payments strategy forum

A Payments Strategy for the 21st Century

Putting the needs of users first:

Supplementary documents – Solution descriptions

November 2016

Table of Contents

Responding to End-user Needs

Request to Pay

What is the solution?

- The proposal is for payment requests to be sent between entities prior to the payment itself (e.g. from an SME to a customer).
- The request for payment would include more information than is currently possible (e.g. the amount requested, the timeframe for responding, the preferred method of payment etc.).
- The payee's PSP will send payment request instructions to the payer's PSP using an agreed messaging standard.
- The payer's PSP will present the payment request to their customer, who will have the ability to accept, decline, hold or respond to the Request for Payment.
- The Payer will have the ability to respond to the requested (e.g. informing them that they intend to pay an amount different to the original request).
- Request for Payments could function in real-time.
- A central database with agreed standards will be required.
- The legal framework for user rights will need to be developed (e.g. to deal with cases of error or misuse).
- PSPs, regulators and end users would need to be involved in the solution's development and operation.

Is it competitive or collaborative?

The proposed solution takes a collaborative approach to establishing a minimum customer proposition for the solution and a competitive approach to the provision of request-to-pay services.

What are the alternative solutions?

- Current payment types such as Direct Debit will continue at first and competition will determine which payment type(s) are used in the longer run.

What are the key risks and dependencies?

- There is a risk that the market chooses not to implement or adopt 'request-to-pay'.
- The key dependencies of this solution are the implementation of PSD2 and Open Banking. The technical standard of the proposed framework would need to encompass and be conscious of how payment schemes adopt these two initiatives.
- There is a risk that corporates do not want to move away from their current payment method.

Further information about this solution can be found at:

www.paymentsforum.uk/eun-wg-report

Assurance Data

What is the solution?

- The proposal is to enable assurance of both customer identity and the status of payment. In any transaction, the payee's PSP will send notifications to the payer PSPs regarding:
    - The receipt of payment;
    - The processing of payment;
    - The final settlement of payment.
- The solution should allow payer's to track the progress of a payment they have sent.
- The solution will require participation by both PSPs and regulators.
- The solution will assure payer's that the payment was received by the intended recipient. It could also give payers the opportunity to have some control over how the beneficiary uses the payment.

Is it competitive or collaborative?

The proposed solution takes a collaborative approach to establishing a minimum customer proposition for the solution and a competitive approach to the provision of assurance data services.

What are the alternative solutions?

- Potential solutions include:
    - Validating the payee based on previous transaction history held by scheme:
    - An industry-wide proxy service such as phone numbers and emails that would leverage KYC data at each end of the transaction.

What are the key risks and dependencies?

- Data protection requirements will need to be balanced against the need to provide a simple customer experience as well as attempts to prevent financial crime and phishing.
- The key dependencies of this solution are the implementation of PSD2 and Open Banking. The technical standard of the proposed framework would need to encompass and be conscious of how payment schemes adopt these two initiatives.

Further information about this solution can be found at:

www.paymentsforum.uk/eun-wg-report

Enhanced Data

What is the solution?

- The proposal is to for PSPs to have the capacity to attach data to a payment to allow a recipient to easily identify what the payment relates to. This would ideally be done using unique references.
- Data could include pictures, data files, remittance information etc.
- Consumers should be able to review the information linked to payments through multiple channels.

The solution will be developed in three stages:

- Fuzzy matching – the Payer's PSP will be able to respond to the Payee's PSP to confirm that extra data sent alongside a payment has been mapped and is error free.
- Adding the extra assurance data to existing payment schemes.
- Enabling reference data to be fully reconciled through the new Simplified Payment Platform.

Is it competitive or collaborative?

The proposed solution takes a collaborative approach to establishing a minimum customer proposition for the solution a competitive approach to the development of richer data products.

What are the alternative solutions?

- Potential solutions include:
  - Validating the payee based on previous transaction history held by scheme.
  - An industry-wide proxy service such as phone numbers and emails that would leverage KYC data at each end of the transaction.

What are the key risks and dependencies?

- Data protection requirements will need to be balanced against the need to provide a simple customer experience as well as attempts to prevent financial crime and phishing.
- The key dependencies of this solution are the implementation of PSD2 and Open Banking. The technical standard of the proposed framework would need to encompass and be conscious of how payment schemes adopt these two initiatives.

Further information about this solution can be found at:

www.paymentsforum.uk/eun-wg-report

Improving Trust in Payments

Guidelines for Identity Verification, Authentication and Risk Assessment

Why do we need an Identity specification

Criminals can assume identities of individuals and businesses, allowing them to create payment accounts, to misuse third-party or their own payment accounts or to misdirect payments and collections to accounts in their control. Payment services can also be used by criminals to 'layer' illicit funds thereby building a 'veneer of legitimacy'. This results in direct loss incurred by users or payment service providers, anxiety and effort by payment service users, increased cost and work for payment service providers, loss of public confidence in payment schemes, and funding for criminal activity and terrorism.

Inadequate identity management and verification is one the primary reasons why society is exposed to financial crime. Specifically, Financial Fraud Action UK quantified the losses from fraud as £755 million for 2015 – the vast majority of which is estimated to be from misuse of identity. This leads to a loss of trust and, as consumer confidence in specific payment instruments is undermined, they may switch to less efficient forms of payment, compromising the smooth operation of payments systems and decreasing efficiency throughout the economy. Consumers may also turn to value transfer means outside of the regulated environment – for example reverting to using cash – reducing the integrity of the payments market and making it harder for law enforcement to take action against criminals.

Examples of these detriments include:

- Criminals use card details of other payment service users to purchase goods and services online or over the telephone;
- Criminals use the details of other payment service users for sign-up of Direct Debits, for example signing up for a mobile phone contract and obtaining a handset at little or no cost;
- Criminals call payment service users pretending to be their payment service provider resulting in takeover of account and identity fraud;
- Criminals dupe customers into making payments to a fraudster's account, where the victim does not have an opportunity to confirm the owner of the destination account.

Within the industry, primary causes of these problems are:

- Inconsistent terminology and usage;
- Limited consistency between payment instruments;
- Variable application of primary industry guidance regarding identity verification and authentication (e.g. JMLSG guidance);
- Reliance on other PSPs is permitted legally but not straightforward from a risk management perspective;
- No identity assurance scheme for use with payments.

The proposed solution

The proposal is to develop and implement a published, non-compulsory specification as an assessable benchmark to determine how the identity of a payment service user is established, verified, used and subsequently relied upon by other payment service providers.

Whilst there are a number of separate pieces of regulation and legislation which cover this area – including 4th Anti-Money Laundering Directive (2015/849), PSD2 (2015/2366), Regulation Technical Standards on authentication and communication supporting PSD2 and the Wire/Funds Transfer Regulation (2015/847) – there is no consistent, end-to-end approach for managing the identities of payers and payees, providing criminals with the opportunity to exploit loopholes and weaker controls for their gain, to the detriment of payment service users, the payments industry and the UK as a whole. This proposal's aim is to create an overarching, end-to-end approach and overlaps with these pieces of legislation and regulation in order to establish consistent rules for identity which are independent of the payment type and therefore reducing significantly the risk when transferring money using different payment mechanisms.

Compliance with the proposed specification should therefore be proportionate to the scope and size of operations of the payment service provider. By taking this approach the burden on smaller providers should be consequently reduced.

Key components/ features of the solution

The proposal covers both technical implementation, including definitions and capabilities, and governance, including key principles of operation and reliance by third parties. Six main components of the proposed specification are given here:

i. Terminology for identity assurance

   Definition of key terms used by payment service providers with respect to identity establishment, validation and verification. Crucially, this needs to be in the context of different payment services, in consumer friendly language and related to appropriate existing standards.

ii. Convention on use of common identifiers

   Obligation on payment service providers to use a consistent format for representation and storage for common identifiers of payment service users, such as name, address, place and date of birth and personal identity document.

iii. Risk assessment framework

   Obligation for payment service providers to assess payments transactions for risk related to identity. This could be achieved by assessing each transaction or by pre-assessing a group of transactions with similar characteristics.

iv. Identity capabilities

   Key capabilities and principles for a payment service provider which each should be considered when performing risk assessment of transactions.

v. Adherence and assessment

   A payment service provider's adherence to the specification should be assessable such that the senior management of payment service providers, regulators, law enforcement and payment service users can have confidence in the identity establishment, validation and verification processes applied by any particular payment service provider.

vi. Reliance framework

Through consistent adoption, clarity of understanding and auditability, a reliance framework can be established which would enable payment service providers to make informed decisions about the degree to which they wish to reply on identity verification and assurance undertaken by another payment service provider without having to develop an understanding of that organisations' processes and controls. This could reduce the burden of compliance for PSPs and, by providing evidence of good practice by payment service providers and thereby improved risk management, this will support the PSR's goal of improving access to payments markets.

Future phases for this solution

The first phase of this solution is to establish and implement the specification.

The second phase of the proposal is to collaborate in order to create or further develop a number of supporting solutions which exist in the competitive or non-financial services space. These are:

- Digital identity scheme to facilitate identity verification: It is proposed to liaise with the bodies, commercial and governmental, which are setting up identity assurance schemes to ensure the needs of the payments industry are catered for.
- Capability to confirm the identity associated with a payment account proposed to be used in a transaction – for example a link between a cardholder and his/her payment card; between an direct debit payer and her/his account; between an ACH-payment recipient and his/her account – for which some solutions currently exist in the competitive/commercial space. In its simplest form, this would be linking an identity with the identifier of an account, directly or indirectly, using a service like Paym.

Scope

The specification is focussed primarily on:

- Accounts of natural persons, who
- Make payments using:
    - ACH (Bacs, Faster Payments, SEPA);
    - RTGS (CHAPS, TARGET2);
    - Payment card (debit card, credit card, prepaid card).
- Either face-to-face or remotely.

This specification could be further applied to business accounts and employees of businesses, and cheques and other payment types if decided appropriate. In line with the UK's risk-based approach to AML, it is envisaged that electronic money accounts (including prepaid cards), or potentially all payment accounts, that qualify for simplified due diligence arrangements in line with the current (3rd) Money-Laundering Directive and the forthcoming 4th directive (4MLD) would not need to be in the scope for this specification in the first implementation, although they may be in scope in future.

(Payments between online electronic money accounts (or wallets) are not explicitly listed in scope, above, as they typically occupy the position of intermediaries in the payment process, situated between two financial institutions).

Business Case (Benefits & Costs)

The benefits of this proposed solution are:

- Reduced number of payment accounts which are fraudulently set up by more consistent identity verification across all payment accounts (ACH, RTGS, payment card);
- Reduced number of payment accounts taken over or misused by criminals by more consistent identity authentication across all payment accounts (ACH, RTGS, payment card);
- Enhanced and simplified compliance with regulation and legislation around payer/payee identity and information accompanying payments (ACH, RTGS). Reduced ability to conduct cardholder not present fraud by confirming the identity of cardholder/payer (payment card);
- Reduced ability to misdirect payments as part of invoice, supplier, subscription and direct debit fraud by confirming the identity of the accountholder/payer or payee (ACH, RTGS);
- Increased confidence in counterparty payment service providers on their customers' identities by auditable compliance with the specification (ACH, RTGS, payment card);
- Creation and/or extension of existing solutions to confirm identity associated with payment accounts by further collaborative work.

Costs for the first phase are primarily:

- Development of the specification: estimated £150,000 potentially by BSI;
- Assessment costs: either by internal compliance/audit teams or third-party assessors;
- Compliance with the specification: This is difficult to estimate at this stage. Our proposal is to create a specification, but the precise requirements of the specification have not been defined as part of this strategy proposal; that would be done in the detailed design stage. For example if the specification requires real-time checks on identity to support risk-assessment, this would have significant impact and costs for PSPs' real time payments systems. In addition, each PSP will be starting from a unique position so will need to identify areas for remediation.

The costs of the second phase are primarily collaboration costs and are typically borne by impacted parties.

Implementation, compliance and further development

It is anticipated that many of the requirements of the specification are either in place to some degree in payment service providers and that they have capabilities which are not applied consistently across customer groups or payment types. It is therefore envisaged that initial implementation would be primarily a case of documenting existing processes and identifying a limited number of remedial cases.

A benefit of this first phase will be improved confidence between PSPs, and therefore better risk-assessment for payment transactions.

Over the following decade, as the industry improves its risk management and as additional solutions to identity problems become available, it is likely that payment service providers would expect to further improve the robustness of their identity verification and authentication methods, leading to an ongoing reduction in risk across the industry; this is envisaged to require little or no change to the specification and specifically, the risk assessment framework.

Risk assessment

The principle of assessing the risk of transactions is at the core of the proposal. In some cases the risk can be assessed prior to transaction based on criteria such as payment type, value, identity verification already performed and method(s) of authentication used. Furthermore, by documenting the risk assessment, it allows supervisors to confirm that processes meet industry requirements.

Payments Transaction Data Sharing and Data Analytics

Problem Statement

This solution is intended to help prevent and address a range of existing financial crime and fraud-related problems faced by users (consumers, businesses, government) and payment services providers, such as problems in relation to funds repatriation, 'money mule' account activities, and issues related to the confirmation of payer and payee. As such, this solution is expected to play a significant role in addressing a number of the key detriments identified by the Payments Community, as listed below. Furthermore, the intention would be for this solution also to provide the high degree of flexibility and capability necessary to tackle new forms of fraud and financial crime-related activity as these emerge in the future.

Current Detriments

Key detriments addressed relate to the ability to prevent 'money mule' activities, fraud and other financial crime aspects, and also to join up PSPs in a more cooperative approach to sharing information about payee validation with the initiating remitter. Detailed detriments identified at the outset by the Forum that are addressed include:

- Day-to-day concern about risk of identity theft, risk of fraudulent activity on an account;
- Insufficient reference data and lack of knowledge share results in gaps in preventing financial crime: fraud, money laundering, terrorist financing, bribery and corruption;
- Real-time payment risk assessment is limited, reducing the capacity of customers and PSPs to act against fraudulent payments. For example, business customers and Government departments are constrained in identifying fraud by the lack of information available on the payee/beneficiary account, and the payer/remitter account;
- When customer realises a payment is actually a fraud, banks cannot work quickly together to target mule accounts and to prevent funds being paid away;
- The beneficiary bank has limited information about the remitter, the reason for payment, the network of accounts that the beneficiary account transacts with - impacting its ability to identify accounts used to receive proceeds of fraud;
- Unnecessary bank secrecy prevents effective control of money laundering.

Our Solution Proposal: Description

The proposal is to combine the use of central data repository(ies) with high volume data analytics. The central data repository will store existing, current payment transaction data for key UK payment systems (such as BACS and Faster Payments Service). The high-volume data analytics will be applied to the dataset to deliver valuable insights and conclusions for tackling financial crime.

In this context, the following capabilities would need to be established:

- Collaboration and data sharing: Collaboration between payment systems participants (and/or data owners) to share or pool their existing payments data in the interests of combating Financial Crime;
- Data sharing compliance and controls: Data sharing and industry-led data protection related rules, controls and considerations to be applied to deal both with regulatory requirements as well as to provide permitted analytics-related value;
- Application of analytical capabilities to extract actionable insights: Analysis and extraction of appropriate insights which address each of the priority financial crime use cases;
- Distribution of insights: Insights to be made available to relevant industry participants;

- Real-time vs batched: Initially a batch process, it is anticipated that use of these insights vs. the historic and in-flight data will evolve reasonably quickly to provide real-time notifications of potential 'problem' transactions or profiles to participating PSPs.

Solution description: Operating detail and Delivery approach

The Working Group proposes there are two high level options for how this could work.

Under **'Option 1'**, the data repository service would be established as a central industry service, while the analytical capabilities would be established locally by individual PSPs in a devolved manner.

Under **'Option 2'**, a centralised data repository service would be coupled with the provision of centralised analytics capabilities that meet the mainstream needs of a broad range of PSPs. Under this option all participating PSPs would be expected to engage in full with the central analytics capability, while it would also be feasible for individual PSPs to establish additional analytical capabilities in house.

Considering these two options, the Working Group's view is that **Option 2 is preferred to Option 1** for the following reasons:

- Cost effectiveness: Option 1 would logically be significantly more costly overall than Option 2 due to the duplication of effort and expense involved in requiring each participating PSP to maintain its own separate analytics capability. This individual cost requirement could also act as an inadvertent access barrier to smaller institutions wishing to benefit from the solution;
- Solution effectiveness: Option 1 would significantly reduce the potential solution benefits on offer, as many of these are dependent on being able to analyse the full set of transaction data (identification of money mule accounts being a good example), whereas under a devolved model there would be data protection and/or competition issues with PSPs seeing anything other than their own data set.

Option 2: Centralised data and centralised analytic capabilities: Delivery Approach

The Working Group has identified two alternative delivery approaches for this preferred solution option.

Firstly a competitive market-based approach ('**Option 2a'**) whereby an appropriate industry self-regulating body would be responsible for defining the high level solution requirements for relevant services to be delivered from the competitive market place. Commercial provider(s) would then compete to provide the capabilities required to support this solution – i.e. the data repository and analytics capabilities. At a contractual level, this Option could operate based on there being either a centrally procured and negotiated contract with the commercial provider(s) or based on direct contracting between the participants and the commercial provider(s).

An alternative delivery approach could be where the central data repository and analytics capabilities are created as a public utility service, with direct public sector oversight and governance ('**Option 2b'**).

The Working Group is of the view that **Option 2a** is the recommended Delivery Approach, based on the following rationale.

- Incentives for ongoing investment and innovation: It will be critical to ensure that solutions are kept current and receive ongoing investment. Option 2a would ensure that the optimal market incentives are in place to drive future investment and innovation and also to ensure high levels of cost efficiency. A public utility-type approach would not provide these incentives to the necessary degree;
- Maintaining the appropriate balance between competition and collaboration: Under competition law, the free operation of the market should be left to deliver services to meet the needs of consumers except in cases where the market on its own would not be able to deliver. In the latter cases, the level of collaboration should be the minimum necessary to achieve the objective. In the case of the PSF's 'payment transaction data sharing and data analytics' initiative there is clear evidence that there are commercial providers who could - and are interested in - providing such solutions, hence the free market should be left to deliver;

- Maximising the potential for competition for and in the market: In terms of the competitive landscape, Option 2a would promote competition 'for' the market and additionally would allow for competition 'in' the market.

Ultimately, Option 2b (public utility approach) could be seen as the long-stop approach in the (unlikely) event that the market was to fail to step up to the opportunity to deliver commercial solutions in line with Option 2a.

Dependencies

The solution is dependent on PSOs and data owners providing access to payments data, defining how data will be consumed and agreeing rules and standards, (rules do currently exist on data use via an external supplier). PSOs need to support data sharing. The solution will need to consider legal issues such as stated in the Data Protection Act. This is set out in the Working Group's Legal work-stream paper.

Other dependencies have been identified. Payment schemes need to be considered in respect of gaining their support for the data to be used in the interests of combatting financial crime, and the approach in respect of the Data Protection Act for use of customer data in order to tackle Financial Crime needs to be worked through. There are linkages to the EU's second Payments Services Directive (PSD2) such as new IT security requirements, 3rd-party access to payment accounts and payment account information, and reducing barriers to accessing payments systems. Furthermore, there is a linkage between this solution and delivery of the Open Banking Standards programme.

Benefits

This section sets out the principal areas of benefit delivered by this solution proposal.

Decrease in number of instances and victims of fraud, and reduction in the economic losses associated with payment fraud

- Transaction data sharing would create new opportunities to detect fraud patterns, most specifically fraudulent receiving accounts, earlier in the life-cycle of a fraud than today, resulting in lower likelihood of fraudster success. This should reduce the number of customers caught up as victims in a particular fraud type, and increase the proportion of fraud funds that are caught before encashment and therefore can be repaid to the victim.

Improved recovery of 'scammed' funds (funds repatriation to victims)

- In the last four years there has been a material increase in the number and value of customer authorised payments made to the benefit of fraudsters (e.g. invoice fraud, impersonation of bank staff or law enforcement, conveyancing scams) where the victim is not always entitled to a bank refund. Estimates are that over £130M of funds sitting within the UK Banking system that cannot accurately be traced back and returned to the victim. This proposed initiative would also improve payment traceability and therefore increase the level of funds returned.

Improved effectiveness and efficiency in police/CPS costs and effort associated with prosecuting banking fraud

- With improved capability to link cases of fraud to one another across multiple PSPs, the quality of intelligence handed to Law Enforcement should substantially improve, resulting in more effective investigations & prosecutions.

Reduction in financial services' operating costs associated with payment fraud

- The earlier a fraud is detected the lower the operating cost, given that a successful fraud invariably requires material activity to return all parties to their pre-fraud state. This initiative should succeed in reducing financial services' operating costs associated with payment fraud detection and investigation. This will also lower barriers for small PSPs to operate and compete.

Improved payments efficiency for high volume payments receivers (retailers, service providers)

- Improved detection capabilities and rates should lead to fewer excepted transactions and improved sampling levels, likely resulting in ability for transaction size 'floor' requiring compulsory exception for investigation to be raised, increasing net working capital for payee retailers/service providers and reducing their need for trade or bank credit reliance.

Increased client confidence in payment modes such as electronic payments, and in the ability to identify debit and credit parties.

Wider socio-economic benefits and redistribution effects

- Reduction of banking costs, prosecution costs and lower economic losses can be redistributed in the economy through increased investment and consumption, improved working capital conditions for SME retail and service providers, lower cost of funding, etc.

Costs

The cost analysis in this section centres on Option 2a set out above, the Working Group's recommended Delivery Approach for this solution.

The expected costs of the **design phase** should not be great; it is suggested that this phase be time-limited (to a maximum of six months after issuing the strategy), should focus on the high level requirements only and should cover, from a central basis, a limited range of participants and potential suppliers rather than an exhaustive view. Actual solutions can be expected to be proposed from the commercial market against the high-level requirements set out by the working group. Detailed design specification would not be required at the central level, not least to avoid limiting future innovation and constraining the ability of market participants to propose and develop their solutions in this space in a competitive market.

Key high level cost categories for **build and implementation** would include setting up a secure, high-volume data warehouse(s) and buying or building analytical tools (software) and establishing analytical capabilities. There would be costs for participating PSPs to be capable of using the data insights (e.g. adapting existing in-house systems to incorporate new data fields); and potential additional costs for PSPs where they choose to establish their own local analytical capability to complement the central service.

Key high level **ongoing cost** categories for commercial solution providers would include costs for collecting and sharing the payments data, the operation of a data science team(s), the operation of interfaces and processes for securely distributing outputs to PSPs, and the maintenance and running costs of data storage facility(ies). There would also be costs for the security of the repository and the shared analytical capability, and standard IT service costs including maintenance (hardware, software & COTS), vendor support (software & tools, hardware/servers), power, predictive maintenance, facility rent, facility costs, staff recruitment, staff, and telecommunications.

Costs for PSPs directly would include operating costs such as subscription cost (central service), changes to data model, expert IT staff (API management), plus other costs elements.

The Working Group considers that Option 2 would be significantly less costly overall than Option 1 due to the duplication of effort and expense involved in Option 1 in requiring each participating PSP to set up and maintain its own separate analytics capability. This individual cost requirement could also act as an inadvertent access barrier to smaller institutions wishing to benefit from the solution

The Working Group's view is that innovation and market competition would be the most efficient way to ensure incentives are in place for an optimum cost model and ongoing investment to keep up with ongoing Fraud trends and regulatory changes.

Existing services or in-flight initiatives

A number of relevant initiatives are being looked at or are in development by industry participants e.g. SWIFT, VocaLink, Experian. For example, Accura, part of VocaLink, has established a data analytics business. Three of Accura's main areas of focus are fraud, identity and AML. Accura have a 'proof of concept' service under way for Fraud with a number of UK FIs. Relevant aspects of the Accura approach include: i) Data Permissions Rules and Controls with approval from the FIs; ii) Access to payments data agreed by the FIs and Schemes for specific purposes; iii) separate secure data warehouse; iv) Advanced analytical tools; v) Industry skilled data scientists.

Other relevant initiatives / bodies include:

- NCA/Joint Money Laundering Intelligence Taskforce (JMLIT);
- Credit reference agencies;
- CIFAS;
- Joint Fraud Taskforce;
- FFA UK;
- BBA – FCAS;
- Centre for Financial Crime and Security Studies – RUSI;
- Fraud Intelligence Sharing Systems (FISS);
- National Fraud Intelligence Bureau (NFIB);
- Insurance Fraud Bureau (IFB);
- Open Bank Working Group/Open Data Institute;
- FIU type functions already in place, or being developed across the banking community.

Financial Crime Intelligence Sharing

Problem Statement

Currently the sharing of financial crime data and intelligence between PSPs is inconsistent, incomplete, duplicated, untimely, and collected by certain crime types only. There is no single source of the truth which can be interrogated to provide a single view of all known financial crime, which leads to inaccurate assessments of threat levels and trends and missed prevention opportunities.

Several barriers exist constraining intelligence sharing. These include legislation such as DPA, Tipping-off risk, and Proceed of Crime Act amongst others.

Data and intelligence is held in a number of existing databases focused on specific financial crime types, predominantly fraud at present. These rarely interface with each other because a number of the databases belong to commercial suppliers to which PSPs subscribe for the value-added services they provide.

The challenge is to provide access via a single source of data and intelligence without increasing workloads for PSPs, significantly changing working practices or increasing the security risks.

Current Detriments

There are a number of detriments identified by the Forum's Payments Community and Working Groups that are positively impacted by the solution proposals set out later in this paper. These detriments include:

- Insufficient reference data (i.e. documentation of crime types) and lack of knowledge being shared resulting in an inability to prevent financial crime: fraud, money laundering, terrorist financing, bribery and corruption;
- The impact of legal liability creates unnecessary bank secrecy preventing effective control of money laundering;
- The industry and authorities have no single view of financial crime, the data is held in a number of separate databases that are not connected.

Solution Proposal: Description

The proposed solution is to establish and operate a capability or service to share data and intelligence on financial crime, underpinned by the necessary processes and rules, legal permissions, and security. In other words, to set up an industry-operated multi-stakeholder, shared governance, shared funding intelligence-sharing capability underpinned by a formal, strict legal agreement, security code of conduct and appropriate data protection dispensations. Under this model, the stakeholders jointly contribute to and extract benefit from the solution as a single, highly secure, central industry data and intelligence sharing enabler. This ensures that the industry is in full control of the system, its evolution and the manner in which it operates.

Key features include:

- Role and permissions based user access and functionality;
- Near-real-time and real time, all known financial crime data records for confirmed, attempted, suspected or at-risk events relating to an identity, financial account or article of crime, for the purposes of data matching, data mining, trend analysis, and profiling;
- Flexible and open interfaces (APIs) for tight integration;
- Dynamic and flexible inward and outward extract/transform/load capability;

- Ring-fencing/ segregation capability;
- Flexible automated data submission and extract capability;
- Targeted online query capability;
- Bulk submission/ extract capability subject to the appropriate permissions for washing of black and grey data against white databases ;
- Accept multi-media file types - to facilitate a central repository/library of products e.g. threat assessments;
- Stakeholders remain data controllers and custodians of their own data.

The solution can be achieved via a single data repository or virtual distributed virtualisation model containing all the Financial Crime data.

The scope of this solution is to include all financial crime data, encompassing anti-money-laundering, counter terrorist financing, bribery and corruption (and politically exposed persons, PEPs) as well as fraud, and including intelligence on attack methods used.

Solution description: Operating detail

The intelligence sharing service will share the following types of data:

- Data relating to transactions either fraudulent or laundering proceeds of crime;
- Data which relates to an individual, addresses and contact data relating to an application for a product or service;
- Data which relates to both which includes devices , IP addresses;
- Intelligence Products relating to specific threats, attack methods, trends.

Three categories of data should be included in this repository:

- Confirmed and confirmed attempted financial crime data ('black data');
- Suspected, which can be varying levels of suspicion of a financial crime ('grey data');
- Compromised data (stolen data at risk of being used to facilitate a financial crime) .

The data will be used for the prevention, detection, and investigation of financial crime, for identifying networks of linked data entities for organised crime gangs (OCGs), for profiling of victims and mules,) for risk scoring and trend analysis:

- Prevention – High risk data entity matching to add to risk scoring both at application vetting and transaction;
- Prevention – products detailing intelligence gathered from the analysis of data;
- Detection – the matching of black/ grey data against white to identify suspect cases for investigation;
- Profiling – data mining looking for commonalities in data sets;
- Network analysis – linking common data entities to create relationships between records;
- Trends – data mining looking for comparisons of the same data between given data points;
- Investigation – Query matching pulling back all known data matching to or linked to a data entity, may be white, black or grey.

The single view of all financial crime data and intelligence can be achieved through two possible **operating models**.

A first operating model is a **distributed model standard virtualisation approach using open API**. What is meant by this is that a query is made about a 'subject' or specific 'data entity' and all intelligence known about it is displayed through a single view. This would be achieved by a capability which searches all assigned* databases and pulls back the single view. The databases are accessed via the open API (*assigned means those who are a party to the utility) The solution would need to be able to create networks from linked entities and find commonalities in data sets without a starting data reference.

Virtual databases have the advantage of utilising existing databases which already have their protocols and the data updated in accordance with those arrangements.

The disadvantage is it does not readily enable bulk ingest capability favoured by PSP and used to facilitate the identification of sleeping fraud in databases where accounts have been taken over or were not identified

The alternative operating model approach is a **single database** through which all data is gathered and made available. This could also be accessible by all other databases via an open interface (API) into the database.

The data would be shared from one database. The existing databases used for value add services could obtain the data they require through an open API e.g. come and get what they need or the data could be pushed to the other databases. Therefore one database would have a complete single view and others a subset.

If a new database was formed it would mean further duplication of data across the industry and there would need to be additional controls about updating data records from one source and then onto recipients. If utilising an existing database as the primary source, this will not extend the existing risk nor alter existing operating procedures but will create one source for interrogation and data ingest.

There would be a need for very tight security and it would become an obvious target for attack. The obvious benefit would be a bulk ingest capability.

Further work on design is required and a full evaluation of security is required before a decision can be made on the most appropriate.

Whichever solution is found to be the most appropriate, must facilitate the sharing of confirmed fraud data to existing fraud reporting groups (Action Fraud, FFA UK, CIFAS); each reporting group's data to be combined or accessed.

Governance

A flexible yet robust governance structure will be established to oversee the utility's operation, thereby ensuring appropriate participation of all stakeholder groups pursuant to the ultimate objectives of the utility as data sharing matures.

Solution Description: Delivery approach

There are three key deliverables for this solution proposal:

- A data sharing scheme which mandates the sharing of data, provides operating principles and standards. In order to ensure the accurate matching of entities and typologies, all records shared need to map to a common framework which maps out the criminal activity flow. Each typology will have an agreed set of data entities which a financial crime record needs to contain. This sets out the data entities which must be present to ensure the record can be identified as the crime type and the proportionality for the sharing of the data. There will need to be a data dictionary that describes the meaning for each data entity held within the each typology. - Timescale 12 months;
- Identify candidate solutions which meet the business requirement within the current infrastructure, identify the gaps and providers to meet these. - Timescale 12 months (concurrent);
- Robust enabling Legal framework- current legal barriers identified, evidenced and clarity provided or legal changes made to POCA (Tipping Off), DPA (GDPR) removing the risk of PSP being liable for breach of the law and subsequent fines. - Timescale 24 months (concurrent).

It is suggested that the UK's new financial services trade association (New TA) be the place to lead and deliver this solution as this mirrors existing work which covers the future data sharing model for Fraud but should be extended to include the whole of financial crime data sharing in line with the new remit of the New TA. This would need to be supported by the regulator and Home Office to agree the scheme and remove the legal barriers.

Benefits

This solution proposal would deliver benefits in the following areas:

1. Reduction in operating costs associated with payment fraud: Financial crime and fraud intelligence/ data sharing would allow better early detection of fraud patterns at a lower cost, therefore reducing financial services' operating costs associated with payment fraud detection and investigation and leading to a higher success rate in prosecutions;
2. Decrease in economic losses associated with payment fraud due to earlier detection: Financial crime intelligence data sharing would allow better early detection of fraud patterns and fraudulent accounts, thereby reducing the number of instances of payment fraud and the associated economic losses for customers and banks;
3. Increase in successful prosecutions from police/CPS from existing resource levels, better intelligence to support investigations: Better awareness of payment fraud schemes through financial crime intelligence sharing would result in fewer instances of payment fraud and therefore lower costs for the police/CPS associated with prosecuting banking fraud cases;
4. Wider socioeconomic benefits and redistribution effects: Reduction of banking costs, prosecution costs and economic losses can be redistributed in the economy through increased investment and consumption;
5. Reduction in operating costs for anti-money-laundering from better detection of mule accounts: The early identification of money laundering accounts through the cleansing of data bases and sharing of suspicious data would reduce the costs in new account openings for accounts which are not actively used as the PSP intends;
6. Increased confidence and trust by users of the payments system and PSPs: A range of stakeholders and customers hold a view that the industry participants do not do enough to tackle fraud and financial crime carried out across the banking/payment systems.

Costs

The principal cost areas for this solution proposal are summarised here:

- Specialist Resource to develop the scheme, operating principles and framework;
- Legal advice to build the necessary legal agreements and frameworks;
- Building of interfaces for API at PSP or solution providers;
- Security advice for agreement for any security codes of conduct for the users of the solution;
- Set up / implementation/ delivery costs;
- Ongoing operational costs for suppliers or database housing.

It is not possible to provide specific cost estimates until further work has been undertaken to define the most appropriate design and whether this is new or builds upon existing solutions.

Existing services or in-flight initiatives

- Counter Fraud Defence Alliance (CFDA) – confirmed fraud (DWP/HMRC/ IFB/ Banks). The Cabinet Office is working with public and private sector partners to develop the business case for a Counter Fraud Defence Alliance. The CFDA vision proposes the bringing together of confirmed fraud data from a range of public and private sector organisations to enable them to check customer records and new customer applications against this data. It is anticipated that over time the partners within the alliance will extend to other government agencies. The banking industry has agreed to share its data with these other sectors via this route;
- The National Fraud Intelligence Bureau (NFIB) 'Know Fraud' system already receives confirmed fraud data and this will need to continue with any future solution.

Trusted KYC Data Sharing

Problem Statement

Know Your Customer (KYC) is the due-diligence and regulations that payment services providers must perform to identify their customer and ascertain relevant information from them to perform business with them. KYC controls are designed to prevent identity fraud, money laundering and terrorist financing. While the need for the control is understood and accepted, its current method of implementation is costly to operate, contains significant duplication of work and has negative impacts to both customers and payments service providers (PSPs).

Indeed a number of initiatives have come to market in recent years offering PSPs the opportunity for greater industry collaboration and the ability to retrieve customer information related to activities such as on-boarding.

A logical case exists for a sharing KYC data to provide greater transparency and thus risk reduction, to increase the speed of customer on-boarding and transaction execution, and to reduce KYC efforts for both customers and PSPs.

This solution assessment summarises how an industry KYC shared service can address the problems identified. It is recommended that an industry KYC shared service is created that is governed by an industry body linked to relevant public authorities. This governing body should commission the shared service from competitive providers to meet the needs of participating PSPs and deliver on objectives to tackle financial crime.

Current Detriments

Currently, each PSP must collect, classify and verify KYC information based on the nature of the relationship that customer has requested and the type of customer. This data is collected at the point of customer on-boarding and must be revisited periodically depending on the on-going risk posed by the relationship and the observed customer activity.

The implementation of KYC within PSPs leads to significant duplication of efforts as KYC information collation process must happen for each PSP and customer relationship that exists. A customer will provide KYC information to many requesting PSPs and different PSPs will ask the same customer for KYC information. In addition, KYC processes take time for the customer to undertake and unless correct information is available it can delay genuine business activity.

The problem is compounded further when considering the international domain where KYC information is needed to mitigate an AML (anti money laundering) or Fraud risk relating to a customer or Beneficiary that originates or is domiciled outside the PSP's country footprint. Obtaining and validating effective KYC information in such situations can be difficult if not impossible to achieve.

The problem is also complex and costly to address; to obtain sufficient KYC information may require the orchestration of multiple external data sources and systems for the onboarding, compliance and ongoing maintenance operations. The environment within which these must be implemented is however fairly volatile where regulatory requirements continue to evolve and new data sources and systems become available to the market. Implementing and maintaining appropriate systems can be costly.

The solution proposal set out here aims to address the issues and detriments relating to KYC that were identified in the Triage report in February:

- Insufficient reference data and lack of knowledge share results in gaps in preventing financial crime: fraud, money laundering, terrorist financing, bribery and corruption;
- Switching to a new bank, or establishing a new relationship with another bank, means re-doing checks for KYC, anti-money-laundering (AML), anti-terrorist financing;

- Banks cannot make fully reliable risk decisions on 3rd-parties as they cannot be 100% sure of identity and information about them;
- Banks cannot comply easily with KYC, AML, anti-terrorist-financing requirements on their own customers, or on 3rd-parties;
- Lack of understanding of ultimate beneficiary owner (UBO) and robustness of KYC;
- Cross border payments being made under the disguise of domestic payments ('Hawala'-type payments), give consumer safety issues, and money laundering opportunities.

Our Solution Proposal: Description

The solution needs to provide a mechanism for sharing KYC data supporting identification and verification; providing a significant benefit by minimising the duplication of this effort between member Banks or PSPs and improving efficiency where a member can rely on another organisation's collection & verification of the customer data, where the other organisation has processed the contact to the agreed standard. The initial scope is business customers, both SMEs and corporates.

The solution is required to provide a method of sharing customer information among PSPs and other participants in such a way that AML and KYC checks would require less resource-intensive internal processes for many PSPs. The payments community should engage with the wider Financial Services industry and authorities to advocate a common KYC approach utilising the sharing of KYC data between PSPs and ultimately extending the sharing of data beyond KYC.

The solution must support:

- The collection and classification of KYC data for business customers, according to an agreed set of standards, with the ability to update customer details as the need for update is recognised. Classification to extend to filtering the data stored to ensure that data is only exchanged when material to the need of the other PSP with the ability for the customer to specify that certain data attributes, e.g. phone numbers, are not to be shared;
- The auditing of the creation of the data together with any subsequent updates;
- The storage of data within the repository with an associated status indicating the 'integrity;' of the data stored, i.e. Awaiting Verification, Verified;
- Data sharing including the transmission, using industry recognised encryption techniques, of such data between participating PSPs. A related assumption being that permission from the customer to share the data in accordance with the licence of their PSP is implicit, i.e. no specific permission is required for each PSP requesting the data;
- An Access Control function ensuring that the organisation requesting use of the Solution is permitted to do so;
- The use of up-to-date and proven new technologies leveraging digitising Identity and its Access Management functionality. Access initially to be provided to all organisations, in payments and wider Financial Services;
- Data Compliance and controls with regulatory updates applied;
- A low cost of entry ensuring that the solution is accessible to medium-sized and smaller PSPs.

For members to join the service they would agree to a minimum set of standards when handling data provided by the service.

Solution description

The working group has proposed two options for member banks or PSPs:

Solution A: Sharing Data Solution

The member organisations retain all of the responsibilities for understanding and process checks on existing customers and prospective customers and will continue to hold the KYC data for their customers. On request, with sufficient entitlement safeguards, the member organisation can send customer data to the requester. The solution does not preclude a central service to manage the sharing.

Solution B: Shared Service

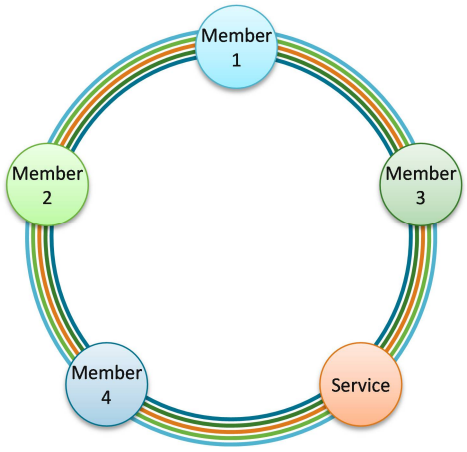
The member organisation share changes to the customer data with the industry shared service where, with sufficient entitlement safeguards, the data can be shared with other member organisations. Importantly in this approach the shared service will independently complete customer checks, verifying and classifying all information.

For either option, the solution should be industry governed, support a consistent level of data format and standards, and enable various data-usage permissions and rights.

Solution A: Sharing Data Solution

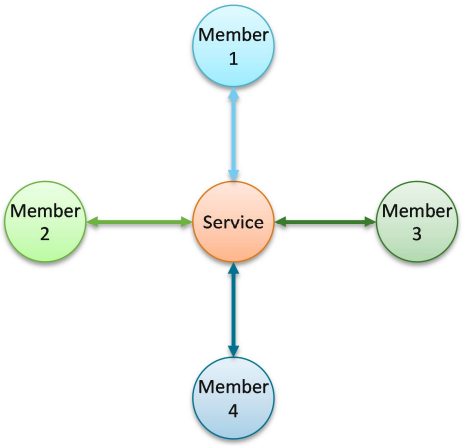
Solution Option A proposes a distributed model whereby the KYC data is stored by the initiating PSP and published to other members either directly or via a central service hub. (The two diagrams below represent two technical approaches for this solution, where both enable the sharing of KYC information held by the customers' PSPs).

Direct Sharing Architecture



Members collect, verify and classify KYC data from a variety of approved sources. On completion of the KYC process the data is published to both the members and the Central Service.

Hub Sharing Architecture



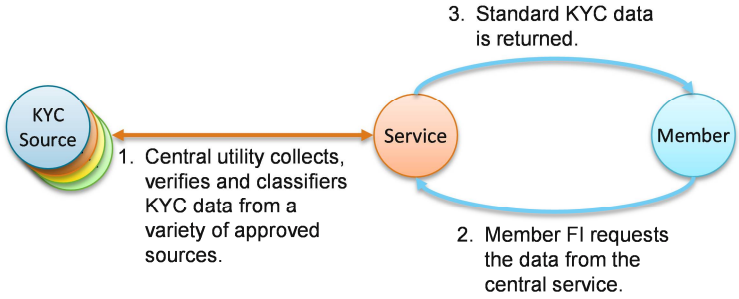
Member collects, verifies and classifies KYC data from a variety of approved sources. The KYC data is passed through the Central Service which, on completion shares the KYC data with other members.

This solution proposes that KYC information for business customers is held by the initiating PSP but shared amongst members using a subscription model providing for KYC data and identity to be shared, on creation and updates, amongst member PSPs. This architecture could be designed in different ways: one possibility is a direct sharing model (the diagram on the left) where the service along with the participating PSPs receive the KYC data, and another option being a hub solution where the KYC data is created by the initiating member and passed to the central service for transmission to other PSP Members. In either architecture other PSP members may have to supplement time-limited KYC checks if the data is stale.

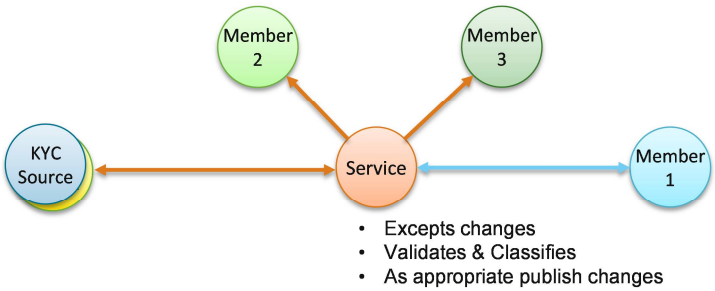
The service in this case will provide administration and governance services. The administration service will include the vetting of candidate members as well as activates such as billing.

Solution B: Shared Service

The solution proposes an industry shared service involving a central repository that stores the data required to support a PSP's KYC procedures for business customers.



The solution actively carries out KYC checks against participants' clients and prospective clients. The solution will source data and use the services from multiple vendors. The KYC information is stored centrally at the shared Service where participant PSP's can request data. Updates and other additional information can subsequently be made by the initiating PSPs or other PSPs that have 'gleaned' more information in the course of doing business with the customer.



The participating PSPs would publish the change to the central service where it would be validated, classified and published as appropriate. This would give the central repository the ability to withhold change identified as potential fraud. With the centralised repository, data returned could be restricted to the set the participant is permitted to access. Some KYC data is time limited and the service could collect this in real-time upon the request. The data would be returned in a secure block that only the member would have the keys to view. Essentially the functionality would be the same functionality as Solution A where the data is published via a central service with additional KYC functionality.

Solution B will also provide administration and governance services plus a service to carry out the KYC activity.

Solution Description: Delivery approach

Both solutions provide the ability to share KYC data, it is only the source of the KYC data and where it is stored that will differ. In both cases many PSPs will benefit from the existing checks and remove the need to collect some of the KYC data.

One aspect worthy of note is that the two solutions should be considered as an evolution in that Solution A could be adopted first and after a period of time a migration project could be initiated to adopt the Solution B approach (this aspect to be an important question in the RFP). To illustrate this further:

- Both solutions provide the ability to share KYC Data, it is only the source and stewardship of the KYC Data which differs. In both cases many PSPs will benefit from existing checks and remove the need to collect some of the data;
- Our current research into providing a solution to address the KYC for the SME market indicates that sharing of data in a controlled and structured format is recognised as an initial step. This allows both the public and sensitive party data to be shared through the stewardship of PSPs.

The initial adoption of the 'Sharing' Option A also enables:

- Data privacy requirements to be more easily managed as GDPR impacts on option B are unclear at present;
- The customer to maintain and evidence their data and provide approval of stewardship more easily than to the central utility used in Option B;
- Technologies to be leveraged faster as they come to market to ensure the currency of the solution;
- Enables new starters to 'on-board' easier as less Industry Testing is needed for Option A;
- Allows innovation services to provide commercial offerings to enhance the objectives of the KYC financial crime and ease the account opening process by offering a faster time to market than the utility option B.

An additional point for consideration going forward as a future enhancement is enabling the customers (e.g. SMEs) to input/update their own KYC data thereby giving them the incentive to keep their KYC detail up to date.

Functional elements of the solutions include:

- The organisation data is linked to the individual, but the organisation or other individuals cannot access the individual's data;
- Data is held in an encapsulated structure;
- Fragments of the structure can be unlocked and viewed;
- It is envisaged that updates to the data will always be via a PSP Member;
- The service will be governed by the industry.

The following tables provide a tabular view of the features/services offered by each solution allowing a side by side comparison.

Services offered by the solution include:

	Solution A	Solution B
Central Service to provide Governance Control	✓	✓
Central Service to provide billing capabilities	✓	✓
Central Service to provide ID&V capabilities for individual and organisations	✗	✓
Central Service to update and correlate core information from public sources	✗	✓
Central Service to collect and respond with KYC information of a request and regular basis.	✗	✓
Central Service to publish changes or alerts against	✗	✓

Technical elements of the solution include:

	Solution A	Solution B
The record needs to be held in a secure immutable way – an approach would be to hold this in Block Chains where the scheme and the individual have the keys	✓	✓
With the option leveraging "Distributed Ledger" principles.	✓	✓
Enterprise functions i.e. Reporting, HR, Billing, etc	✓	✓
Processing various formats including structured and unstructured data	✗	✓
Rules, workflow, and Events for processing the information	✗	✓

For the industry service to be successful, the standards of operation should be centrally governed (e.g. by an industry body subject to regulatory oversight), while enabling competitive providers to bid for implementing and operating the service on fully commercial terms, provided they satisfy standards and governance rules. The governance would monitor adherence to standards and rules, and include responsibility to mitigate the risks of abuse, fraud and security issues.

Given the diverse nature of payment providers, it is important that the cost implications to payment providers are to be affordable particularly to those operating at smaller scale. The service should be free for the providers of information, e.g. asset managers, hedge funds, corporates, whereas the consumers of information would be charged fee which could be either a flat fee or combination of license fee and variable fee.

Timeframes for the initiative from inception to implementation development are expected to be in the mid-term, i.e. three to five years while the IT build element is estimated at 2 years.

Benefits

The solutions have both been identified in providing the following:

1. Reduce the ability for bad actors (i.e. criminals) to open accounts and execute payments/move money
    - Reduced ease of funding for org crime gangs, for terrorism;
    - Catch more bad actors/ bad transactions – and let fewer bad actors/transactions slip through.
2. Improve the experience for good actors (good customers)
    - Faster processing / service (when everything goes through OK);
    - Less effort and cost in supplying the information that PSPs request;
    - Fewer delays due to being delayed for further checks - 'false positives' (or being prevented altogether).
3. Greater efficiency / reduced operational cost for PSPs (including account opening, transaction execution, regular KYC refreshes)
    - Cost savings for established PSPs; more effective process;
    - More affordable entry point for medium/small PSPs and new entrants looking to expand their range of services.
4. Capability to use of data can be monetised and a market can emerge
5. Standardised, more controlled approach across industry
    - Easier and quicker to introduce changes to KYC requirements to deal with new risks, intelligence;
    - More dynamic AML risk monitoring across the industry and reporting suspicious activity.
6. Wider society benefits
    - Harder for organised crime gangs (OCGs) to operate – e.g. drugs, people trafficking etc;
    - Harder for terrorist organisations to operate;
    - Harder for sanctions-targeted regimes/ countries to operate;
    - Law enforcement authorities, and the public, have higher confidence in role of PSPs.

In addition Option B is designed to have the benefit of reducing a PSP's operating costs associated with account opening and KYC refresh, as well as being able to validate data against a central store before publishing. Whilst Option A would have few benefits in terms of efficiency savings it would represent a cheaper and a simpler option.

Costs

The Build costs for Option A are estimated to be £20m to £40m while Option B build costs are estimated at £28m to £56m.

Run costs are estimated at £4m to £8m for Option A and £24m to £48m for Option B (the higher cost reflecting the BPO approach for Option B).

Enhancement of Sanctions Data Quality

Problem Statement: Summary of the Issues this addresses, and their priority

A sanctions list entry with detailed, clean and structured data enables more accurate detection and thus fewer false positives (stopping or delaying 'good' customers). Conversely, a poor quality entry can cause many false positives that i) result in additional work, and ii) can cause operational problems and unnecessarily delay genuine customer business. More importantly however, efforts by Financial Institutions to (FIs) to tune their sanctions screening systems in order to overcome poor quality sanctions-list entries increase the opportunity to generate false negatives (allowing 'bad actors' to slip through the process).

The issues are recognised in the FSA report from April 2009 that flags the quality of some 'identifiers' on the HMT list:

"'Identifiers' are the personal identifying information on the HMT list used by firms to screen their customers. Identifiers, on the HMT list, that are too general make it difficult for firms to identify matches with their customers. They also increase compliance burdens significantly. While firms acknowledge there has been progress in this area, they remain concerned that some of the identifiers on the HMT list are too general."

While FSA report refers to HMT list, similar principles may be applied to other sources and additionally complexity increases by cross-border and cross-regulator inconsistencies.

When identifying an individual or an organisation, relying on just their name information is typically not enough. There are a number of common names used globally for people and companies, which correlates to the distribution of names populated on sanction lists. Therefore organisations need 'secondary identifiers' to reduce the number of matches and help validate people in their due-diligence process. The industry's requirement is to improve the integrity of well-populated secondary identifiers, thereby to help uniquely identify an individual or organisation.

While significant effort goes into the intelligence gathering to capture data for Sanctions Lists, the value that can be extracted is somewhat constrained by the failings in data management during publication. Examples gathered from our Working Group where corrections were required:

- Entity added to the list without a unique ID number;
- Happens frequently: 7/3/2016, 19/1/16, 10/12/2015, etc. Numbers have lost leading all leading zeros (effect from converting from a text field to integer / number field);
- Entity added without a prime name or ID included;
- Name Jameel inserted into the Title field instead of the name field;
- Carriage returns inserted within the middle of two records –lines 628, 630;
- TXT version updated but CSV remains the same;
- When requesting the data file an old version of the file is returned by the server (issue now fixed by HMT with new server infrastructure);
- Data file change with no notification –change was in error and subsequently reversed;
- Multiple date of birth entries;
- Missing/Inaccurate gender information.

The reliance on well-populated good quality data and data management is imperative when it comes to client on-boarding and payment screening. Compliance teams need this data to aid in making their judgements when carrying out customer due diligence (CDD) and investigation of screening hits. Without this data the risk is higher numbers of false negatives ('bad actors' not being stopped) and operations being slowed down due to high volumes of false positives (screening hits on good actors, which take time to investigate and often require further data submissions by the customer).

Solution Description

Our proposal is for the UK payment industry to work closely with HMT Office of Financial Sanctions Implementation (OFSI) to deliver an improved approach for collecting and managing data for sanctions screening to address the detriments identified. This will encompass the quality of the data in sanctions lists and the approach for managing that data between the authorities and payments industry.

A. Data Improvements

- Engage with HMT to improve the population of accurate data within sanction lists for both primary and secondary identifiers (e.g. more verified passports/ NI's etc.). This could be carried out by HMT increasing the research team and sources of data to ensure more complete sanction profiles carried out by the sanction list provider;
- Payments industry to engage with HMT to perform a sanction data assessment to detect issues for existing unverified data and for HMT to fix problems identified.

B. Process Improvements

- Industry work with HMT to create a single common Sanctions list for the UK with consistent format and structure, and effective data management for storing and distributing the list;
- PSPs to collaborate to define common standards and industry practices regarding use of attribute information for screening investigations;
- PSPs to collaborate with HMT to share common best practices and challenges as a way to improve data quality.

C. Sectoral and Dual Use Goods List

In addition to the need to improve the sanctions lists used in the UK, an additional detriment was identified concerning sanctions for sectoral and dual-use good. Currently UK regulatory bodies provide regulatory requests to PSPs regarding screening requirements which are not included in the HMT list. Examples include sectoral sanctions (e.g. Chimera) and dual use goods. Current practice from PSPs is to take the untrusted requests and manually construct screening lists using the data provided.

- A proposed solution is for PSPs to collaborate with authorities and third parties to use the improvement process described above to create a new list to include these regulatory requests.

The solution proposals above assume that a standard for how data is captured accurately (identity and verification) by PSPs for consumers will improve the matching capability against sanction lists, and this standard will be delivered by the Forum's proposal for Identify, Verification, Authentication and Risk Assessment.

UN's Advanced Sanctions Data Model

In addressing the solution proposals set out above, the industry should support HMT in assessing whether there is a case for the UK to adopt the UN's Advanced Sanctions Data Model, or whether the UK should continue to use its own sanctions list and data model tailored to the UK market environment. The approach for international payments transactions will need to be fully addressed alongside the requirements for domestic transactions.

- An Advanced Sanctions Data Model has been developed by the UN 1267/1988 Security Council Committee which OFAC in the USA have implemented and UN will implement by June 2017 (on current plan). The rationale driving this model was to enhance the quality of the Sanctions List entries and thus their effectiveness in use. The model provides a linguistic basis for the storage and classification of Sanctions entity information and covers different scripts, transcriptions and cultural variances. Adopting this model would position the UK to address current inconsistencies between differing issuing bodies, and the roadmap moving forward could be managed as a global community.

Scope

The scope of the improved sanctions list will be for all entries, encompassing individuals and companies/ organisations.

The requirements for sanction screening extends beyond PSPs, this proposition is focused on PSPs requirements only. If further work is required to create a common approach with other types of organisations, then the PSR should contribute to these discussions to ensure the payments fields is well represented.

The solution must be inclusive to all PSPs, regardless of size, channel and payment services they provide.

Cost Benefit Analysis (high-level)

Benefits

Adopting this enhanced approach to sanctions data quality and data management for the UK would not only enable improved detection capabilities for FIs, but also help eliminate the frequent errors that find their way onto the lists.

If adopting the UN's Advanced Sanctions Data Model, promoting this model internationally would not only aid detection quality domestically, but also help the transfer of Sanctions Entity information between states.

Adopting this standard would greatly support maintenance and universal use of the data file over time.

The benefits from improving the data quality of sanctions fall in the following areas.

- Reduce the ability for bad actors to open accounts and execute payments/move money
    - Reduced ease of funding for org crime gangs, for terrorism;
    - Catch more bad actors/ bad transactions – and let fewer bad actors/transactions slip through;
    - Increased accuracy and speed in identifying matches for sanctions screening.
- Improve the experience for good actors (good customers)
    - Faster processing / service: If the CDD process gains more confidence (through improved sanction data) this in turn will improve the turnaround time to on-board a new client and thus improve the experience for the customer;

- Less effort in supplying the information that FIs request;
- Fewer delays due to being delayed for further checks (or being prevented altogether) – 'false positives'.

- Greater efficiency / reduced operational cost for FIs (…account opening, transaction execution)
  - Cost savings for established FIs; more effective process;
  - Lower barriers to entry for medium/small FIs and new entrants looking to expand their range of services;
  - Increased confidence in CDD: a greater depth of accurate secondary identifiers (e.g. DOBs, countries, passports etc.) provided by the sanction list, compliance teams have more certainty when carrying out due diligence of new parties;
  - A greater level of good quality data, compliance teams are aided in prioritising good quality matches that have a significant amount of supporting and matched data.
- Standardised, more controlled approach across industry, and sharing best practices
  - Easier and quicker to introduce changes to Sanctions requirements to deal with new risks, intelligence;
  - Better highlighting of existing issues in the data;
  - Sharing methods within the industry on managing screening-matches.
- Wider society benefits
  - Harder for organised crime gangs (OCGs) to operate – e.g. drugs, people trafficking;
  - Harder for terrorist organisations to operate;
  - Harder for sanctions-targeted regimes/ countries to operate;
  - Law enforcement authorities, and the public, have higher confidence in role of FIs.

Costs

The costs associated with change to the HMT list is to be in line with the general cost associated with modifying a sanctions list.

Implementation costs for PSPs to implement the new sanctions list will be in line with the costs they will face when OFAC changes their list to the new Advanced Sanctions Data Model. Further research is required to estimate the implementation cost at this point.

Existing or In-Development Solutions

OFAC implemented the Enhanced Sanctions Data Model in 2016 and the UN is currently initiating the project to implement within the next 18 months.

https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150105.aspx

There are a number of data vendors that focus on improving the quality of sanction list data. This includes improving data accuracy / validity, ensuring consistent formats and enhancing/ completing profiles. Some of the vendors in this list management and quality space are:

- Dow Jones – provide an enhanced data file: Dow Jones Watchlist, which consolidates a number of Sanction lists, PEPs and Adverse media records with improved data quality and completeness;
- Thomson Reuters – provide an enhanced data file: World-Check, which consolidates a number of Sanction lists, PEPs and Adverse media records with improved data quality and completeness;
- Innovative Systems –– providing FinScan List Management service for improved data quality for specific sanction lists;
- Other Similar Vendors:
    - RDC
    - World Compliance

People Involvement and Action

HMT – implement Enhanced Sanctions Data Model. The Office of Financial Sanctions Implementation (OFSI), part of HM Treasury, ensures that financial sanctions are properly understood, implemented and enforced in the United Kingdom.

(https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation)

Customer Awareness and Education

This paper provides an overview of the current financial crime education and awareness (E&A) landscape in relation to financial fraud, and sets out the Forum's view on how this can be strengthened as part of the Forum's strategy for collaboration in payments services in the UK.

It is important to note that many organisations provide education & awareness advice; some directly to their customers and others to wider audiences, for example many third-sector organisations undertake research and run fraud and scams awareness campaigns with particular focus on their target audiences. These organisations can be trusted messengers to communicate with hard to reach audiences, particularly the most vulnerable.

Acknowledging the busy landscape, the City of London Police, Economic and Cyber Crime Unit formed a multi-agency campaign group. The group aims to coordinate the development and delivery of Education and Awareness activity and work towards simple, clear and consistent messaging so that audiences are not ultimately left confused. This co-ordination needs to encompass distinct messages to specific segments of the public (consumers and businesses) delivered cross a range of communications channels. It also provides a mechanism for cross industry collaboration with the ambition of contributing to better use of finite resources in delivering these campaigns.

There is a wide range of types of financial-crime and fraud that criminals use and which payments end-users (consumers, businesses, charities etc.) should be aware of. We have documented the priority areas in the supporting tables, liaising across the PS Forum's Financial Crime Working Group. While the majority relate to fraud threats, we have considered the full scope of financial crime, for example we cover the issues of opening or operating mule accounts as a means of money laundering:

- Table 1 below identifies high level campaigns that are already being undertaken to mitigate the effect of the priority threats;
- Table 2 below outlines the key messages and advice being delivered through existing E&A activities.

The Working Group considers that most of the priority messages for current fraud / financial crime threats are already covered by existing E&A activities within the industry, and therefore has concluded that the priority therefore is for the payments industry and community to engage and support existing campaign activities and planning. Building on this existing situation, the Working Group proposes the following:

i. A review of existing plans is undertaken on a regular basis to identify and agree changing financial crime threats to end-users and therefore campaign priorities. The industry would thereby enable a forward-looking component to its E&A plans with consideration for how best to pre-empt small but growing fraud type (modus operandi, MOs) through early advice and messaging;

ii. Regular reviews are carried out of the effectiveness and impact of recent campaigns. (The evaluation toolkit developed as part of the UK Financial Capability Strategy may be useful in evaluating effectiveness and help to build evidence of what works which can then be applied to future activity);

iii. The industry continues to collaborate extensively in order to improve the visibility and cut-through of key messages (to reduce issues of overlap/ duplication where too many campaigns are running in a given period), and to maximise campaign effectiveness from the finite funding available in aggregate;

iv. That the industry's oversight and governance of this collaborative campaign activity is a responsibility of the new trade association, working closely with law enforcement and other public authorities.

Table 1

This table sets out the current financial crime priority threats where the Working Group advocates there should be customer education and awareness activity. The table also shows the existing E&A activity under way and the lead organisation.

Priority Threats	**Existing E&A activity/Lead organisation**
Social Engineering – several MOs employed • Vishing • Courier fraud • Phishing • Smishing • SIM swap • Investment scams • Competition scams • Romance scams • Auction site scams • Invoice fraud • CEO Fraud	Take Five to stop fraud – Financial Fraud Action UK (FFA UK) & partners ScamSmart campaign – FCA – investment fraud focus
ID Fraud	Not with my name - Cifas/CoLP
Money Mule Recruitment	Take Five to stop fraud - FFA UK & partners
Fraud associated with accepting card payments online	FFA UK/Cyber Streetwise (Cyber Aware)
Malware, poor online safety behaviour and securing your online devices • Mobile Banking • Mobile payments (mobile technology)	Cyber Streetwise (Cyber Aware)/Get Safe Online
Distraction card scams	Prevention advice via bank websites

Table 2: Priority Financial Crime Threats and Key Messages

This table shows the key messages for education and awareness, for each of the priority threats identified.

Threat	Audiences	Key Messages
Social Engineering Scams Vishing Courier fraud Phishing Smishing SIM swap Invoice fraud Investment scams Competition scams Romance scams Auction site scams	Consumers (all) Businesses	**Vishing / Courier Fraud** Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers and other officials or companies in a position of trust. Often the fraudster will claim there has been fraud on your account and that you need to take action. How to protect yourself: Your bank or the police will never: • Phone you and ask you to reveal your security information (for example your 4-digit card PIN or your online banking password) or request that you enter the information into a telephone. • Ask you to withdraw money to hand over to them for safe-keeping. • Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name. • Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud. • Ask you to purchase goods using your card and then hand them over for safe-keeping. If you are given any of these instructions, it is a fraudulent approach. Hang up, wait five minutes to clear the line, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud. If you don't have another telephone to use, call someone you know first to make sure the telephone line is free. Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller

		Phishing / Online Phishing is a method used by fraudsters to obtain personal information from victims via email by impersonating a trusted person or familiar company. The email may contain malicious attachments or website links in an effort to infect the computer so that information such as passwords and personal information can be collected by the fraudster. The information collected will be used to commit fraud crimes such as identity theft and bank fraud. How to protect yourself: Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software: check your bank's website for details Only shop on secure websites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser Always be suspicious of unsolicited emails that are supposedly from a reputable organisation, such as your bank or the tax office and do not click on any links in the email Never share your personal or security information on a website that you have accessed by clicking a link in an email or text. **Smishing** 'Smishing' is very similar to 'phishing' but instead of using emails the fraudsters are using SMS text messages to your mobile phone. There are a number of variations on the scam which often starts with the fraudster sending an unsolicited text message within some cases the SMS contains a link, which if accessed can load malware onto your phone but more often will take you to a site where you are asked to enter personal and security information which will be used to defraud you. In most recent cases the customer is sent an SMS with a request to call a fraudulent number. When the number is called they are tricked into divulging security and possibly card details. A fraudulent transaction is then processed using the information provided and because the fraudster still has the customer on the line the customer is duped into releasing funds when they are asked to respond 'Yes' to a genuine SMS sent by the bank to validate the payment. • If you receive an SMS text from a sender that you do not know and are not expecting do not open any attachments or click on any links • If you receive a text from your bank asking for you to telephone them check the number, if in doubt phone the number on the back of your bank card or statement.

		SIM Swap This is when a fraudster cancels the SIM card linked to the victim's mobile phone and activates a new SIM card which is under the fraudster's control. This will allow the fraudster to re-route any calls and messages from the victim's phone and usually follows a phishing attack so that the fraudster already has the victim's bank account information: • If you stop receiving calls or text messages unexpectedly check with your phone operator immediately • Never disclose your PIN or internet mobile banking passcode in response to a SMS text - you would never be asked for the full four digit code or full internet/mobile banking passcode over the telephone • Be careful of the information that you add to social media sites such as your date of birth or maiden name and if possible use a different email address for social media than you use for contact with your bank and other sensitive applications. **Invoice Fraud** Ensure that all staff who process invoices and who have the authority to change bank details are vigilant. They should check for irregularities including changes to invoiced amounts Changes to supplier financial arrangements should always be verified with that supplier using their established on-file details. When a supplier invoice has been paid, it is good to inform the supplier of the payment details made, including the account the payment was made to. Check company bank statements carefully. All suspicious debits should be reported to your bank. If you are suspicious about a request, ask if you can call back. Do so using their on-file contact details to establish if they are the genuine supplier of the services. Perpetrators of fraud often conduct extensive online research to identify suppliers to particular companies. Consider if it would benefit your company to remove this information from your website / other publicly available materials Never leave sensitive materials such as invoices unattended on your desk

		Establish a designated point of contact with suppliers to whom your company makes regular payments. Raise all invoice issues and concerns with this person Consider a more vigilant strategy for larger invoices. A meeting with the supplier involved will ensure the payment is made to the correct bank account before the transfer is made Look carefully at every invoice. Counterfeit invoices won't often withstand scrutiny. Compare suspicious invoices with those you know are genuine Logos on counterfeit invoices often contain account details to which the payment should be made Be vigilant for amendments to contact numbers and email address on company invoices. Amendments to these may be so minor that they are difficult to spot Never accept invoice changes or new payment instructions via emails unless you first contact the designated contact that you know, often email accounts are hacked or fake email accounts that have one character different are used e.g. John.smith@ / John.sm1th@ **Investment scams** Investment fraud is often sophisticated and very difficult to spot. Investors are pressurised, into making purchase or sale decisions based on falsified information, often from an unsolicited phone call. Fraudsters can be articulate and appear financially knowledgeable. They have credible websites, testimonials and materials that can be hard to distinguish from the real thing People offering high risk investments or scams will often cold call. The firms that the FCA regulate are very unlikely to contact you in this way about investment opportunities. If you're called about an investment opportunity, the safest thing to do is hang up There are ways that callers can pretend they aren't cold calling you. They may refer to a brochure or an email that they have sent you. That's why it's important you know the other tell-tale signs that suggest the investment opportunity is likely to be very risky or a scam. Callers may do one or more of the following: • Make contact unexpectedly about an investment opportunity. This can be a cold call, email, or follow up call after you receive a promotional brochure out of the blue • Apply pressure on you to invest in a time-limited offer, for example, offer you a bonus or discount if you invest before a set date, or say that the opportunity is only available for a short period of time

		• Downplay the risks to your money, for example talking about how you will own actual assets you may sell yourself if the investment doesn't work as expected, or using legal jargon to suggest the investment is very safe • Promise tempting returns that sound too good to be true, for example, offer much better interest rates than those offered elsewhere • Call you repeatedly and stay on the phone a long time • Say that they are only making the offer available to you, or even ask you to not tell anyone else about the opportunity. If you recognise any of these, you have every reason to be suspicious If you have already or are thinking about transferring your pension, FCA strongly recommend that you do not send any more money. Find out more about pension scams on The Pensions Regulator website Not all investment opportunities offered out of the blue will be very risky or scams, but you should be very wary, especially if they are unusual investments. An investment offered to you in this way is unlikely to suit your specific needs and could be a very bad idea or a scam. It is generally best to seek out your own investment opportunities, either through research or with the benefit of impartial advice from a financial adviser **Competition Scams** A competition scam is when a victim is told that they have won a competition or overseas lottery and in order to 'claim' the prize which is usually something of high value, they must send money to cover a booking fee or the tax element on the overseas lottery prize money. • If you are asked to pay an up-front fee in order to receive a prize or winnings it is likely to be a scam. • If you do not remember entering the competition be sceptical, if you have received a letter try searching the exact name quoted on the internet to see if there are any references to a scam • If you believe the competition/lottery to be a scam do not respond, fraudsters will often use personal information they have gathered to play on the emotions of potential victims.

		Romance Scams These scams are often perpetrated through lonely hearts sites but can also occur as 'friendships' on other types of social media. The fraudster will build up a trusted rapport with the victim over a period of time and will take advantage of the victim's compassion to extort money through deception. **Auction Site Scams** A common scam occurs when the seller asks the buyer to pay the monies due by bank transfer directly into their bank account rather than using the auction site preferred settlement mechanism, often the reason given is to avoid the site charges or provide an additional generous discount. • Read the terms and conditions of the site very carefully especially those relating to dispute resolution before making any purchase • Beware of sellers offering discounts below the bid price especially as they want to trade outside of the auction site on which they are advertising. • Always check a website is secure before entering any kind of account or card details. Look for the 'HTTPS' at the start of the web address and the padlock or unbroken key icon at the top of the page or next to the address bar.
Money mule recruitment	Consumers: Students New entrants to UK	A 'money mule' is a person that will receive funds that have been obtained by criminal activity into their account and then forward those funds to other accounts, often overseas for a commission payment. Criminals will recruit 'money mules' to distance themselves from the crime and its proceeds. It is the 'money mule' that is taking the risk because they are committing 'money laundering', which can lead to up to 14 years imprisonment if found guilty. Behaviours that put you at risk: • Responding to job adverts, or social media posts that promise large amounts of money for very little work • Failing to research a potential employer, particularly one based overseas, before handing over your personal or financial details • Allowing an employer, or someone you don't know and trust, to use your bank account to transfer money. • Opening an account in your name for someone else to use

		How to protect yourself: • No legitimate company will ever ask you to use your bank account to transfer their money. Be very cautious of unsolicited offers or opportunities to make easy money • Be especially wary of job offers from other people or companies overseas as it will be harder for you to find out if they really are legitimate • Never give your financial details to someone you don't know and trust
Fraud associated with accepting card payments online	SMEs	**Know Your Customer** There are a number of tools and techniques which can be utilised when selling online to build up a profile of your customers Many of these can be working in the background as your website accepts an order from shoppers or when they first register on your site **Get Paid Securely** An important consideration for a merchant is to gain and validate a secure means of payment from your customers for the goods or services they are purchasing In the case of payment cards, as neither the card nor the cardholder are physically present at your business, it is vital to both validate the card number is genuine and authenticate that the customer is the rightful holder of that card **Internet cardholder authentication** Verified by Visa, MasterCard SecureCode and American Express SafeKey are authentication solutions offered to retailers and cardholders to assist in making internet transactions safer from the threat of fraud Retailers enrol into the service and make enhancements to the checkout process on their website Contact your acquiring bank or payment service provider (PSP) for more information about taking payments securely and internet authentication

Malware and poor online safety behaviour and securing your online devices	Consumers Businesses	**Firewalls** A firewall acts as a barrier between you and the wider internet including trusted and internal networks. Personal firewalls are usually software-based and should be installed on each computer which connects to the internet. However, firewalls for businesses may require hardware to protect their network further **Passwords** Make your passwords stronger with three random words **Security Software** Security software such as antivirus helps protect your device from viruses and hackers **Install software updates** Software updates contain vital security upgrades which help protect your device from viruses and hackers **Create a safe wireless network** You should secure your wireless network (WiFi). Failing to do so could give someone else access to your sensitive data, including passwords or bank details, and use your network for illegal behaviour
Distraction fraud Card Scams	Consumers	When using your bank card be aware of people trying to divert your attention, perhaps by pretending to be helpful, dropping something or bumping into you so that they can take your card or cash, or find out your PIN. How to protect yourself: • Always shield your PIN when using your bank card • Always be aware of who is behind you when using your bank card and don't let anyone stand too close. • Don't let anyone distract you during the transaction • If anything about a cash machine looks suspicious don't use it. Tell a member of staff or the police

Legal Work-stream: Summary of Legal Issues arising from Financial Crime WG Proposals

Technical Standards for Identity, Verification, Authentication, and Risk Assessment

Solution in a nutshell (see pages 3 - 28 of the Solution Paper): System for digital identity, supported by a technical and governance standard (referred to below as the "PSF standard" to avoid confusion)

Legal issues arising from proposed solution; relevant legislation and guidance and possible ways in which to resolve legal issues

a) The legal issues are likely to depend on the approach which is taken to this solution (e.g. whether there is a single solution or numerous solutions) and whether use of the PSF standard is compulsory or not.

b) The PSF standard may conflict with or need to be taken into account in the existing rules and other contractual arrangements for payment systems (e.g. Faster Payments Scheme or Bacs); this could be resolved through amending the scheme rules to reflect the PSF standard.

c) It will be necessary to ensure that the PSF standard does not duplicate or conflict with other legislation, regulations, standards and initiatives which are relevant to PSPs. It should be possible to ensure that this happens during the development of the PSF standard (and ongoing reviews of PSF standard). The relevant legislation, regulations, standards and initiatives include:

   i. The EU Payment Services Directive (2007/64) (currently in force);

   ii. The Payment Services Regulations 2009 (currently in force);

   iii. The EU Second Payment Services Directive (2015/2366) (due to be implemented by 13 January 2018);

   iv. The Payment Accounts Regulations 2015 (currently in force);

   v. The EU Wire Transfer Regulation (1781/2006) (currently in force);

   vi. The EU Wire Transfer Regulation (2015/847) (due to come into force on 26 June 2017);

   vii. The Third EU Money Laundering Directive (2005/60), Money Laundering Regulations 2007 and JMLSG guidance (all currently in force) ("MLD3");

   viii. The Fourth EU Money Laundering Directive (2015/849) (and accompanying guidance and standards) (due to be implemented by 26 June 2017 and likely to be further amended by a subsequent directive, "MLD5") ("MLD4");

   ix. The EU eIDAS Regulation (910/2014) (currently in force);

   x. Existing national identity initiatives; and

   xi. The European Banking Authority's Regulatory Technical Standard on Strong Authentication (which sets out a harmonised framework intended to ensure an appropriate level of security for consumers and PSPs).

d) The legal structure for the development of the PSF standard will need to be agreed (e.g. ownership of the PSF standard, responsibility for ensuring that it is kept up to date, whether there should be consultation before the PSF standard is amended, etc.). At present, the Working Group's recommendation is that use of the PSF standard should not be mandatory. However, if the use of the PSF standard is mandatory, it will be necessary to determine how this should be implemented, how compliance with the standard will be supervised and the penalties for breach.

e) The PSF standard will need to be consistent with PSPs' data protection and privacy obligations under the Data Protection Act 1998 ("DPA") (and the EU General Data Protection Regulation (2016/679/EU) (due to come into force on 25 May 2018) ("GDPR")). This issue could be addressed by obtaining customer consent to the use of data or potentially through a FCA-mandated change requiring the provision of data. However, it may be difficult to obtain customer consent, particularly from existing customers; the GDPR requires a very high standard of consent and consent must be given by a statement or clear affirmative action establishing a freely given, specific, informed and unambiguous agreement to data processing. As a result, legislative action and/or engagement with the Information Commissioner's Office may be required to ensure that appropriate safeguards are in place and that PSPs can be confident that they are complying with their data protection and privacy obligations.

f) It will be necessary to address any cybersecurity risks and comply with cybersecurity obligations. An appropriate liability framework may be required; however, if the PSF standard allows PSPs to choose their own technical solutions, cybersecurity may only need to be addressed as between each PSP and its solution provider.

g) The PSF standard may lead to an increase in breach of mandate (or similar) claims by customers if PSPs refuse to carry out transactions because a customer's identity cannot be authenticated in line with the standard. On the other hand, PSPs may face claims by victims of fraud (e.g. dishonest assistance claims). It may therefore be necessary to establish a liability framework between users of the PSF standard (e.g. to address a PSP's liability to its customer and liability between PSPs).

h) Development of a single system could be anti-competitive; this will need to be reviewed once a preferred solution has been selected.

i) There is a risk that the PSF standard could have a particular impact on disabled or vulnerable customers or on those who are financially excluded; this could be addressed through alternative options for disabled, vulnerable and financially excluded customers to ensure access and inclusion.

j) In the case of UK-authorised PSPs offering passported services on a cross-border basis to non-UK EEA1 customers, even if the PSF standard is not expressed to be mandatory, such customers should be either allowed to benefit from the creation of a digital identity under the PSF standard or explicitly protected from discrimination or denial of services on the grounds that they cannot create such a digital identity.

Interaction with other proposed solutions: Solution 4 (Trusted KYC Data Sharing and Storage Repository): this will be relevant if the PSF standard leads PSPs to request KYC information from other PSPs about mutual customers

[1] European Economic Area

Payments Transaction Data Sharing and Data Analytics

Solution in a nutshell (see pages 29 - 41 of the Solution Paper): Creation of a pool of shared transaction data within a repository which can be data-mined to combat financial crime

Legal issues arising from proposed solution; relevant legislation and guidance and possible ways in which to resolve legal issues

a) The creation of a shared pool of data which is then data-mined raises data protection and privacy issues under the DPA (and the GDPR), in particular in relation to a customer's right to control the use of personal data and correct data.2 Data on the commission or alleged commission of an offence are considered sensitive personal data under the DPA and subject to additional protection. Whether the data provided to the repository and/or used for data analysis is pseudonymised may affect the legal considerations. Processing of data is only lawful under certain conditions,3 including if the customer's consent has been obtained; the processing is necessary to comply with a legal requirement; the processing is necessary for a legitimate interest of the PSP, except where such interests are overridden by the interests or fundamental rights of the customer which require the protection of personal data; or if it is necessary for the performance of a task carried out in the public interest.

   i. The scope of the "public interest" and "legitimate interests" test are not clear (in particular because the "legitimate interests" test is a balancing act) and so PSPs may not be able to rely upon these grounds. Although Article 43 of MLD4 provides that the processing of personal data on the basis of the directive for the purposes of the prevention of money laundering and/or terrorist financing shall be considered to be a matter of public interest under the existing Data Protection Directive (95/46), this may not be sufficiently wide to cover all of the activities under the proposed solution (e.g. data analysis for the purpose of fraud prevention may not be covered). Legislation to define the scope of the "public interest" may therefore be necessary;

   ii. Data protection and privacy concerns could be addressed by obtaining customer consent (from both new and existing customers) to the use of data. However, consent can be withdrawn, which is problematic in a financial crime context. In addition, obtaining consent may not be feasible for a PSP if the data which it wishes to share relates to a non-customer;

   iii. An alternative may be a FCA-mandated change requiring the provision of data and/or guidance from the Information Commissioner's Office on the scope of the consent requirements and how consent can be obtained to enable the proposed solution to operate;

   iv. Alternatively, legislative action may be required, but further analysis is necessary to determine this. The Home Office and HM Treasury Action Plan for AML and CTF4 states that the government intends to consider legislating to create legal information sharing gateways between private sector entities to improve AML and CTF information sharing;

   v. If customers are permitted to opt out, this option might address the data protection and data privacy issues, but could undermine the utility of the repository (e.g. it would not be possible to trace funds paid into an opted-out account);

   vi. The GDPR provides customers with additional rights, including a right to erasure (also known as the "right to be forgotten"), a right to restrict the processing of data and a right not to be subject to profiling. These rights can be restricted in certain circumstances, such as

[2] Article 41(3) of MLD4 requires regulated entities to inform new customers about the processing of data for AML/CTF purposes.
[3] This is the test under the GDPR, which is likely to be in force by the time this solution is implemented.
[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517993/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf

where the processing of data is in the public interest or pursuant to legal obligations, but the impact of these rights on the efficacy of the proposed solution will need to be assessed. Again, legislation on the meaning of "public interest" and/or to authorise profiling may be required;

vii. Article 14 of the GDPR also requires data controllers to disclose certain information to data subjects (i.e. customers) if the data controller receives personal data about the data subject from a source other than the data subject. This may place a significant burden on the repository (and potentially "tip off" criminals) and so it will be necessary to consider whether any of the exceptions to disclosure apply (e.g. because it involves a disproportionate effort or because the data subject already has the information, e.g. from their PSP) and/or whether legislation is necessary to address the issue;

b) As well as considering the impact of the DPA and the GDPR, the issue of confidentiality should also be considered. The general duty of confidentiality is likely to apply in the context of a relationship between PSPs and their customers. The general duty of confidentiality5 is only allowed in three circumstances (a) the information must be confidential, (b) the information must not be useless or trivial, and (c) it must be in the public interest to keep the information confidential. In England and Wales, banks owe their customers a specific duty of confidentiality, which applies to all the information which the bank acquires in its capacity as a bank.6 There are four broad common law exceptions to this duty: (i) if the disclosure is compelled by law; (ii) where there is a duty to the public to disclose the information; (iii) where disclosure is in the bank's interests; and (iv) where the customer has given express or implied consent to the disclosure. There is limited case law on the scope of these exceptions, so banks may need to obtain customer consent or be compelled by law before they can provide data to the repository. It has not been established whether other PSPs (e.g. EMIs and PIs) are benefit from the exceptions permitting disclosure, nor whether this approach is applicable in Scotland. If the provision of data to the repository was mandatory, the duty of confidentiality would be overridden.

c) The ownership of the data repository and the data within the repository will also need to be clearly determined, as well as any oversight and governance (including deletion of data when no longer required and dealing with subject access requests). It should be possible to resolve this as part of the creation of the repository and through the contractual framework which will need to be in place between the repository and the PSPs which supply data to it. It will also be necessary to resolve (potentially through legislation) whether the supply of data to the repository is mandatory.

d) Potential errors in the data supplied to the repository or the conclusions reached through data analysis may also raise legal issues, including the potential liability of (i) the repository to PSPs and customers; and (ii) the potential liability of a PSP to other PSPs, the repository and customers (including victims of crime). Inaccurate data and/or inaccurate conclusions drawn from data could have a significant impact on customers, so it may be necessary to give customers a "right of reply" and/or to put additional safeguards. In addition, it may be necessary to determine whether PSPs are entitled to rely on insights from the repository without taking other steps (for example, whether a PSP can decline to process a transaction because data analysis from the repository indicates that it is suspicious – or vice versa).

e) The creation of the repository may lead to claims against PSPs by customers if the PSP has refused to carry out transactions. This could be addressed through an agreed liability framework, whether contractual or statutory.

f) It will be necessary to address any cybersecurity risks and comply with cybersecurity obligations. This should be possible as part of the establishment of the repository.

[5] *A-G v Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109 at 281-282 (HL)
[6] See *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 (CA)

g) In the case of UK-authorised PSPs offering passported services on a cross-border basis to non-UK EEA customers, such customers should be excluded from the scope of the data repository unless the national data protection authorities in the rest of the EEA agree to the pooling of personal data of their nationals/residents. This issue may be further complicated by any post-Brexit settlement (or the absence of one).

h) Other legislation which may be relevant includes:

   i. The EU Payment Services Directive (2007/64) (currently in force);

   ii. The Payment Services Regulations 2009 (currently in force);

   iii. The EU Second Payment Services Directive (2015/2366) (due to be implemented by 13 January 2018);

   iv. The EU Wire Transfer Regulation (1781/2006) (currently in force);

   v. The EU Wire Transfer Regulation (2015/847) (due to come into force on 26 June 2017); and

   vi. The primary money laundering offences, reporting obligations and tipping off provisions under the Proceeds of Crime Act 2002; and

   vii. MLD3 and MLD4 (which are likely to be amended by MLD5).

Interaction with other proposed solutions: there is potential for overlap with Solution 4 (Trusted KYC Data Sharing and Storage Repository)

Enhancement of Sanctions Data Quality

Solution in a nutshell (see pages 42 - 45 of the Solution Paper):

a) Improve the quality of sanctions list entries by adopting the UN Advanced Sanctions Data Model; and

b) Introduction of new list for screening requests in relation to sectoral sanctions and dual-use goods.

Legal issues arising from proposed solution; relevant legislation and guidance and possible ways in which to resolve legal issues

a) Adopting the UN Advanced Sanctions Data Model does not raise any legal issues, although the Office of Financial Sanctions Implementation (within HM Treasury) may want to agree this initiative at EU level to encourage consistency.

b) Introduction of new list for screening requests in relation to sectoral sanctions and dual-use goods raises a number of legal issues, including the legal basis for implementing such a list, the right of listed parties to challenge their inclusion on the list and the potential penalties for failing to stop payments and business relationships relating to listed parties or goods. It may be appropriate to ensure that PSPs with no sight of products or services purchased or without the ability to stop payments in real time do not incur liability and/or that other defences are available to PSPs. A new list would need to be implemented through legislation. The interaction between any such legislation and the existing sectoral sanctions legislation7 and export controls legislation8 (which do not require screening to be carried out) would also need to be considered.

[7] Council Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (as amended) and the Ukraine (European Union Financial Sanctions) (No.3) Regulations 2014

Interaction with other proposed solutions: If a common standard or best practice regarding screening investigations is developed, it would be prudent to ensure that it is consistent with any other relevant standards (e.g. the proposed Technical Standards for Identity, Verification, Authentication and Risk Assessment – see paragraph 1)

Trusted KYC Data Sharing and Storage Repository

Solution in a nutshell (see pages 46 - 56 of the Solution Paper): Development of a registry or repository for KYC data which can be used to onboard customers, reducing the compliance burden on all parties. The solution focusses on business customers and there are four options:

a) KYC Sharing between Financial Institutions;

b) Customer to Financial Institution;

c) Central KYC Utility Repository Model; and

d) Central KYC Utility Registry Model.

The "Customer to Financial Institution" option is the only option which puts the onus on the customer to provide and update KYC data. Under the other options, the onus is on the PSP to collect KYC data from the customer and supply it to other parties (e.g. other PSPs).

Legal issues arising from proposed solution; relevant legislation and guidance and possible ways in which to resolve legal issues

a) If a centralised repository is the chosen solution, the ownership of the repository and the data within the repository will also need to be clearly determined, as well as any oversight and governance. It should be possible to resolve this as part of the creation of the repository and through the contractual framework which will need to be in place between the repository and the PSPs which supply data to it. It will also be necessary to resolve (potentially through legislation) whether the supply of data to the repository (by customers and PSPs) is mandatory.

b) There is a risk that development of a single repository could be anti-competitive (by discouraging the development of other solutions); this will need to be addressed as part of the establishment of the repository.

c) The solution envisages sharing data between PSPs, so data protection and privacy are relevant issues, including a customer's right to control the use of data and correct data. There are four possible options for this solution, and the possible solutions to any data protection and privacy issues will depend on the option which is ultimately chosen (e.g. if the Customer to Financial Institution model is chosen, the customer controls its own KYC information). Possible solutions to these issues include allowing customers to opt out of KYC data sharing, obtaining customer consent (from both new and existing customers) to the use of data or potentially through a FCA-mandated change requiring the provision of data. Alternatively, legislative action may be required, but further analysis is necessary to determine this (and see paragraph 2.2(a) above).

d) Money laundering legislation requires KYC information to be kept up to date. As a result, it will be necessary to determine which party or parties are responsible for updating the KYC information for a particular customer (e.g. the customer, the registry, any party which becomes aware of a change in the KYC information, etc.).

[8] Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (as amended) and the Export Control Order 2008

e) The liability framework will also need to be determined, either through contractual arrangements or statute. For example, if a repository is established, which party will be liable if data is incorrect, incomplete or out of date and what limits will be established for liability? There may be potential liability to the repository itself, customers, PSPs and to victims of crime.

f) If a repository is the chosen solution, legislative change may be required to make use of the repository mandatory (assuming this is the preferred route).

g) A further issue is whether FIs/PSPs are entitled to rely on the repository data without taking other steps (for example, whether use of the repository data satisfies a PSP's obligations under MLD3, Money Laundering Regulations 2007 (and MLD4, once it has been implemented – for example, see Article 25, which provides that member states may permit regulated entities to rely on certain third parties to meet KYC requirements, but the ultimate responsibility for meeting KYC requirements lies with the regulated entity, not the third party).

h) As part of the development of the solution, it will necessary to consider how the option which has been selected will complement and/or conflict with other KYC standards and guidance and PSPs' global anti-money laundering ("AML") and counter-terrorist financing ("CTF") policies.

i) It will be necessary to set out the relationship between the repository and the provisions in MLD4 (and MLD5, if applicable) that allow firms to apply some measure of simplified due diligence to their customers. The existence of KYC data on its own should not lead to the presumed identification (and thus presumed knowledge of that identity by the firm) of customers where the PSP is not required to identify the customer and/or verify the customer's identity.

j) It will be necessary to address any cybersecurity risks and comply with cybersecurity obligations. This should be possible as part of the implementation of this solution.

Interaction with other proposed solutions: As noted in the Solution Paper, if Solution 1 is implemented (Technical Standards for Identity, Verification, Authentication, and Risk Assessment) the assumption is that individuals will not need to use Solution 4.

Financial Crime Intelligence Sharing

Solution in a nutshell (see pages 57-61 of the Solution Paper): Improved sharing of intelligence on financial crime between PSPs (both in relation to trends and customer and transaction data) through the creation of a single data repository.

Legal issues arising from proposed solution; relevant legislation and guidance and possible ways in which to resolve legal issues

a) Sharing typologies and trends (without sharing underlying customer data) does not present a tipping off risk and should not raise data protection, privacy or confidentiality issues. If transaction and customer data is shared, it will be necessary to consider the following:

   i. Data protection and privacy issues under the DPA (and the GDPR), in particular in relation to a customer's right to control the use of personal data and correct data. Data protection and privacy concerns could be addressed by obtaining customer consent (from both new and existing customers) to the use of data or potentially through a FCA-mandated change requiring the provision of data. It may also be necessary to establish a clear process to enable customers to challenge and/or correct data. Alternatively, legislative action may be required, but further analysis is necessary to determine this (and see paragraph 2.2(a) above);

   ii. Banks owe their customers a contractual duty of confidentiality, which applies to all the information which the bank acquires in its capacity as a bank. There are four broad exceptions to this duty: (i) if the disclosure is compelled by law; (ii) where there is a duty to the public to disclose the information; (iii) where disclosure is in the bank's interests; and (iv) where the customer has given express or implied consent to the disclosure. There is limited

case law on the scope of these exceptions, so banks may need to obtain customer consent or be compelled by law before they can share data. If data-sharing was mandatory, this would override the duty of confidentiality;

iii. Under section 333A of the Proceeds of Crime Act 2002 ("POCA"), it is an offence to disclose that suspicions of money laundering have been reported and/or that a money laundering investigation is being contemplated or carried out if that disclosure is likely to prejudice an investigation. The offence is known as "tipping off" and can only be committed by someone in the regulated sector. Sections 333B to 333D of POCA expressly permit certain disclosures, e.g. disclosures for the purposes of detecting, investigating or prosecuting a criminal offence. However, sections 333B to 333D are narrow in scope and may inhibit information-sharing. As a result, it may be necessary to amend POCA to ensure that tipping off concerns are not a barrier to the implementation of this solution.

b) As part of the establishment of the solution, the ownership and management of the data repository should be considered. Rules on access to and sharing of data are also likely to be required, including to address the point at which data should be shared (e.g. if data should only be shared when a PSP has a suspicion, how will suspicion be defined? Will the point at which data should be shared differ depending on the type of data?).

c) It may be necessary to establish a liability framework in relation to the data which is shared, e.g. to determine the liability of participants for providing incorrect information or failing to share information. It will also be necessary to consider the potential liability of participants to victims of crime, e.g. where the repository contains information which might lead a PSP to suspect fraud, but the information is limited and the PSP permits the transaction to proceed (or potential liability to a customer if the transaction is blocked).

d) One aim of the solution is to facilitate the repatriation of funds to victims. The legal basis for this will need to be determined (the FFA is actively working on this issue).

e) It will be necessary to address any cybersecurity risks and comply with cybersecurity obligations. This should be possible as part of the implementation of this solution.

Interaction with other proposed solutions: There is potential overlap with Solution 2 (Payments Transaction Data Sharing and Data Analytics) because both solutions concern data sharing and analysis.

Other initiatives or proposals which may be relevant to the proposed solutions

The Simplified Access to Markets (SAM) working group has set up a sub-group which is mapping the parties within a payment chain and setting out the regulatory and legal responsibilities of each party, in particular in relation to AML, CTF and sanctions.

Consider possible legislation allowing a payer to be provided with their payee's account name (as through the PAYM service) to prevent financial crime. Under the PAYM service, this information is provided with the payee's consent, but legislation may avoid the need for consent.

Simplifying Access to Promote Competition

Access to Sort Codes

Problem Statement

New participants that wish to connect directly to a payment system currently have to arrange to use a sort code within the range of an existing Bacs direct participant. This means they have to approach an existing participant that may be a competitor. In addition, there are various restrictions to the use and transfer of sort codes that particularly constrain new participants.

Bacs is progressing this activity in its role as operator of the Bank Reference Data for the industry. The solution will see the establishment of a range of sort codes that may be applied for by new participants.

Sort codes are a key routing mechanism for payments in the UK. The bank code element of this is a way of grouping sort codes together. Through the industry Sort Code Directory, a participant's status as having direct or indirect access in a payment scheme is recorded.

There was strong support for this solution in the draft strategy consultation responses (91%).

Current Detriments

- New types of PSPs may encounter difficulties in finding direct PSPs to sponsor them and get access to a payment system, due to having new models where current sponsor bank risk appetite will not support such entities;
- There are a small number of sponsor/commercial solutions for indirect PSPs;
- Third party users (end user PSPs) can't initiate real time payments and access data as they have difficulty gaining access.

Solution Proposal: Description

The solution requires that Bacs, in its role as operator of Bank Reference Data, makes a new range of sort codes available. This removes the dependency for new Payment Service Providers to obtain these from existing direct participants (who may be competitors).

New participants of Faster Payments, Bacs and CHAPS can be allocated one or more of these sort codes. It is also planned to accommodate PSPs who require a sort code but do not want to participate in a payment scheme (for example to be able to issue a UK IBAN).

In the longer term (within five years) it should be considered whether sort code governance should be run and managed independently from Bacs. This is likely to be considered as part of PSO consolidation proposals.

It was also recognised as noted in the consultation responses to the draft strategy that at some point in the future the industry may begin a debate on whether BIC/IBAN should be used as an alternative to sort codes.

Solution Description: Operating Detail

Bacs in its role as operator of the Bank Reference Data for the industry has made available a new range of 04 sort codes. This has been done by setting up a utility bank to hold these 04 sort codes, which combined with the supporting VocaLink technical release has enabled the enhancements to Bacs to support the changes to sort codes. Bacs has confirmed that these changes were successful and they can now allocate sort codes independently of other PSOs;

New FPS/Bacs/CHAPS participants can be allocated one or more of these sort codes. The application process is now in place and following testing and piloting the service is now live.

Technical changes will be required to deliver the solution noted above for those participants who want a sort code but don't want to participate in any schemes.

C&CCC will continue to have some sort code constraints due to the use of the leading two digits of the sort code for cheque sorter configuration. This will be addressed in the planned launch of the Image Clearing Service (ICS).

Bacs is currently well placed and has the necessary experience to deliver these services on behalf of the industry. Further work is already underway to improve the availability of sort code information.

Solution Description: Delivery approach

This solution is now live and has been delivered by Bacs as a collaborative enhancement on behalf of the Payments Industry.

A supporting website has been created to further improve understanding and access to sort codes and to smooth the application process. This is also now live. Plans are in place to provide links to this from scheme websites.

With the involvement of the cross-scheme Clearing Codes Management Group, Bacs will continue its strategic review of the governance and operating model for Bank Reference Data.

Benefits

- Additional sort code availability;
- Clearer, simpler processes for participants in payment systems to obtain sort codes;
- Early delivery of a simple improvement to payment system access which will benefit new participants;
- Removal of dependency on a competitor.

Costs

- Introduction of 04 sort code range budgeted, funded and delivered. Costs have been shared between the four impacted PSOs (Bacs, CHAPS, Faster Payments and Cheque and Credit Clearing);
- Amendment to sort code allocation processes forms part of PSO development budget;
- Costs of development are estimated at £100k. Any project and legal costs have been met from Bacs company budget;
- Collaborative effort has required commitment, resources and co-operation to deliver the solution.

Existing services or Initiatives Underway

As noted above this solution is now live and has been delivered by Bacs on behalf of the Payments Industry, with future developments and enhancements to bank reference data in general being assessed.

Aggregator Access

Problem Statement

Collectively to ensure that a broader range of connectivity options for direct and indirect PSPs exist in the market, by encouraging the development of commercial aggregator solutions, capable of supporting both direct and indirect access to any PSO through a single gateway.

The term “aggregator solutions” used here refers to commercial services for a PSP to gain access to one scheme or for these services to allow a PSP to access multiple schemes.

Responses to the consultation on the draft strategy indicated a 96% support level for delivery of this solution.

Current Detriments

- Multiple PSOs (including card schemes) are expensive, complex and time-consuming to join for PSPs, to connect to by retailers and commercial companies and confusing for end users;
- There are no clear or transparent on-boarding processes or requirements for Participants to join a Scheme, and the process for joining can be lengthy and costly for participants; and
- PSO requirements and rules are too complex, therefore making them expensive to join and/or comply with.

Our Solution Proposal: Description

The proposal is to create the conditions that support the development of a range of competing, commercially developed connectivity solutions to improve access to payment systems.

The access solutions would be accredited for use by, or on behalf of, the payment system operators (PSOs). PSR will oversee PSO progress while the creation of the single entity to govern 3 of the PSOs will support progress.

Technology providers would facilitate access to a payment system for PSPs through a standard common connectivity approach. It is expected that providers will support modern messaging standards e.g. ISO20022. Commercial solutions may then develop to enable PSPs to access multiple payment systems through a single provider.

Designated PSOs and C&CCC are expected to ensure their rules, processes and systems interfaces, enable simplified, efficient and speedy connection for aggregator providers;

This model is already live for Faster Payments and Link. BACS is currently in the process of consulting on an appropriate model, while the planned Image Clearing Service for Cheques will support this approach.

Solution Description: Operating Detail

It is proposed that all PSOs will review and improve access for those wishing to offer aggregator services and to develop a framework model to support this. The proposed solution envisages that retail PSOs will accept and encourage input and output from aggregators, including the Card Schemes;

Whilst most work will be completed by individual PSOs, the collaborative work to deliver common participation models and rules (see separate solution) will support delivery of a consistent approach to connectivity and requirements for aggregator services;

Once enabled services can be further developed in the competitive marketplace and a variety of services such as format mapping and translation for new standards or other payment types could be offered through these portals, in addition to the core technical connection capability;

It should be emphasised that the solution proposed focuses on development of aggregator services in the competitive market space and creating the conditions to allow this competition to flourish. It does not envisage a single common aggregator or even a single aggregator provider for an individual scheme either of which would be unlikely to have positive competition effects;

Given the unique and largely wholesale nature of CHAPS, it is less likely aggregator services will emerge in the commercial space. This should not preclude CHAPS from examining its rules to ensure there are no barriers or onerous conditions for connection to its services. It is worth noting that CHAPS utilises SWIFT messaging, so an aggregator offering SWIFT connectivity (which is generally a core competency) could form part of an access solution to CHAPS.

Solution Description: Delivery approach

It is important to build on the experience of Link and the progress being made with respect to FPS, Bacs and C&CCC aggregator solutions.

Delivery will be through review and simplification of requirements for aggregators to connect to individual schemes. As noted above this will be supported by the work underway to develop common participation models and rules, which will also reduce some of the barriers to these services flourishing.

Competitively, aggregator solutions may then emerge to access multiple schemes from one technology provider.

The PSR has regulatory oversight of the PSOs to oversee progress towards a common approach across PSOs.

Benefits

- Broadening of connection options for PSPs and other new entrants. This directly addresses access issues and provides a service to those who prefer to have the convenience of this type of model.
- Development of multiple payment scheme access through aggregators further simplifying connection. This will be in the competitive space once the environment has been created to allow aggregators to offer these services.
- Reduced costs of access expected for lower volume challenger banks, innovative new providers and existing PSPs. The quantitative impact will be determined by the level of multi scheme services offered by aggregators in the competitive space.
- Increased competition between aggregators and sponsors and gives a real alternative to indirect sponsorship models. When a technical aggregator is combined with a commercial settlement provider, this offers an integrated solution for connection needs.
- Encourages innovation as resources and time can be focused on product development rather than on the need to satisfy multiple connection models.
- Interoperability is encouraged as aggregators would be better placed to support revised future standards when compared to indirect sponsorship models.
- Aggregators can broaden services to include translation capabilities and mapping

Costs

- Investment by PSOs to facilitate aggregator access. Much of the change is expected to be removing complexity and ensuring commonality across schemes so direct costs are expected to be minimal.
- Promotion of the service by PSOs. This is likely to be the communication of the changes to rules made to facilitate these services to the industry and potential suppliers. Costs expected to be modest with delivery through own websites, industry bodies and the trade media.
- Collaborative effort to deliver change in all affected PSOs. This will have resource implications for schemes but these are not considered substantial with financial implications minimal.

Existing services or Initiatives Underway

LINK has developed aggregator service with eight providers currently connected to the scheme.

Faster Payments has been working on an effective aggregator model over the past 2 years and its proposed approach is set out in their report: Faster Payments New Access Model published in May 2015 and researched by Accenture;

The Faster Payments model focuses on all the goals that this solution seeks to achieve with regard to broadening access options. It specifically addresses the needs of a scheme offering real time payments, where indirect options through a sponsor may not deliver this capability;

Bacs is consulting on offering similar services, with Cheque and Credit Clearing Company seeking to enable these services as part of the new Image Clearing Service.

Accessible Settlement Account Options

Problem Statement

Certain payment systems (e.g. Bacs, CHAPS, Cheque & Credit and Faster Payments) require their direct system participants to hold a settlement account at the Bank of England. Other systems (e.g. LINK and Visa Europe) have some direct participants who do not hold, nor are eligible to hold settlement accounts.

Bank of England eligibility for a settlement account requires that the institution is a bank or building society and already holds a reserve account.

Currently, no PSP that is not a bank or building society can obtain a reserve account and hence a settlement account, and thus cannot be direct system participants.

Consultation responses to the draft strategy confirmed 100% support for delivery of this solution.

Current Detriments

- There is no level playing field for PSPs that are not credit institutions. Difficulty in obtaining a Bank of England settlement account as a new direct participant;
- New types of PSPs may encounter difficulties in finding direct PSPs to sponsor them and get access to a payment system, due to having new models where current sponsor bank risk appetite will not support such entities.

Solution Proposal: Description

The objective of this solution is to improve and widen the availability of settlement accounts to those wishing to access the payment systems.

The solution is reliant on the Bank of England, both as supervisor of the retail payment systems and settlement agent to these and other payment systems. This dependency also applies to the Bank of England as operator of the RTGS (Real Time Gross Settlement) System, which houses the Reserve/ Settlement Accounts.

The Bank launched a one year strategic review of its RTGS in January 2016 to develop a blueprint for the future RTGS service by early 2017. A consultation began in September 2016, with any build expected to take 2-4 years, i.e. delivering by 2018-2020.

The Governor of the Bank of England announced on 17 June 2017 that the Bank intends, over time, to extend direct access to RTGS to non-bank Payment Service Providers (firms granted the status of E-Money Institutions or Payment Institutions in the UK), collectively known as PSPs. This will be balanced against continuing to safeguard resilience.

An assessment of the likely future growth in the types and numbers of participants wishing to self-settle is expected to be considered as part of the RTGS strategic review, as any new solution will need to be capable of handling such growth.

Solution Description: Operating Detail

The operational detail of any solution to broaden access to settlement accounts will be determined by the Bank of England. This will be based on the outcome of the consultation it is leading, the subsequent design of the new RTGS system and how it chooses to balance wider access with maintaining the resilience of the payment system.

The fundamental issue will be the Bank's willingness to open up settlement account access to a wider range of participants. This is largely a policy issue, in that the Bank of England needs clarity over the implications of doing this in the context of its statutory obligations, for example the obligation to act as lender of last resort, what happens if things go wrong in terms of participants' liquidity management, and how it can gain comfort around managing AML risk.

The Bank of England will seek to broaden access to settlement accounts as an interim measure using the existing RTGS system. If so it is likely to be constrained by the limited capacity of the current system to support increased numbers of accounts.

Changes may be required to the Settlement Finality Directive to include a broader range of PSPs, e.g. Credit Unions, Electronic Money Institutions (EMIs) and Payment Institutions (PIs).

Solution Description: Delivery approach

Delivery will be entirely dependent on the Bank of England's policy on widening settlement account access and the timetable for the design and build of the new RTGS system, which it is consulting on.

Benefits

- Wider range of participants able to have settlement accounts and hence participate directly in payment systems;
- Legal/regulatory framework that reflects the role of Authorised Payment Institutions and allows their direct participation in payment systems;
- Competition is likely to increase if more institutions have access to settlement accounts in a timely and efficient manner.

Costs

- Technical changes to RTGS platform to enable larger number of participants/accounts, and associated new processes;
- Legal and regulatory changes needed to support wider access to Bank of England settlement accounts;
- PSOs will need to amend scheme rules and participant agreements to reflect agreed changes to settlement practices arising from Bank of England review process;
- Changes will be needed to the legal and regulatory framework to reflect any new practices agreed from the review.

Existing services or Initiatives Underway

The Bank of England is currently consulting on the future of the RTGS system and related access to settlement accounts. Following this it will determine both its short and long term approach to settlement account access based on the decisions it will take on the design and build of the new RTGS system.

Common PSO Participation Models and Rules

Problem Statement

Participants wishing to join more than one PSO face a range of challenges:

- There are different application processes;
- There is no common entry point into the PSOs;
- Significant costs are involved in replicating work across the PSOs;
- Each PSO uses different terminology, which may describe the same activity.

There are areas of commonality, but over time different procedures and terminology have developed, going well beyond the different rule sets for individual payment instruments.

PSOs participating in this initiative are Bacs, Faster Payments, Link, Cheque and Credit Clearing and CHAPS. Consultation responses to the draft strategy showed 95% support for delivery of this solution.

Current Detriments

Multiple PSOs (including card schemes) are expensive, complex and time-consuming to join for PSPs, to connect to by retailers and commercial companies and confusing for end users;

There are no clear or transparent on-boarding processes or requirements for Participants to join a Scheme, and the process for joining can be lengthy and costly for participants; and PSO requirements and rules are too complex, therefore making them expensive to join and/or to comply with.

Our Solution Proposal: Description

The proposal is to minimise non-essential differences between payment system operators BAU procedures, on-boarding processes and terminology. This should reduce the complexity, time and cost for payment service providers (PSPs) that want to become direct members of multiple operators. It should also simplify processes for PSPs for existing members.

Ten areas for collaboration between PSOs have been identified to form the basis for the solution, which aims to deliver a common approach unless there is a justifiable reason to retain differences:

- Common technology and infrastructure terminology across Payment System Operators;
- Common eligibility criteria and baseline requirements for every Payment System Operator;
- Common categorisation of Payment System Operator participants;
- Consistent articulation of payment products, their features and characteristics;
- Common connectivity models across Payment System Operators that facilitate easier on-boarding;
- Improving awareness, involvement and communication with indirect participants
- Considering how rules differ across Payment System Operators and whether they need to;
- Gaining clarity on the differences between Payment System Operators technical requirements;
- Managing the risk that new or existing participants bring to Payment System Operators;
- Improving access to information and documentation to help Payment Service Providers and advisors (recognising that some PSPs and operators may enter into non-disclosure agreements).

Solution Description: Operating Detail

This work is already being taken forward by the Interbank System Operators Coordination Committee (ISOCC) supplemented by other key stakeholders. Link who are not a member of ISOCC will participate fully.

A programme with a dedicated manager is in place to oversee progress and drive activity within each PSO. Regular meetings of the programme team are held alongside a supporting stakeholder advisory group.

A programme plan is in place and has identified those areas from the 10 issues that can be addressed in the short term and those which will require more substantive work.

Solution Description: Delivery approach

Work will be prioritised on common terminology, common eligibility criteria, categorisation of participants and comparison of payment products.

Other items will form a second phase of the work including engagement with indirect participants, on-boarding and documentation. Technical and Annual assurance together with rules alignment will be the most complex items to address but it is expected that PSO consolidation proposals are likely to help progress this area.

Early prioritisation items are expected to be addressed within 12 months while second phase areas will be addressed in a further 12 to 24 months.

Work will be funded by ISOCC members with budgets in place for 2016 and 2017 funding in the course of agreement.

Benefits

- Clearer, simpler processes for participation in payment schemes will enable easier direct connection;
- Creation of a common minimum set of rules, security levels and a clear compliance process across schemes will speed up joining times when access to multiple schemes is required;
- Time, resource and cost in new entrants businesses will be saved rather than having to meet different requirements for multiple schemes;
- Similar savings in time, resource and cost will be made by existing PSP's in dealing with common requirements across multiple schemes e.g. dispute resolution, reporting, compliance requirements, etc;
- With a simpler and common approach to participation models, costs of entry should be reduced to reflect the new environment;
- Innovation will be stimulated as new entrants and non-bank PSP's can gain easier access and develop payment products to support new business models;
- This initiative will also help to improve connectivity for aggregators and PSPs across multiple schemes and further simplify this connectivity option.

Costs

- Amendment to current processes and systems in PSO's will require resources and time to deliver across multiple schemes;
- Collaborative effort will require commitment, resources and compromise to deliver;
- Existing PSPs will need to make changes to current practices and procedures as changes are made across different schemes to align processes;
- ISOCC will need to continue to be resourced over coming years to drive this process given that some of the changes proposed will be longer term.

Existing services or Initiatives Underway

As noted above the programme to support this initiative is in place, resourced and funded.

This solution will be complementary to the work of the new single entity once it is established. It is likely that the single entity will take forward much of this work once it is in place.

Establishing a Single Entity

Problem Statement

A variety of detriments were identified by the Payments Community relating to access. They cover issues relating to choice and competition among PSPs needing to connect to PSOs in order to offer services to end users; limited innovation; the difficulties caused by a lack of common standards and rules between PSOs; costs and resources needed to join different PSOs; and schemes rules and governance arrangements.

These issues would be addressed to varying degrees by this solution while supporting other initiatives set out to improve specific access detriments.

Consultation responses to the draft strategy showed 84% support for delivery of this solution.

Current Detriments

- Multiple PSOs are expensive, complex and time-consuming to join for PSPs, to connect to by retailers and commercial companies, and confusing for end users;
- There are no clear or transparent on-boarding processes or requirements for participants to join a payment system, and the process for joining can be lengthy and costly for participants; and
- PSO procedures and rules are considered complex, adding both a time and compliance challenge.

In addition, some indirect participants, as non-PSO members, consider that change and governance by the PSOs is driven by the large banks. They also consider that PSO governance does not provide scope for them to have an effective voice or their views to be taken into consideration.

Our Solution Proposal: Description

In the short term the overarching governance of Bacs, Faster Payments and C&CCC will be combined. The long-term aim would be integration of the three rulebooks into one over time, building on the Common Payment System Operator Participation Model and Rules Solution.

This would also include the procurement of infrastructure services.

A single entity will provide the opportunity to deliver a more strategic and joined-up approach to the development of the retail interbank payment systems.

One of the objectives of the entity would be to deliver increased interoperability, which should improve systemic resilience and potentially enhance competition in the downstream retail market.

Card schemes, CHAPS and LINK are out of scope for this solution. The other (interbank) PSOs were viewed as utilities, which facilitate and enable competition rather than as entities which compete with each other.

There will be a strong focus on meeting the needs of service users.

The new entity would need to be monitored to ensure that conflicts of interest that could arise from having control of both the rulemaking and procurement functions are appropriately managed.

Solution Description: Operating Detail and Delivery Approach

Following consultation between the Bank of England and the Payment System Regulator a PSO Delivery Group (PDG) has been created, which is led by and independent chairman to develop an implementation approach.

The PDG is made up of the three PSO chairs, the independent chairman and three members nominated by the Payment Strategy Forum. The latter includes a representative of the larger PSPs, one from the smaller PSPs and a consumer representative.

The PDG will make implementation recommendations by end March 2017.

The implementation plan will include detailed design of the consolidated PSO covering areas such as its nature, role, purpose, objectives and governance. It will also address the process to transition to it.

The chair of the PDG will report progress to the PSR and Bank of England.

Following delivery of the implementation recommendations in March 2017, the target will be to complete the consolidation process by the end of 2017, ensuring that the PSOs are operating as one entity.

Benefits

- A more uniform approach between PSOs will bring a simpler, cost effective and more navigable experience to end-users;
- There is potential to improve efficiency and generate cost savings for new and existing PSPs by only dealing with one governance structure rather than multiple PSOs;
- A simpler structure will more easily meet regulatory requirements for effective oversight;
- More users of all types should be encouraged to participate in payment schemes as it becomes understood that the simplified structure and reduced costs make participation achievable;
- Individual PSP's can reduce management time devoted to each scheme with simplified committee and representative structures;
- Opportunities exist to improve resilience of PSOs by harmonising approaches across schemes;
- London Economics analysis indicates that positive competition impact may be possible depending on the chosen delivery approach. At a minimum no adverse competition impacts are expected.

Costs

- Bringing commonality of governance to the PSOs will require committed resources and compromise to achieve;
- A period of transition will be necessary to achieve a fully operational simplified model and this change period will need to be managed carefully to avoid disruption to all stakeholders

Existing services or Initiatives Underway

The solution proposed to address Common Participation Models and Rules will progress areas of consistency and harmonisation across the PSOs pending the establishment of the new governance entity.

Moving the UK to a Common Message Standard

Problem Statement

UK payment systems, like those elsewhere, have developed over time to meet different payment needs. They operate on different payment message standards, which in format and type lead to limitations on interoperability between the systems, on competition for infrastructure and act as a barrier to cost-effective open access.

Despite its advanced payments market, the UK is now an exception among the world's larger payments markets in not having a formal plan to migrate its payment systems to the global payments message standard ISO20022. This has become an increasing necessity, and with the look ahead to Open Banking and PSD2, demands for ISO20022 have increased. Payment system operators are developing individual interim mapping solutions to meet participant demand.

Defined modern message standards will be an essential enabler for the UK's future payments architecture, as they have been in the SEPA, and it will be important to develop new standards. These will address known current limitations and also support the needs for enhanced data capacity, to meet user needs and potentially support financial crime intelligence sharing proposals.

The draft strategy consultation responses showed 97% support for this solution, with responses reinforcing its essential and important nature.

Current Detriments

- Too many standards and too much complexity reducing front end simplicity and stifling innovation, unlike the EU where SEPA has aligned rules for DC/DD;
- Different rules and standards within EU to the UK. SEPA has largely aligned EU standards/rules for DC/DD and should do for instant payments. Still in country variances;
- Range of standards could limit infrastructure competition. If Operators set the rules, there could be multiple infrastructure providers, provided they are all aligned to an ISO standard;
- No real substitutability between payment systems in the event of system failure.

Our Solution Proposal: Description

The solution set out two phases:

i. Tactical for Current Payment Systems

To address the immediate needs of participants that wish to connect to the FPS and Bacs systems using an ISO20022 message format. This will involve mapping exercises between FPS ISO 8583 and Bacs Standard 18 to ISO20022 and back into the UK formats. FPS is complete and available and Bacs is underway.

An immediate benefit of these mappings is their support for new FPS participants via accredited aggregator services, who without this may have needed to develop their own tactical mappings and thus could have led to a potential future lack of interoperability. This supportive development may also increase the longevity of these commercial propositions to the benefit of both participants and technical providers.

For other systems it has been validated that:

- SWIFT MT to ISO 20022 – this is being delivered as part of the Banks of England's RTGS 2.0 programme

- ICS/FCM ISO 20022 format – as a new system this is adopting ISO20022 and the standard will be openly available. Important similarities exist between the message flows in ICS and Bacs and consideration will need to be given to whether to develop harmonised mapping documents for both systems in both the tactical and strategic phases;

- Link mapping – excluded from this stage as its message standard is closely aligned to Card System message standards. The consensus view is that any adoption by Link of ISO 20022 would require a shift by the Cards industry to this standard.

ii. Strategic for the New Payments Architecture

The long-standing industry vision for UK electronic payments is that they should operate based on common ISO 20022 message standards, most likely refined for usage for UK electronic payments by UK-specific Implementation Guides (Guides). These Guides will codify the Operator rules and business processes in the form of business rules and technical/data restrictions.

The proposals for the future architecture offer a clear opportunity to deliver this transition. Both Bacs and FPS are required as part of their next infrastructure tenders to move to formal competitive tendering, which will incorporate the adoption of ISO20022 message standards. It is expected that as a result that there will be more potential infrastructure providers capable of competing on this basis. We noted that the transition may be easier for FPS as a newer payment system with a less rich message range, than for example Bacs.

Solution Description: Operating Detail

It will be important to ensure that there is:

- Clear agreement on the end date for PSP-to-PSP migration to the new message standards, whilst accepting that a period of co-existence will be required;

- Awareness of the potential adverse impacts on business users as happened in the SEPA implementation, which became a mandated transition to the required standard. In particular for Customer-to-PSP migration, which is likely to require mapping services for a period until market solutions emerge to support wider end-to end adoption. Larger Corporate users, who may already have invested for the SEPA, may seek to align their processing quickly to achieve efficiencies;

- Adoption by payment system as the design of the new architecture progresses.

Solution Description: Delivery approach

Implementation of modern message standards is inextricably linked with the plan for the design, development and delivery of the new payments architecture.

In addition, there are also links to the CMA Implementation Entity and its delivery programme, which are considering technical standards for APIs. There will be a need for ISO20022 payment messages, particularly looking ahead to PSD2, and this will drive the need for early messaging design.

A co-ordinated design and delivery structure for all aspects of the Forum's developments is under consideration, and will be aligned where necessary with wider industry developments. This is particularly relevant during 2017, where the focus is on enabling activity such as the consolidation of the three PSOs and messaging standard design should form part of this phase.

International drivers for national messaging standards adoption and development are a combination of inclusive consultations leading to an adoption plan, sometime encouraged by a regulatory impetus. The Forum approach is one that brings all such engagement together, and set out the UK's plan for strategic payments change.

Benefits

- Enhanced competitiveness and ability for UK electronic payment systems and services;
- Improved payments integrity;
- Reduced development costs, operational and compliance risk;
- Efficiency and cost reduction potential for payment processing operations;
- Standardised implementation reduces cost, time to change and improves overall performance;
- Helps ensure re-use and longevity of the message standards once developed;
- Vendors have already created tools to produce ISO20022 compliant messages.

Costs

- Identification/setting up of Standards Setting body building on current work performed by Payments UK;
- Resources to work on development of standards mappings to ISO20022;
- Work to promote standard translation software via web-site(s) where mapping information is published;
- Implementation work to agree common ISO20022-based standard;
- Migration of current payment systems to the new ISO20022 based standard, most likely in parallel with supporting their current message standards for a limited period;
- Investment in central infrastructure changes, payments technology and wider systems. Sunk costs of legacy systems;
- IT maintenance costs, networks/communications costs, training costs, incremental technology replacement etc.

Existing services or Initiatives Underway

Tactical mapping is underway and for FPS capable of being used by participants.

Indirect Access Liability Models

Problem Statement

This solution addresses the challenge for some PSPs to obtain a bank account with a PSP that is a direct participant in a payment system. The indirect PSP may need the account to make and receive payments for its customers, or to hold funds separately from its own business-use bank accounts (often termed 'safeguarding').

The solution recognises that in a healthy payments ecosystem, there should be clear criteria for access whether this is direct or indirect, and that all participants should understand their responsibilities and accountabilities, and be aware of any regulatory guidance which impacts them as a participant.

Feedback is that this is not always the situation currently, as market supply of a bank account to support such indirect access is now tighter, because of changes to money laundering and terrorist financing risk factors. Certain client types, ranging from charities to correspondent banks, have seen their accounts closed by banks in recent years, under the term 'derisking' which spans risk appetite changes, regulatory/supervisory requirements, and commercial criteria.

The provider market is small, but with some emerging growth. Providers remain constrained by the threat of cross-jurisdictional AML/CTF/Sanctions breaches/fines, which reduces the choice and availability of solutions for indirect PSPs.

The access challenges mean that end user PSPs are unable to initiate real time payments and deliver the propositions their customers expect.

Detriments

- New types of PSPs may encounter difficulties in obtaining a safeguarding client bank account or finding a direct PSP to sponsor them and get access to a payment system, as their business model is one which a direct PSP's risk appetite will not allow it to support;
- There are only a small number of sponsor / commercial solutions for indirect PSPs.

Our Solution Proposal: Description

The draft strategy proposed a mapping exercise to clarify the party holding responsibility for relevant obligations; and so identify gaps where clarity was still needed. It recognised the complexity and extent of the issues identified, the range of interested parties, and the various, and not always successful, efforts by industry and regulators to address the issue. All have lead to the industry's conclusion that a multi-stakeholder group, akin to the Forum, is needed to address these issues.

Potential spin-off proposals from impacted PSP representatives were for:

- provider PSPs to define more clearly the criteria they would expect a PSP to meet to obtain a bank account, noting that providers would continue to exercise commercial and risk based decision-making criteria as defined within their corporate policies;
- the introduction of a simplified and standardised accreditation process of direct and indirect access for smaller payment institutions at the time of their authorisation and periodically, potentially through external accredited audit.

Solution Description: Operating Detail

The Emerging Payments Association funded research to consider mapping liabilities. This concluded that the impacts of regulation have caused the costs and complexities involved in engaging with and monitoring the activities of new and smaller regulated entities, to become less commercial and at the same time, not offset the risks of engaging in that activity.

The research instead proposes actions which it believes could lead to a more normalised business environment for bank account access, but concludes that this will only achieve progress with pan-industry and regulator engagement.

Specifically, it sets out the need for:

- Updated current guidance together with specific supporting business and transactional guidance;
- Clearer guidance from regulators of 'what constitutes failure' by a provider PSP;
- Open discussion on the costs of monitoring and how to cover them;
- Co-ordinated development of Best Practice Guidance on developing working relationships with provider PSPs and what constitutes a 'good risk profile' for the indirect PSP type and its transactions.

Solution Description: Delivery approach

We are aware of further engagement by the industry with regulators on PSD2 on bank account access for smaller PSPs. This relates to proposals to open up the payments market to new types of service provider, which may pre-empt further action on this solution, or provide an impetus towards a broader solution.

Article 36 of PSD2 will introduce a new obligation on Member States to ensure that Payment Institutions have access to 'credit institution (CI) payment account services' in order to provide payment services in an 'unhindered and efficient manner'.

HMT has engaged with stakeholders on the implications of the article and is considering whether the UK approach should require CIs, amongst other things to:

- Grant payment service providers (PSPs) and prospective PSPs access to payment account services on an objective and non-discriminatory and proportionate basis;
- Make available to PSPs which request access, the criteria the CI applies when considering applications;
- Maintain arrangements to ensure the criteria are applied in an objective non-discriminatory and proportionate way;
- Ensure that, where access is provided, it is sufficiently extensive to allow the PSP to provide payment services in an unhindered and efficient manner;
- Notify the relevant authority where access is refused or withdrawn
- Furthermore, HMT is asking whether 'payment account services' should be interpreted as:
- Payment accounts used for the purposes of making payment transactions on behalf of clients; safeguarding accounts; and operational accounts.

It is expected that the FCA will become the monitoring regulator, with the PSR being involved for the implications on indirect access.

HMT are mindful, as respondents to the draft consultation expressed, that the interests of different stakeholders need to be balanced. It will be essential for all parties, that these new obligations are clarified.

We recommend that this new workstream should also create parallel regulatory and wide industry engagement to address the many facets of the issue identified through this further work and new information.

Benefits

- More types of PSP able to access bank accounts with a provider PSP (CI) for the provision of payment services (or as specified by Article 36/PSD2);
- Engagement and activity by regulators and industry participants to develop clear guidance and support materials to facilitate an effective market;
- Increase in competition for payments through more types and diversity of payment provider.

Costs

- Development of new policy and process documentation requiring potential legal oversight and review;
- Staff training and communication on new processes; adherence monitoring;
- Collaborative engagement and effort to reach agreement on all external facing aspects of policy.

Existing services or Initiatives Underway

The UK Action Plan for anti-money laundering and counter-terrorist finance envisages an increase in HMT and Home Office's international reach to tackle money laundering and terrorist financing threats by working with international groups, such as the G20 and Financial Action Task Force, to take action overseas.

We would wish to see UK regulators also raising the PSD2 proposed change with relevant international regulators, with the objective of clarifying the obligations on provider PSPs, which operate in those other jurisdictions, or clear transactions in them.

The continued concern of the main provider PSPs of the implications for liability when they provide access in the UK to other PSPs for account and payment provision remains essential.

The Financial Crime group's initiatives may also have some bearing on this work, in particular identity verification standards and the potential UK adoption of enhanced sanctions data quality.

New Payments Architecture

Simplified Payments Platform

Problem Statement

In the UK today, numerous systems make our payments possible (managed by Payments Systems Operators – PSOs), including Bacs, Faster Payments, LINK, Cheque & Credit Clearing, and CHAPS, using widely known methods to customer such as cheques to direct debits to newer forms by way of mobile payments. All schemes provide payment services in a reliable and secure way and are trusted by the industry and their consumers. However, in order for Payment Service Providers (PSPs) to be competitive, they need to sign up to all of the schemes individually – either directly or indirectly via the agency-sponsor bank model.

It has been noted that the payment systems are not interoperable, and access to them is complicated and can be expensive. The difficulties in access act as a brake on innovation and competition between PSPs. The design of current systems limit scalability and make change slow and cumbersome. In addition, end-users may not get everything they want by way of functionality and information. This has led to the suggestion of the development of a New Payment Architecture that would create a modern infrastructure to address the detriments.

The New Payment Architecture (NPA) is a collection of solutions including the Simplified Payments Platform and APIs which will form the basis of the future infrastructure for the payment industry.

The idea of a new Simplified Payments Platform (SPP) has been developed by the working group members in order to improve competition, accessibility, modernise and future-proof our payments ecosystems and aim to deliver better consumer outcomes.

Current Detriments

Features, or the lack of them in the UK payments systems, lead to some significant detriments for PSPs and end-users. Although not limited to, we have highlighted a few of these below:

- It is not easy to track payments across the payment journey;
- Unbanked/underbanked consumers' needs for simple and cost effective payment mechanisms are not met, leading to a preference for cash usage;
- Data on the payer and payee is not fully utilised, meaning greater challenges to meeting KYC and AML rules as well as richer information required under the original PSD legislation;
- The difficulty and cost of entry to schemes may lead to greater costs on the part of PSPs, which are ultimately passed onto the wider economy both in the form of higher pricing;
- Lack of competition and its resulting lack of innovation;
- Existing schemes are not yet meeting the requirements derived from changing user needs and new regulatory requirements such as PSD2 and their impact on messaging formats and data carrying capability.

The SPP proposal enables the simple implementation of the solutions to the detriments of the End User Needs Working Group.

Our Solution Proposal

We have sought to develop workable solutions to improve both access to, and the performance of, the UK's payment systems including:

- A focus on the growing demand for real-time payments, and;
- Simpler architecture, which reduces reliance solely on a core infrastructure, with maintained security and reliability.

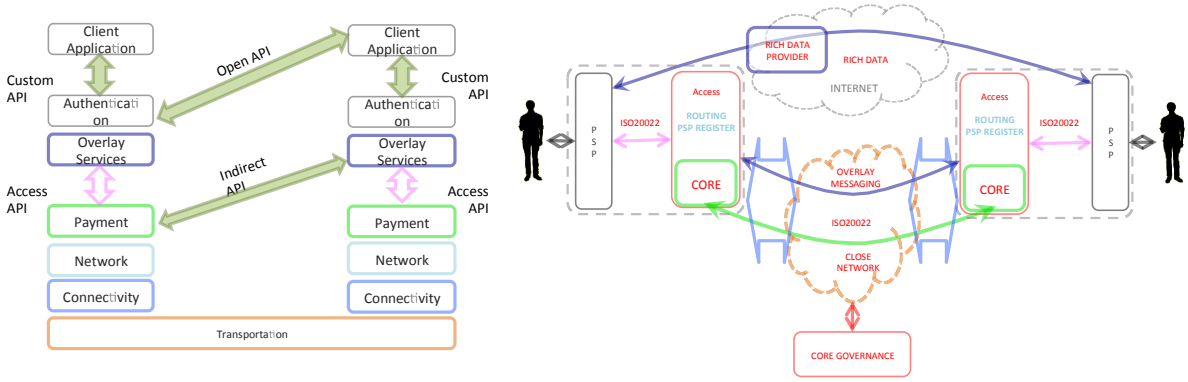
Solution Description

Our proposed SPP solution is the lower layer of a new system, concerned with the payment and not with the context in which the payment is instructed. SPP is tasked with delivering value from A to B, quickly, efficiently and inexpensively.

It's design features and principles are based upon a 'single push rail' model intended to simplify delivery of payments; the SPP solution will also have independent governance, a layered architecture, employ common messaging standards (aligned to ISO20022) and overlay services. We have carefully reviewed the impact on participants – especially for corporate users – and delivered a proposed design which has a compatibility layer for legacy payment solutions, meaning existing direct debit instructions, for example, can continue as-is or be migrated to 'request2pay' depending on the needs of corporate users. This will mean reduced impact and minimal costs for all users.

Service Delivery – How it Works in Practice

This picture, below, shows the formal layered model and the high level implementation building blocks based on a distributed model. Colour coding identifies which element corresponds to which layer in the formal model. The single push rail is a clearing rail and does not include, or assume, any specific form of settlement. It is designed to be independent from settlement process.



Interoperability is key to the new solution: multiple independent PSPs are possible and will be expected to respect and adhere to a single set of standards.

PSPs are added via a 2-step process using the network connectivity and the governance body's approval process. The platform manages the transactional activity through a series of interactions which initiate the transaction via peer-to-peer and various 'calls' between the PSPs.

We have recommended a 'distributed model' approach which will allow collaboration across the platform but also independent deployment by any PSP for use competitively. Clearing will be undertaken directly between PSPs across the network – securely – rather than through a central architecture. It is envisaged that risk is reduced significantly, as there will be no single point of failure.

Delivery of a set of common standards and technological choices are essential to the success of the SPP – these include: standardised APIs; ISO20022 payments messaging; distributed architecture and ledger technology.

Settlement requirements and obligations are known in a real-time basis in the SPP solution, which creates flexibility, however, specific details of settlement would need to be agreed with the BoE during the design period. **NB.** For more detail, please see the HSWG Solution Concept Document – LINK

Governance Proposal

Our proposal for implementing the new SPP solution would be to create and deliver an independent 'body' to both develop, own and enforce a set of standards and protocols for the 'single push rail' – these would ensure that the Overlay Services (e.g. Direct Credits and Debits) worked as per their specification.

In addition, the governance body would certify the technology providers that their technology works as required, authorise/de-authorise PSPs and maintain a master register of PSPs.

Delivery Approach

In developing and delivering a new payments platform for the industry, a new target operating model (TOM) is deemed essential. The first stage of delivery will design and create the key interactions, objectives, aims, governance body and approach, messaging standards, overlay services etc. as well as mapping out the 'customer journeys' (consumer and PSPs), processes, design architecture and concluding with the human capital/cultural changes required. This will affect existing schemes and PSP's, as well as a potential knock-on impact to the wider economy.

Once the TOM has been completed, the design architecture can be developed through production of business and IT requirements.

Definition of the SPP solution, we have estimated, will take c. 2-years. It will include assessments of the existing PSOs, their plans and proposals, and development of outline solution designs, detailed requirements and robust reviews and testing of cost vs. benefit analysis.

Transition

We have considered various transition states in the delivery of the new SPP solution, and the likely solution is that the legacy architecture connects to the new SPP core to allow for existing scheme message types to be correctly routed – enabling existing direct credits and debits to continue effectively. This would maintain critical service as participants move to the ISO20022 messaging standards which interface to the core, prior to full implementation.

Full transition of services expected to be c. 9-years following commencement of new scheme development activities and the design of SPP.

Consideration will be given to those that are impacted most, for example the PSOs, and this will give those PSOs the opportunity to forge new paths in the successful delivery of payments once SPP becomes live.

Benefits

See separate Business Case Evaluation analysis - https://www.paymentsforum.uk/final-strategy

Costs

See separate Business Case Evaluation analysis - https://www.paymentsforum.uk/final-strategy

Known Existing Services/Inflight Initiatives

Given the impending regulatory changes – PSD2, Open Banking etc. – there will be plans in place across a number of banking service providers, PSOs and industry bodies, and therefore these would require careful review by this group ahead of design; this will ensure that effort is not duplicated.

In addition, upon ratifying the proposed solution, we'd expect the new governance body to be a regulated entity (as a PSO). Regulatory oversight, therefore, will be something that we would anticipate being currently in design by the PSR and BoE.

Critical to the success of the SPP solution will be a close working relationship with the Bank of England. It is their intention to develop a new real-time gross settlement (RTGS) solution for the UK; this will undoubtedly affect the scope and design of the future settlement process under SPP and will likely mean changes to regulatory reporting requirements.

We do not believe that any other developments are currently in-flight, or new services being designed (outside of Zapp, which is yet to be rolled out in full); however, we will keep a watching brief on industry activity as part of the HSWG remit.

Key Risks and Issues

The introduction of a new payments system is always extremely sensitive since it involves abandoning a well-known reality for something new.

The key risks identified are on security, robustness of core applications, thoroughness of the standards, etc. Sequential deployment of the SPP will mitigate a lot of the risk. Those risks and issues already captured – e.g. migration to the new platform, retiring of aged payment schemes and continued service (Bacs) solutions – will be embraced and managed through cross-industry collaboration, careful design and testing.

Conclusion

The proposed SPP solution will aim to provide a new platform for PSPs to integrate payment propositions across a common governance and set of messaging standards, envisaged to support consumers and end-users. Whilst it will take a significant period to design, develop, test and deploy, it has the potential to greatly reduce the costs of payment services and ensure all banking service providers and PSPs can use it unhindered.

However, an important requirement to its success is to engage meaningfully with the existing PSOs, and the industry in general. By doing so, we can eliminate duplication of effort – avoiding individual scheme developments, reduce risk and ensure delivery of a cost-effective and efficient solution for the UK fit for the future.