	Industry Experts

SME Advisory Group

- Payment Community Round tables
- Education Sessions
- NPA volunteers not allocated above

payments strategy forum

An approach with needs of end-users at the heart

The Requirements approach:

- is based on the agile methodology
- places the end user at its heart
- encourages a collaborative approach to requirements definition from the various stakeholders







1 PSF Solutions

- Request to pay
- Assurance data
- Enhanced data

2 **Identify use cases**

- Identify use cases
- Identify actors and relations
- Identify various tasks between the various actors
- Case Prioritisation

3 **Elaborate User stories**

- Define user stories
- Define acceptance criteria
- Define high level e2e journeys
- Carry out prioritisation

4 **Detail and refine**

- Detailed user stories
- Detailed acceptance criteria
- Detailed non Functional requirements

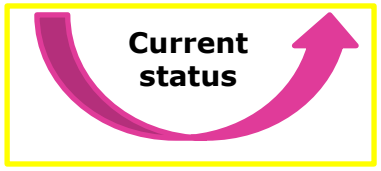
Enablers


Workshops


Stakeholders Consultation


Prioritisation Framework


Review and Sign off



payments strategy forum

General 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

payments strategy forum

Special Case principles

1 Real-time

Request to Pay | Assurance Data

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

2 Definitive

Confirmation of Payee/Payer

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

3 Integrity of Data maintained throughout

Enhanced Data

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

4 Available 24/7 365 days

Confirmation of Payee/Payer

The utility of the Confirmation of a Payer/Payee solution is dependent on it always being available at the point of need.

payments strategy forum

Request to Pay

Use cases

Payee's view

Initiate request to pay

Provide related data (Invoice, receipt, etc.) ED

Receive payer's response

- Reconcile payment
- Update payers account

Associated processes

- Initiate debt recovery

Example

Green Energy (GE), a UK energy supplier, would like to get paid by John, for energy supplied last month. GE sends John a request to pay with a bill amount and due date.

Two days later, GE receives a response from John. He will be paying half of the amount and the rest later. One day before the due date, GE receives a second response from John saying he will pay the remainder immediately.

At the end of the payment cycle, GE reconciles the payments made. They utilize the Request to Pay Reference captured on the payment.

ED Use Case Supported by Enhanced Data

payments strategy forum

Request to Pay

Use cases

Payer's view

Receive request to pay

- Check associated payment info (Invoice, receipt, etc.)

Respond to request to pay

- ✓ Pay Full amount
- ✓ Pay Partial amount
- Request payment extension
- ✗ Decline
- Contact requester/ Help

- Select payment method
- Initiate Payment ED

Example:

John and Mary received a request to pay from Green Energy (GE), their energy supplier, with the amount and due date of their bill payment.

Two days later John accepts to pay half of the amount and initiates the process to pay GE. He then forwards the remainder amount to his dad.

Meanwhile, Mary ignores the request until the due date. On due date, she does not have enough available money so she declines to make the payment and requests GE to contact her to her mobile phone to discuss alternative payment options.

ED Use Case Supported by Enhanced Data

payments strategy forum

Assurance data

Use cases

Payer's view

Confirm Payee's identity

- Determine Payee identity using an associated reference or proxy
- Determine Payee identity using associated reference or proxy details for secondary accounts

Determine Status of payment made

- Determine position on journey to Payee
- Determine Delivery status
- Confirm debit status

Example:

Peter has received a text message from Mark, his window cleaner, with some bank account and payment details for a job Mark just concluded. Peter wants to be sure that the details he received are correct and that the account actually belongs to Mark when he makes the payment. Peter accesses his online banking account, inputs Marks account details and confirms that the account does belong the correct Mark he is willing to pay.

The next day Peter consults the payment he made given that he wants to be sure the payment has reached Mark's account and that the full amount has been accredited to him.

payments strategy forum

Assurance data

Use cases

Payee's view

Confirmation of Payer's identity

- Determine Payer identity using an associated reference or proxy
- Determine Payer identity using associated reference or proxy details for secondary accounts

Determine Status of payment made

- Determine position on journey to Payee
- Confirm credit status

Example:

British Mobile, a Telco, is setting up a Direct Debit for Matt to pay for his mobile bill. They want to confirm that the bank details that Matt has provided them with are accurate, that they belong to him and that he has not provided some else's account.

British Mobile inputs Matts details into the system and confirm that the details are valid and belong to Matt.

British Mobile has the option , if they so wish, to check the payment status of a payment made by Matt

payments strategy forum

Enhanced Data

Use cases

Payer's view

Add additional data to a payment

Identify a payment made

Example:

Anne is making a payment to Northern Water, her water supplier, for February's bill. Within her online banking mobile application, she looks up her customers account and adds it with the payment as required by NW.

Two days layer, Anne accesses her bank and is able to identify every transaction she has made this month and to whom; for what and how much.

Payee's view

Reconcile a remittance to an account

Reconcile a remittance to a transaction

Add additional data to a payment

Example:

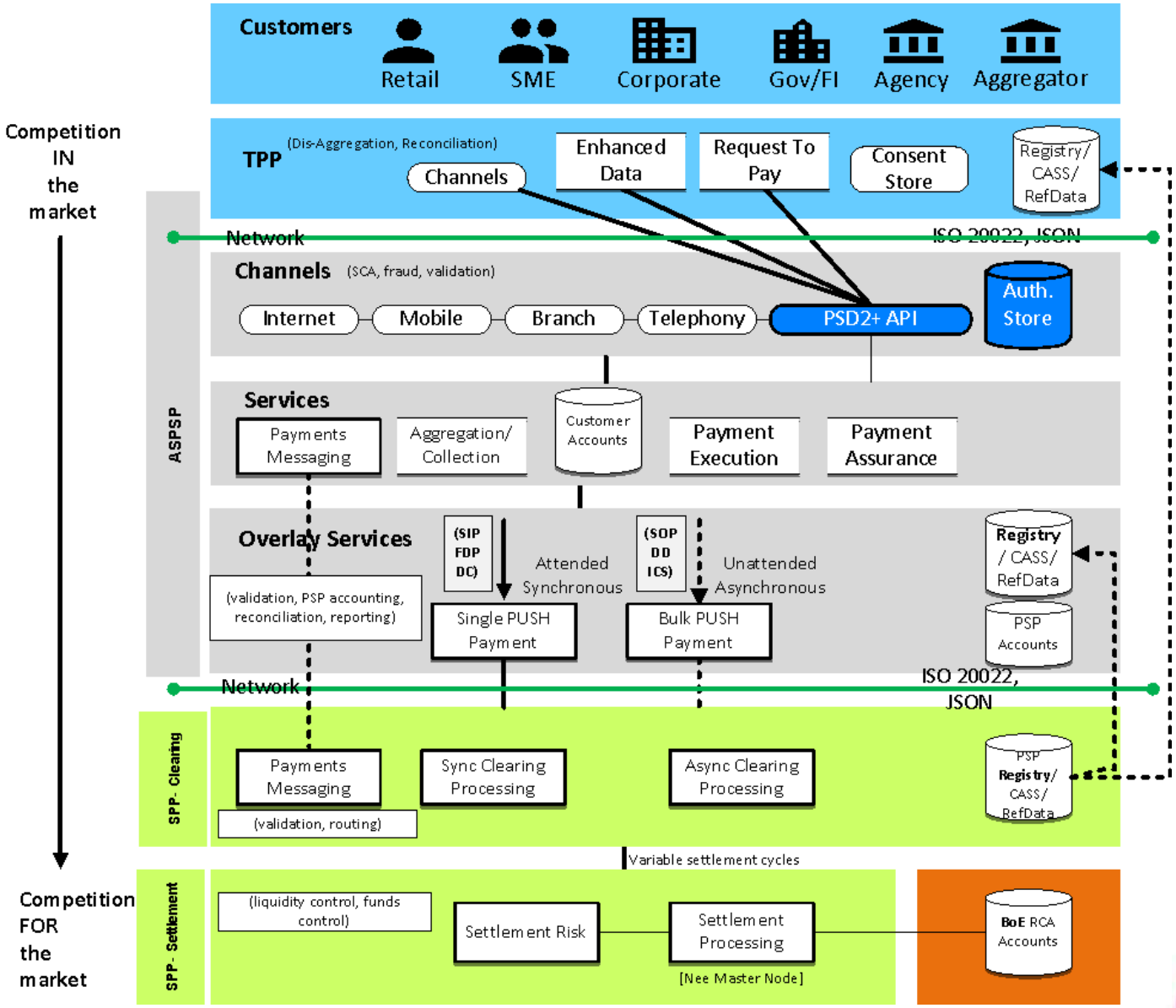
Northern Water (NW), a water supplying company, receives a payment into their collection account.

Using the additional data, they are able to determine that the payment is from their customer Anne (Account holder) for her January sewerage bill. (Transaction). They update her account accordingly.

payments strategy forum

WS02 – Design and Transition

NPA High Level Target Architecture



payments strategy forum

NPA High Level Target Architecture Layers

Name	Description
Customer Layer	The full range of PSUs will be supported, their key use cases will be used to drive the design. - Retail. (Instant Payments, DD/SO management) - Commercial. (High value, Bulk) - Corporate. (Direct Access, Salary, DD Mandates) - Government. (BACS grade 3) - Agency (Messaging) - Aggregator (access RCA, access to Sponsor)
TPP Layer	Created under PSD2, TPPs will provide alternative channels and innovative payments, for multiple ASPSPs - Hold the consent for payments and execute against ASPSP following authorisation - Can implement Request To Pay, using PSD2 APIs - Can provide Channel alternatives and Aggregation and disbursement solutions - ASPSPs can behave as TPPs.
ASPSP Channels	Channels that are directly provided by ASPSPs including APIs required to support PSD2 Open Banking with NPSO extensions to support PULL payments, Overlay specific TRA and variable amounts.
ASPSP Overlay Services	Are approved by the NPSO and implemented on top of PUSH mechanisms (Single Push Payments and Bulk Push Payments). Can be used to emulate existing scheme messages (e.g. FPS, SIPs)
ASPSP Services	Services that are required to execute and process the Payment against the customer account e.g. Debit the customer.
SPP-Clearing	Provides coordination for PSP to PSP payments messaging - Registry records valid PSP participants and roles managed by the FCA/NPSO, with SLAs - Assures validation and correct routing - Separates payments and associated messaging - Real time attended payments will be credited immediately to customer accounts - Unattended and bulk payments will be acknowledged, Refunds process will be available
SPP-Settlement	Single point of settlement control for all payment instructions - Flexible settlement cycles supported by overlay type, to manage settlement risk

NPA High Level Target Architecture Components (1/2)

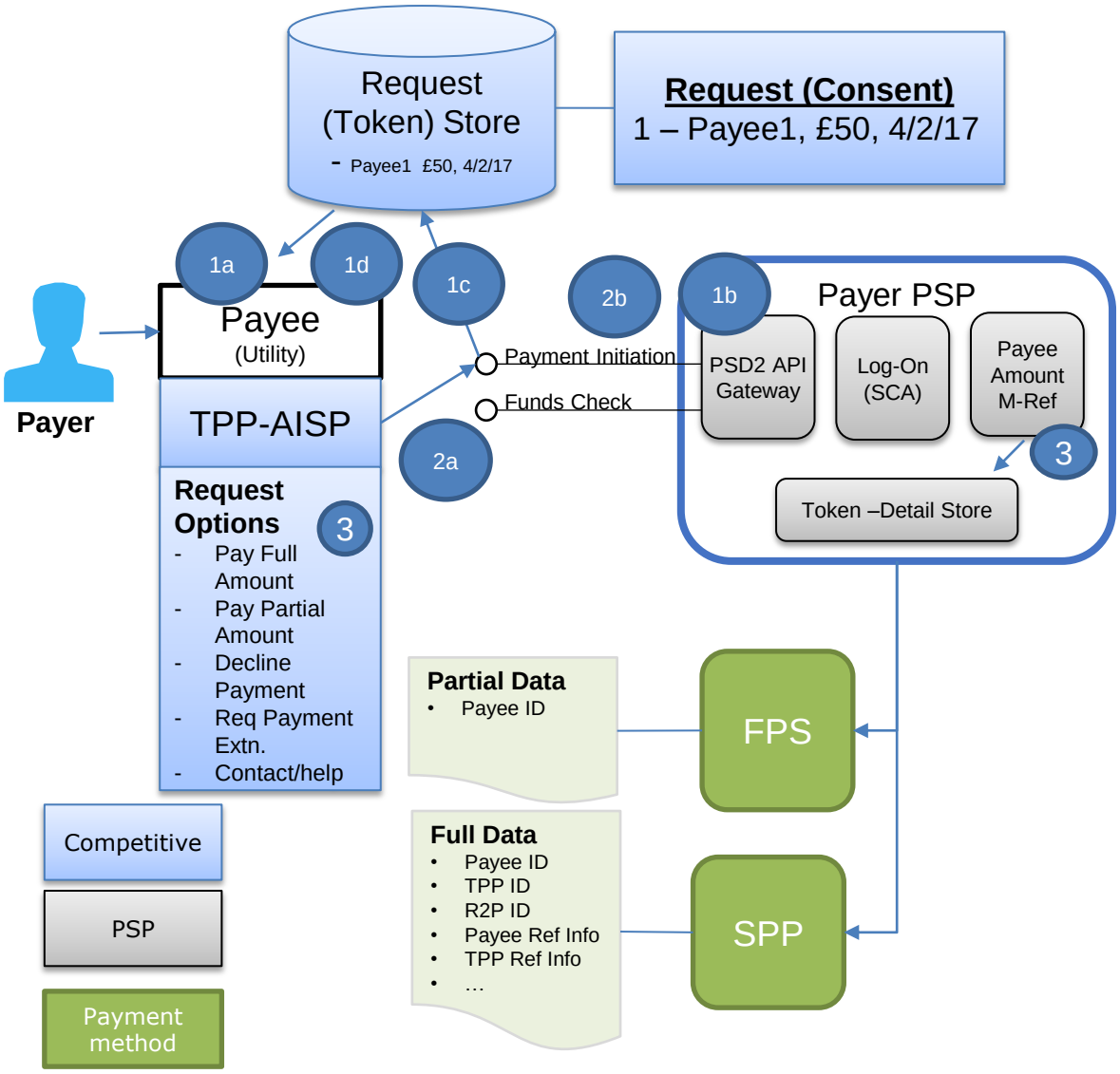
Component Name	Description
Competition for and In the market	The solution will enable competition for each layer and component, PSR/PSF will determine risk criteria and recommend final solution.
TPP Channels	Channels provided by TPPs to their customers in order to access TPP services.
TPP Consent Store	Repository of PSD2 customer consent
Request to pay	The request equates to a PSD2 authorised consent held by the TPP - Customers can change (amend, cancel, defer) consent with the TPP - Customers can withdraw authorisation directly with their ASPSP
Enhanced Data	Support for data content which can be captured by channels or APIs - ISO20022 supports additional data content (including images, cloud data storage references) - Payment messaging is enhanced for optimised business processing
Registry	Provides reference data (Sort Code/Bank/Overlay level (EISCD) reference data, CASS account transfers and customer reference data, PSP and TPP endpoints, roles and certificates) - Managed by the NPSO - Data pushed to participants (TPP, ASPSP) attended channels, unattended channels within SLAs
PSD2+ API	NPA builds on the PSD2/Open Banking APIs and security models. - ASPSP manage customer authentication and authorisation - PSD2 will need extension to support specific use cases (variable amount, TRA, PULL Payments)
ISO 20022	Message content will be based on ISO types - NPA will support JSON syntax for API communications - 4/5AMLD will require that data is not truncated, and available end to end

NPA High Level Target Architecture Components (2/2)

Component Name	Description
Payment Messaging	Advices, Research and Adjustments and reporting
Aggregation / Collection	Aggregation and collection of funds to the customer accounts
Payment Execution	Processing of the payment at the payee or the payer ASPSP account and managing the Overlay Service processing
Payment Assurance	- Confirms Payee Identity - Confirms Payment status - Confirms Payer Identity
Attended Single Push Payment	Routes and manages attended synchronous payment instructions between participants - Ensures that instructions finality rules are followed - Supports multiple overlay payment types, whilst maintaining resilience and safety
Unattended Bulk Push Payment	Routes and manages unattended asynchronous bulk payment instructions between participants - Ensures that instructions finality rules are followed - Supports multiple overlay payment types, whilst maintaining resilience and safety
Network Connectivity	The network is in the competitive space and can be provided by competing providers that comply with the technical standards and rules set by the NPSO.
Settlement Processing	Ensures BOE instruction finality rules are followed and interfacing to BOE RCA accounts - Supplies only the required information for bank to bank transfers
Payment Messaging	Advices, Research and Adjustments and reporting

Request To Pay (R2P) Overview

- Proposed target date for Request to Pay – Q1 2018



1 Step 1 - Create Consent

a. Payee contracts a TPP–AISP to create a Request presented to customer, who approves the **Consent**

b. Customer directed to Log-On to their PSD2[1] compliant PSP, and authorises a One-Off, or Recurring Payment Request from a validated TPP-AISP (optional Confirmation of Payee)

c. Payee-TPP will store the authorised request (consent) token for execution with a Unique ID for reconciliation

d. Customer has visibility of the request in the Payee and their Bank APP

2 Step 2 - Execute Consent

a. TPP-AISP: On the Due date, checks the funds availability before execution (optional)

b. TPP-AISP, on due date executes Token against the customer bank, with confirmation

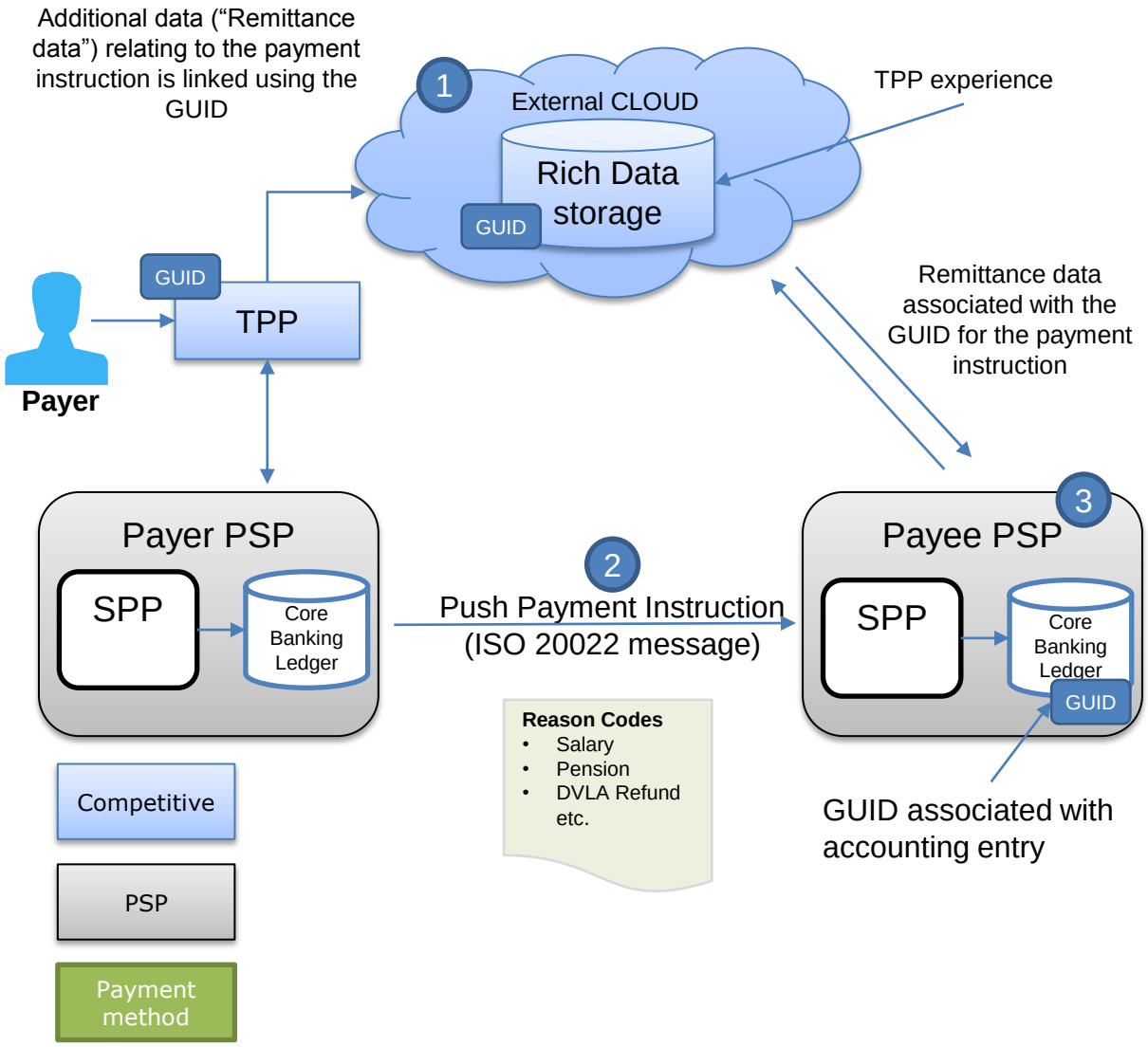
3 Manage Consent – Before Due Date

- Before the due date Customers have control of Requests(consent) from either the Utility or Customer PSP channels
- TPP-AISP provides APIs to the Payee for status changes
- Customers before the due date can select an alternative date option. i.e. TPP-AISP can create a new confirmation consent for a deferred payment

[1] PSD2 does not allow variable debit amounts and changing execution dates

Enhanced Data (ED) Overview

- NPA is a cumulative architecture that will lead to multiple repositories holding enhanced and richer data



1 Step 1

- TPP stores additional payer information in the cloud relating to the payment instruction (linked by the GUID)

2 Step 2

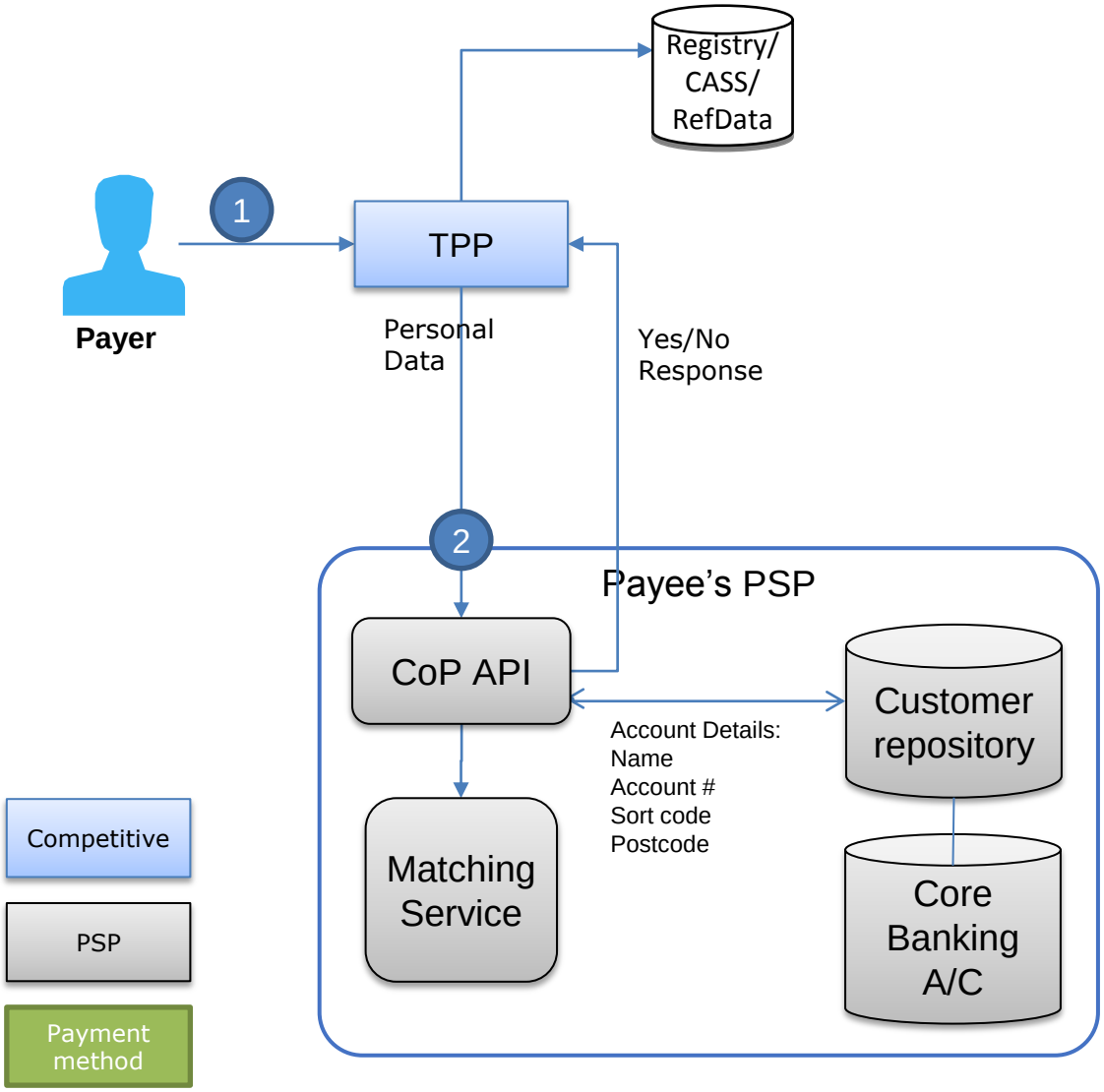
- Payment instructions will be associated with a global unique identifier (GUID) created by the TPP
- The SPP Payer instance pushes an ISO message to the SPP Payee
- A Reason Code will also be included to accommodate the FinCrime requirements
- Additional information captured as part of the Request to Pay process will be linked to the GUID and held in the cloud

3 Step 3

- Payment instruction stored in banking core and provided on statement
- Additional features: CoP used to authenticate access to the cloud data/repositories
- This creates a complete and secure mechanism for data that is held externally to the TPP and SPP

Confirmation of Payee (CoP) Overview

- Confirmation of Payee is independent of the New Payments Architecture
- Proposed target date for Confirmation of Payee – Q1 2018



1 Step 1

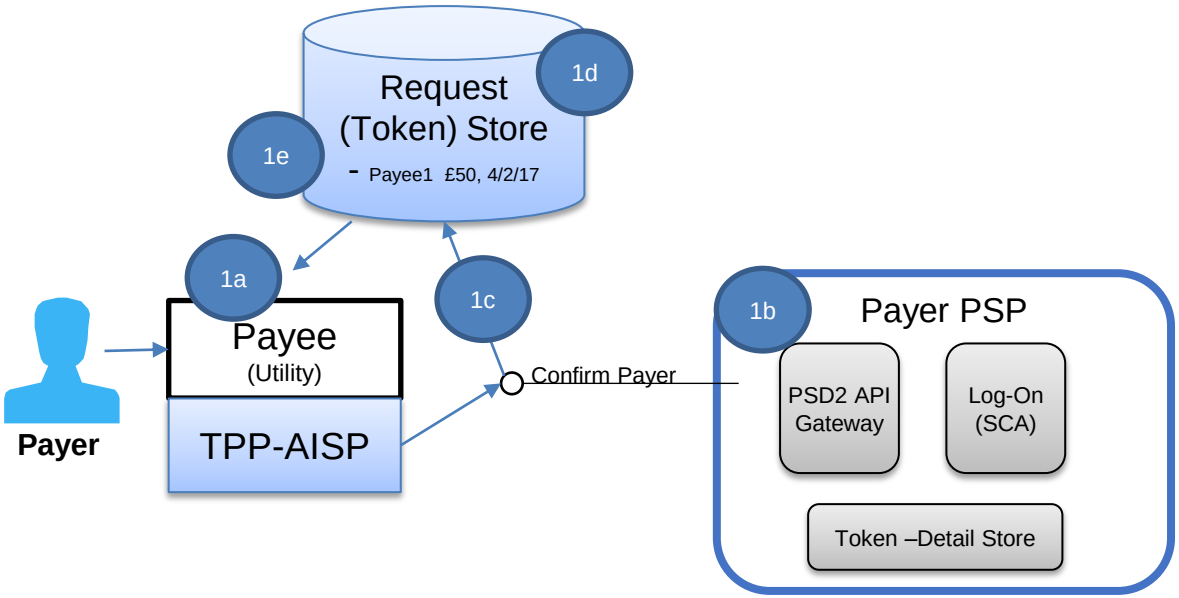
- The payer enter the payee's name, account number, sort code, postcode, and/or any other information requested by their PSPs
- E.g. DVLA prefers to provide the name, postcode, car registration number and location to verify the identity of the customer to whom they want to do a tax refund

2 Step 2

- The Payer personal data will be verified using a matching service built by the PSP
- The payer's PSP carries out a check to verify the payee's details using their account number and sort code

Confirmation of Payer Overview

- Proposed target date for Confirmation of Payer – Q1 2018



1 Steps – Confirm Payer

a. Payee wants to set up a Pull payment for a Payer(customer).

b. Customer directed to Log-On to their PSD2[1] compliant PSP, SCA enables Payee to confirm the Payer's identity.

c. Customer authorises a One-Off, or Recurring Payment Request from a validated TPP-AISP

d. Payee-TPP will store the authorised request (consent) token for execution with a Unique ID for reconciliation

e. Customer has visibility of the request in the Payee and their Bank APP

[1] PSD2 does not allow variable debit amounts and changing execution dates

payments strategy forum

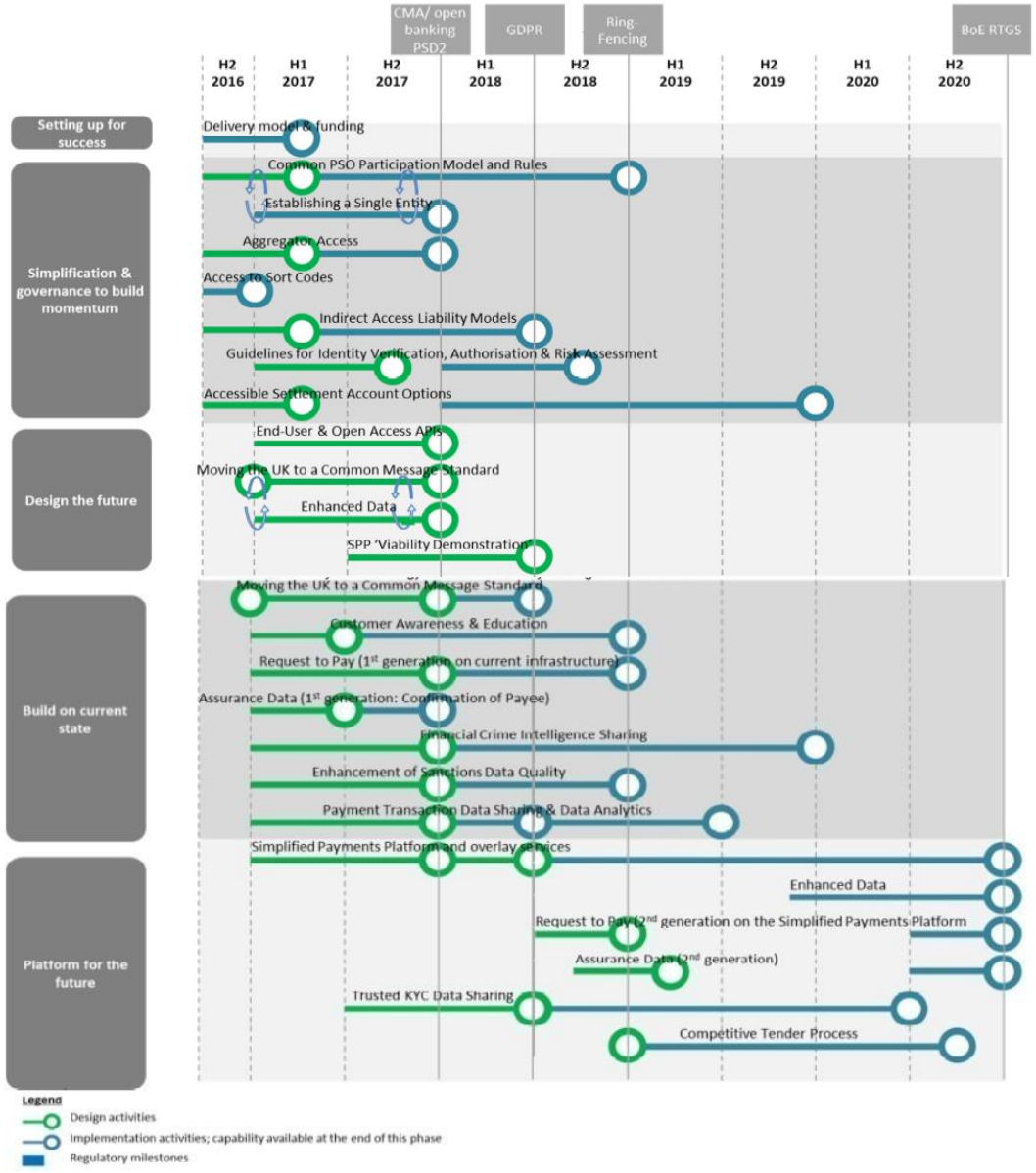
WS03 – Implementation and CBA

Payments Industry Landscape

NPA Implementation

- We have started by generating a view of the change landscape for the payment industry over the next three years in respect of:
    - Landscape – mapping out the key interdependencies between various initiatives, bodies and systems in the payments eco-system
    - Timeline – laying out our understanding of the changes currently underway or planned to be delivered, showing the duration and key milestones, and integrating the requirements of the PSF
- We are assessing Delivery Risk, Change Capacity and Financial Impact
- We have developed a set of implementation principles based on:
    - Customer - Ensuring customer considerations are at the heart of any solution development plans
    - Industry Adoption - Facilitating collaboration with industry participants in the development of any solutions
    - Delivery Constraints - Recognising wider industry developments when developing the plan
    - Technology Complexity - Using best practice in technology implementation
    - Stability - Agreeing plan approach with regulatory bodies including transition through to end solutions

Payment Strategy Forum Requests



TOTAL

25 initiatives

2017

16 Design completed
5 Implemented completed

2018

4 Design completed
7 Implemented completed

2019

1 Design completed
2 Implemented completed

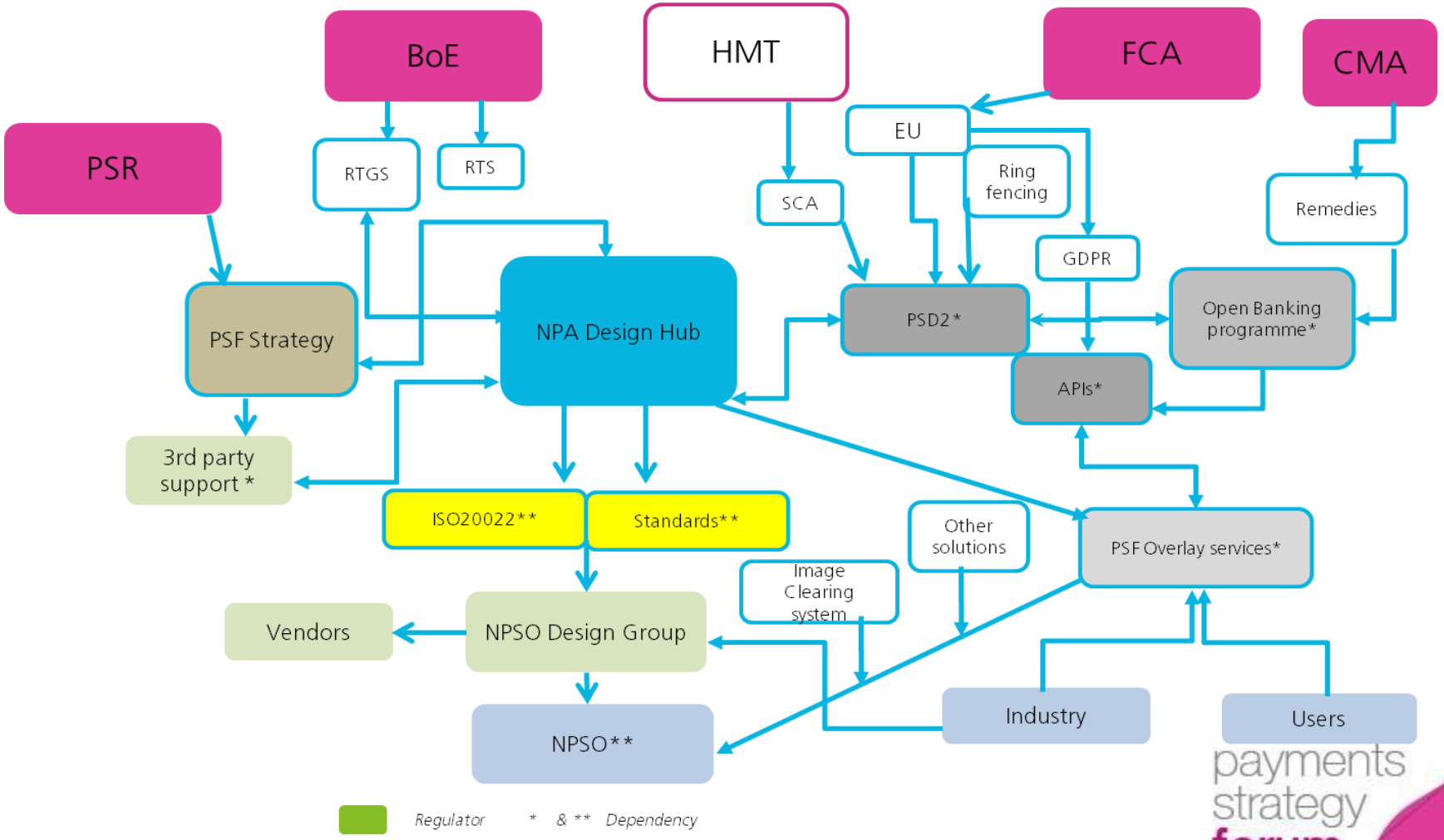
2020

0 Design completed
6 Implemented completed

Source: PSF A payments strategy for the 21st century Nov 2016

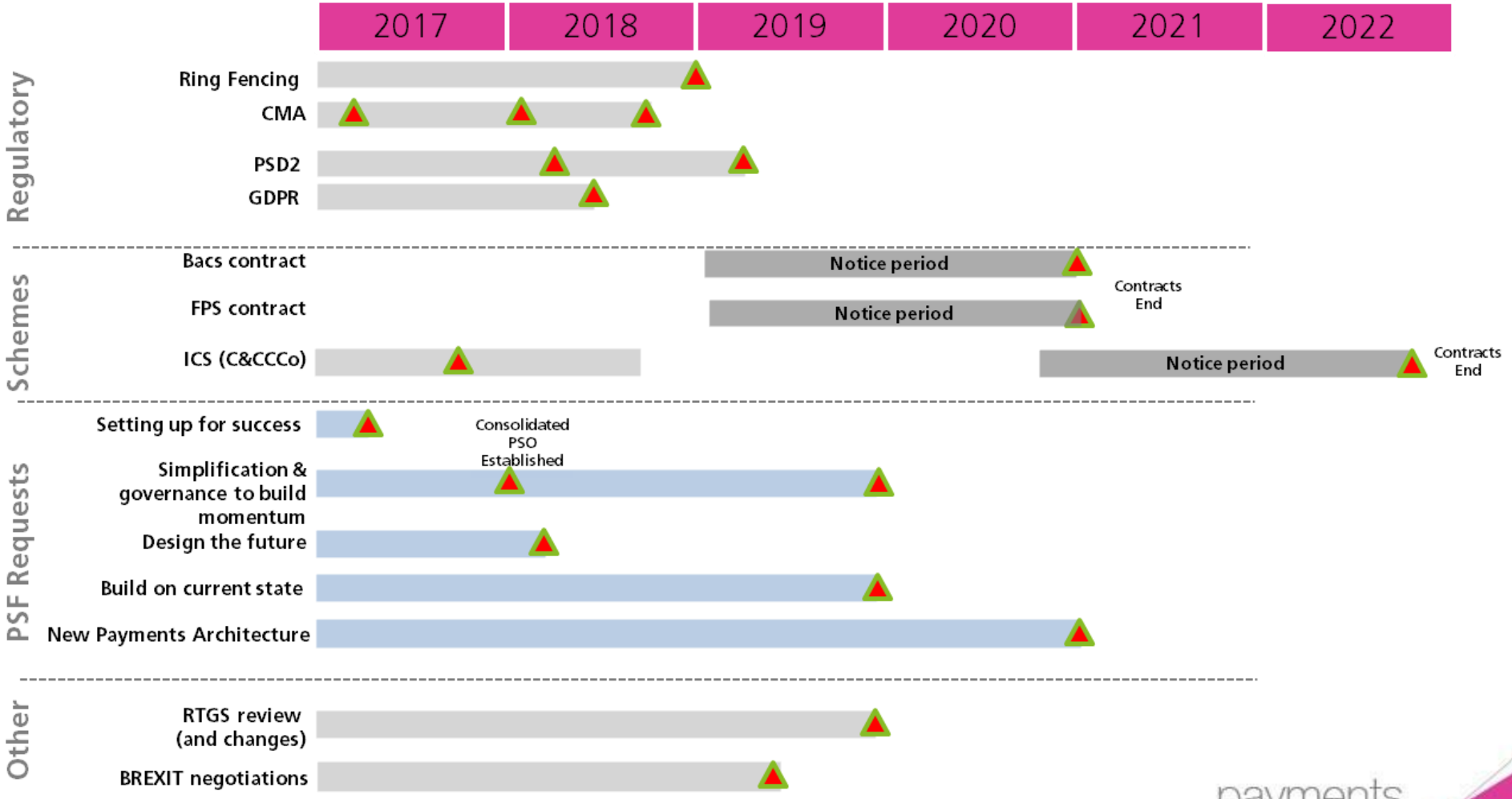
Landscape

The Payments landscape has multiple dimensions: e.g. who, what, when, costs, benefits etc. PSF strategy is being developed in the context of a complex and sometimes inter-related eco system*.



*Example of eco-system dependencies

Current Industry Timeline view



payments strategy forum

Next Steps

Next Steps

- Continue to work up the effort and costs details
- Develop detailed dependency mapping
- Set out and agree a base set of assumptions around migration and take-up
- Specify testing and alignment expectations (to ensure quality and safety of delivery)
- Set out a straw man for stakeholders to understand the possible trades offs that may be necessary between value, safety, resilience and consumer outcomes
- Draw up a draft plan for the consultation
- Continue refining the Cost Benefit Analysis to inform the business case

payments strategy forum

payments strategy forum

Financial Crime, Data and Security Working Group

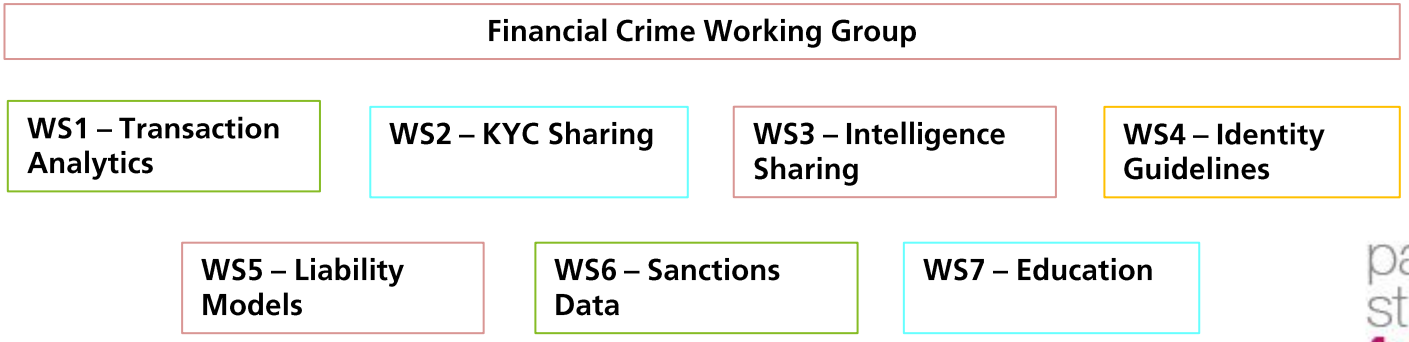
Financial Crime Working Group

Design and implementation

The Forum has proposed seven solutions to address financial crime issues that harm all end users of payments: individuals, businesses, charities, government, and public sector organisations as well as direct loss to PSPs

The Financial Crime Working Group has been established 'to engender user trust in safe and certain payments through collaboratively preventing financial crime'.

- The Working Group is gathering evidence to assist the Forum's next phase of work in relation to the below solutions
- The Working Group has created seven sub groups to drive delivery of their outputs
- Once the solutions have been developed they will be handed over to a suitable body for implementation



payments strategy forum

Financial Crime Working Group Stakeholder Map

- Financial Crime Working Group: broad range of participants
  - trade associations
  - public sector users
  - credit reference agencies
  - small PSPs
  - medium banks/ challenger banks
  - large banks and building societies
  - payment scheme operators
  - payment system operators/ vendors
  - lawyers
  - regulators
  - consultancies

Financial Crime – Customer Detriments

Data Sharing, Reference Data, Analytics

Customer identity, authentication, and knowledge

Customer Education & Awareness

International payments and account activity

Payments Transaction Data Sharing and Data Analytics

What we're trying to do

- High-volume data analytics on existing payments transactions data
- Insights and evidence for fraud, money laundering: funds repatriation, identify mule accounts
- Flexible, adaptable to new crime types (MOs)

Progress in 2017

- Tactical stream – a live service from September, targeting funds repatriation and mule accounts:
  - engaging with 12 banks/ building societies initially, opportunity to extend to other PSPs.
- Strategic stream – develop the capability over 2-3 years:
  - extend range of crime types that can be targeted
  - scale up to industry-wide, open to all PSPs
  - deliver competition in the supply of this service

Next steps

- Detailed planning for the tactical stream: operational design; commercials & funding model, and legals e.g. data permissions
- Produce strategic proposal & plan by end Q2

payments strategy forum

Trusted KYC Data Sharing & Storage

What we're trying to do

- Share KYC information among PSPs, for business (SME) customers
- Manage AML risk: more accurately identify high-risk/ bad actors
- Better experience for good actors
- Robust enabling legal framework and security

Progress in 2017

- Produced a draft proposal on the collaborative role to enable effective KYC sharing
  - minimum set of standards to catalyse the market
  - governance framework to oversee and enhance
- Confirmation of interest from a range of commercial providers to offer data sharing services

Next steps

- Develop principles for definition of standards
- Draft the role/ make-up of the governance body
- Identify route to handover to a new owning entity
- Broader engagement with 3 key groups: PSPs; SME business representatives; KYC service providers/vendors

payments strategy forum

Customer Education and Awareness

What we're trying to do

- Continue to support & engage in co-ordinated industry approach
- Ensure flexible for new threats/ MOs
- Cleaner 'cut-through'; more cost effective

Progress in 2017

- Worked with FFA-UK to complete proposal & prepare for handover
- Handover achieved 31 March
- FFA requested to provide an update to the Forum quarterly

Next steps

- Completed; no further action

Guidelines for Identity Verification, Authentication…

What we're trying to do

- Inadequate identity management and verification a contributor to key fraud types
- Guideline aims to:
    - ease consistency of understanding, interpretation and application of numerous existing regulations and official guidance
    - reduce confusion for PSPs
    - for verifying the Payer and Payee identities

Progress in 2017

- Produced a draft Scope document for the Identity Guideline
- Engaging stakeholders:
    - buy-in and clarity of fit with other identity regulations and guidance
    - identify potential owner for handover
- Produced straw-man view of path to deployment in 2018

Next steps

- Full engagement with potential owner for next phase
- Finalise scope document
- Handover end-Q2/ July

payments strategy forum

Financial Crime Data and Information Sharing

What we're trying to do

- Single, highly secure industry capability
- Span fraud, AML, counter terrorist funding, anti-bribery and corruption
- Confirmed, attempted, suspected, or at-risk events
- Robust enabling legal framework

Progress in 2017

- Agreed objective to produce 'policy paper' setting out the case for more sharing of information
    - i) within industry; ii) with law enforcement
- Identified areas in legislation that would need amending

Next steps

- Deliver draft policy paper during May
- Discuss/ consult with range stakeholders (e.g. BBA, JMLIT)
- Work with BBA, FFA (UK Finance) on handover

Liability Models for Indirect Access

What we're trying to do

- Respective liability of sponsor bank vs. agency bank (or IAP vs iPSP)
- Access for processing payments
- Access to bank accounts for small PSPs
- Enhancements to existing guidance

Progress in 2017

- Approach and scope of activities has been finalised
- Agreed objective is to identify concerns / gaps with existing guidance (e.g. JMLSG)
- Questionnaire drafted to get range of views
    - for Indirect Access Providers (IAPs) and indirect Payment Service Providers (iPSPs)

Next steps

- Plan and run questionnaire consultation (through May-July)
- Use results to propose if the industry should develop further best practice guidance

Enhancement of Sanctions Data Quality

What we're trying to do

- Industry to engage & support HMT & FCO in addressing opportunities to improve operational approach to sanctions compliance
    - Quality of the data
    - Data management framework
    - adoption of international sanctions models

Progress in 2017

- Confirmed areas to address with Government
    - Improved data points – improve the population of accurate data (e.g. for primary and secondary identifiers).
    - Migrate to the new standard of how data is collated, to reduce level of fuzzy matching required (and align to the standards to be used in the US)

Next steps (and end owner)

- Meeting lined up in May with HMT (Office of Financial Sanctions Implementation) and FCO Sanctions Team
- Further actions & planned approach to be agreed with HMT, FCO

payments strategy forum

Thank you