payments strategy forum

Payment Strategy Forum

Financial Crime, Data & Security Working Group report

Update for July 2016

'To engender user trust in safe and certain payments through collaboratively preventing financial crime.'

payments strategy forum

Payment Strategy Forum

Contents

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

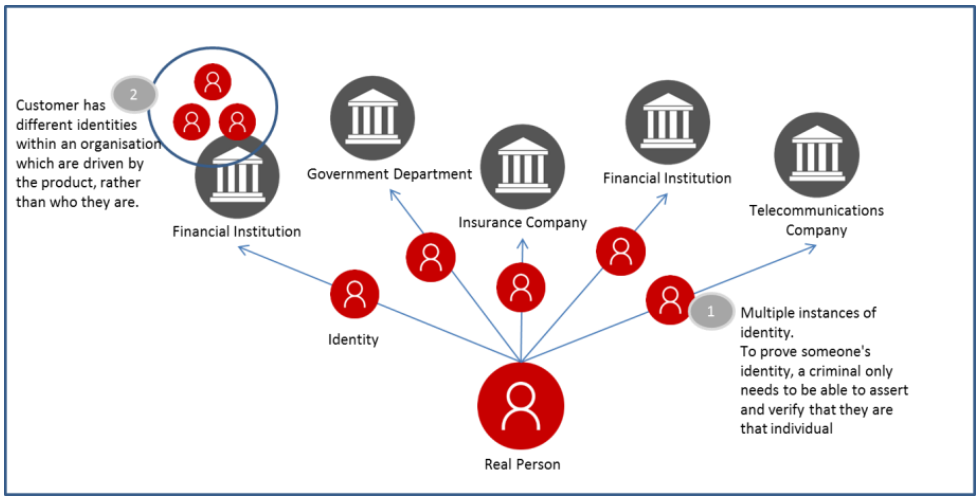
SOLUTION NAME: TECHNICAL STANDARDS FOR IDENTITY, VERIFICATION, AUTHENTICATION AND RISK ASSESSMENT

EXECUTIVE SUMMARY:

Criminals can assume identities of individuals and businesses, allowing them to create payment accounts, to misuse their own payment accounts or to misdirect payments and collections to accounts in their control. This results in direct loss by payment service users, increased cost and work for payment service providers, loss of public confidence in payment schemes and funding of terrorists or criminals.

Inadequate identity management and verification is one the primary reasons why society is exposed to fraud. The Annual Fraud Indicator 2016 report estimated UK annual fraud losses at £193 billion with private sector losses estimated at £144 billion and the public sector fraud losses estimated at £37.5 billion per annum. This leads to a loss of trust and as consumer confidence in specific payment instruments is undermined, they may switch to less effective forms of payment, compromising the smooth operation of payments systems and decreasing efficiency throughout the economy.

Managing identity in an inconsistent fashion, while meets the current needs of regulation, increases exposure to identity fraud given that there is potential for a person to have multiple "identities" in use within one organisation (e.g. a customer takes multiple services from one bank or PSP) and across multiple organisations. In fact, a person may have multiple identities within the same organisation without a single view of them as an individual. More instances of an identity create ever increasing opportunities for a criminal to exploit one or more of these identities.



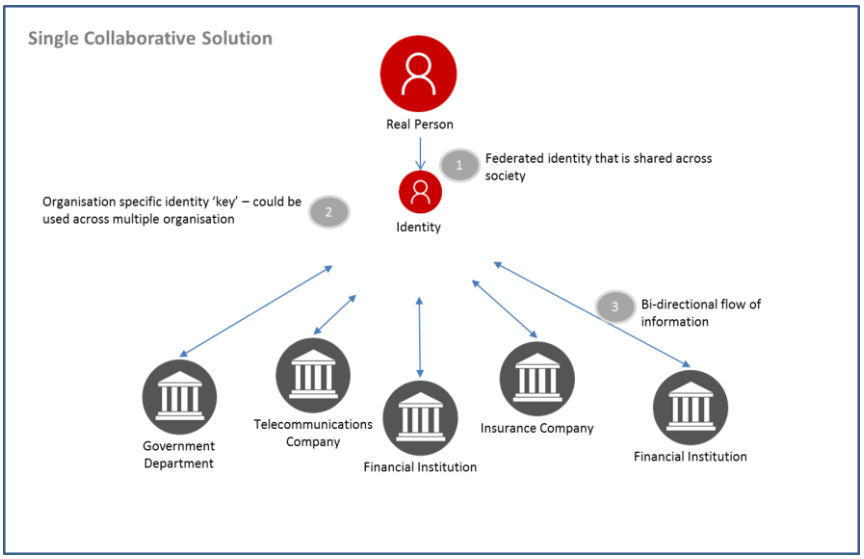
Initial and ongoing identify verification takes place using different processes and systems, depending on the organisation. This can lead to differences in how an identity is captured and how well it is validated and verified, or users are authenticated e.g. variances in failure rates of a biometric, comparison-based authentication system. Criminals exploit these deficiencies to attack the weakest links in the financial supply chain, harming both individuals and organisations.

Currently, there are no specific identifiers that are used broadly across the payments industry and across payment mechanisms, nor are there a single set of guidelines whose primary purpose is that of identifying an individual. The lack of a single set of guidelines adds to the increasing costs of

regulation that organisations have to absorb, which ultimately increases the cost of the end product and gets passed and onto the customer.

Recommendations

The desired end-state is a single system for digital identity, whether distributed or centralised, as a collaboratively-developed solution. This should be a strategic asset at a national level providing identity services for consumers and businesses. In addition to the immediate benefits, reducing the instances where separate identities are used, and by linking accounts together, we reduce the amount of times that it can be abused. It does potentially, however, create a single point of failure and this paper acknowledges and seeks to mitigate those security concerns.



Furthermore, this paper recommends that as part of the roadmap for the delivery of this solution, the current identifier model should be revisited to define a unique single identifier and to take a more pragmatic view of identity.

As a first phase, a standard is proposed comprising technical and governance aspects:

- A single **technical** standard should be developed to ensure that, as an industry, we use the same language when we describe identity and its attributes. This should be a mandatory requirement to avoid consumer confusion and expose weaknesses which could then be exploited by criminals. A data dictionary for identity services should be developed to provide clear guidelines on how key information components should be described and to how they should be referred. There already exist a number of different ISO and other standards for identity definition, management and identity services which would be referenced by such a standard. There would be value is creating an umbrella standard to define a single vocabulary, mandatory for PSPs to adhere to.
- A single **governance** standard should be developed, and enforced through independent audit reviews[1], to establish a common capability framework to:
  - establish the requirement for identity proofing and verifying the identity of an individual;

[1] Similar to PCI DSS assessments

- provide assurance guidance regarding the acceptability, validation and verification of identity evidence that may be presented by an individual to support their identity;
- characterise the elements of validation and verification processes that should be carried out.

This solution proposes a shared service or set of services in which the state, the industry and the end-user (business or consumer) are all stakeholders. This proposal reinforces the principle that preventing financial crime should be addressed not only as an issue for government, law enforcement and the financial services industry, but also as an issue for broader society.

High-Level Approach

The payments industry can reduce Financial Crime by taking a more structured, yet pragmatic view of identity. This could be achieved by the following solutions:

1. **Multiple commercial approach** – many organisations offering different identity solutions as a commercial service
2. **Multiple collaborative solution** – many organisations offering similar identity solutions as consistent services through multiple providers e.g. a solution for Government solution and another for Financial Services and another for Telecoms providers, etc…,
3. **Single collaborative solution** – one group or entity offering identity as a service with individual-specific identifiers and authentication. To use an analogy to illustrate, the payment service user will have many keys to open many doors but only one key ring. This "key ring" for an individual is a set of identifiers and authentication technologies which organisations that use it can trust to verify the identity of an individual and hold key identifiers. The keys may then hold the other information required over and above the core identifiers.

A commercial solution could result in a service that is not inclusive of smaller PSPs; whereas for any solution to maximise its effectiveness, it should be mandatory to all PSPs. It also serves to fragment approaches to identity management and reduces it to a set of corporate propositions. While multiple collaborative solutions do provide a way to overcome the matter of inclusion, this solution has the limitation again of fragmented approaches and simply reducing the problem of multiple identities, rather than tackling it head on. It is worth noting that a multiple solutions may be the starting point for a single collaborative solution.

The recommendation of the working group is to develop solution 3: "single collaborative solution".

PROBLEM STATEMENT AND DETRIMENTS:

Criminals can assume identities of individuals and businesses, allowing them to create payment accounts, to misuse their own payment accounts or to misdirect payments and collections to accounts in their control. This results in loss by payment service users, increased cost and work for payment service providers, loss of confidence in payment schemes and funding of terrorists or criminals.

Examples of the detriments faced include setting up direct debits on third-party accounts, terrorist financing, payments to unintended third-party accounts (invoice fraud, fraudulent merchants), account takeover and fraudulent use of payment cards online. These are becoming the primary concerns of PSPs, central banks, regulators and governments related to the security and integrity of payments systems.

The detriments identified by the working group which are solved by the solution include the following (taken from the 25th February Forum Triage and Prioritisation Report).

Customer perspective - Detriments

1. An identity is used successfully by a criminal (3rd-party)

2. Day-to-day concern about risk of identity theft, risk of fraudulent activity on an account
3. A payment is made to a wrong account
4. Friction in the payment experience, e.g.
   - Online payment verification checks (e.g. a '3D-Secure' retailer)
   - Point-of-Sale card payment declined by PSPs fraud systems (as a 'false positive')
   - Opening a bank account, application is declined due to ID checks
5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notifications
6. Criminals contacting consumers on false pretences (duping) that can result in risk of identity theft and risk of fraudulent payments made on an account

Industry perspective

7. Understand who is the payment initiator (payer) and paying account
8. Understand who is the payment recipient (payee) and the beneficiary account
9. Current ID solution may not be sufficient for proof of identity in criminal cases
10. Know who are vulnerable customers
11. At account opening, where customers are seeking access to payments instruments, understand who is the applying customer

SOLUTION DESCRIPTION

This proposal is to establish **technical and governance standards** to define and recognise the key capabilities that payment service providers need to bring to bear and principles of operation related to identity, including the key principle of a risk-assessment of payment and payment-related transactions.

The standard will establish a common framework for identifying and verifying the identity of individuals and businesses when opening accounts, making payments, or communicating with a PSP (in person, on the phone/mobile, or online). It is not intended that the standard prescribes how to implement identity verification procedures.

Technical and Governance Standards for Identity in Payments

By establishing the key capabilities a payment service provider must consider, but allowing each market participant to make its own technical choice of solution, this standard will support innovation in the key capabilities that are required.

The capabilities as proposed are as follows:

	Capability	Description
1	Identity Validation	Estimate confidence in whether a natural or legal person exists
2	Identity Verification	Confirm the (natural or legal) consumer presented matches the validated identity provided
3	Enrolment and Issuance	Issue, capture and/or enrol tokens, biometrics, knowledge-based security information
4	Authentication	Authenticate the user presented (initiating party) is the user whose identity was verified on a previous occasion
5	Information Attribute Exchange and Confirmation	Confirmation and/or disclosure of key information related to the identity and transaction (including confirmation to a higher

		degree of confidence of the identity of the recipient) when initiating an electronic payment
6	Payment Risk assessment	Quantification of the risks presented by the identity-related components of a payment transaction
7	Mutual Authentication (Account Management)	Protection of non-payments transactions on payment accounts by ensuring that both PSP and PSU authenticate themselves prior to information disclosure or change of account details. This also includes re-assertion of account ownership post-account takeover This encompasses, therefore, authentication of the payment service provider (or 3rd-party service provider) to the user

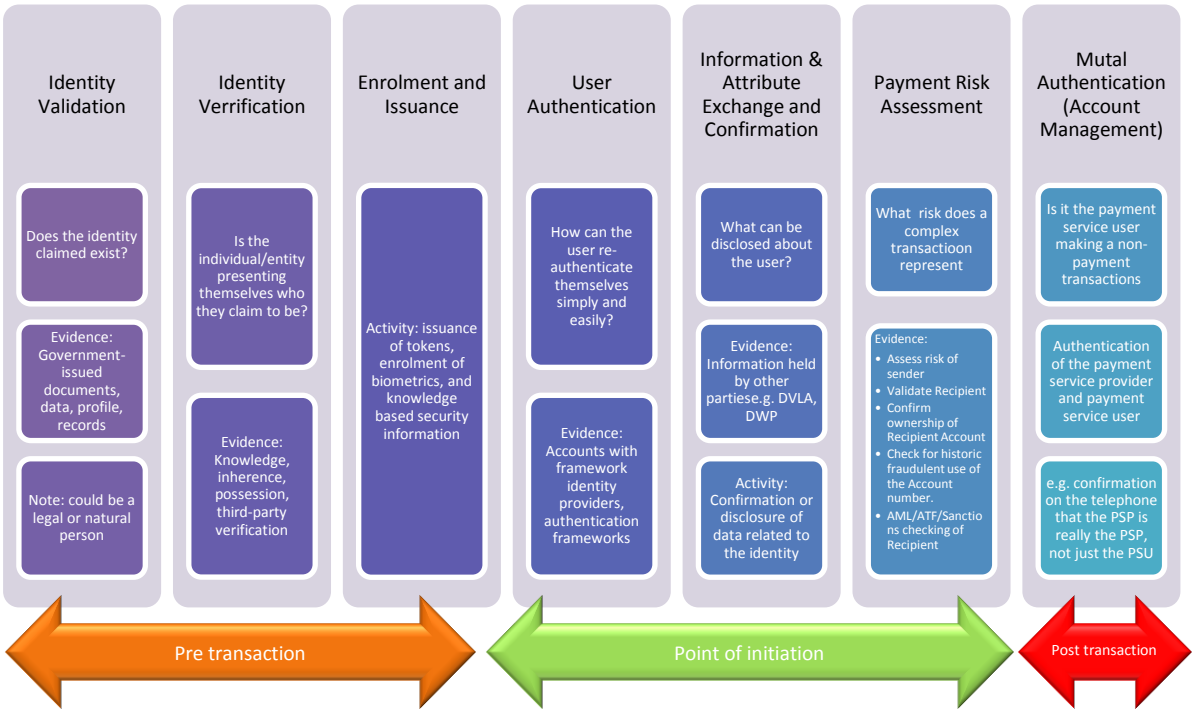
This standard will aim to be similar to and integrate with the Regulatory Technical Standards (RTS) on strong authentication which the European Banking Authority will propose by end-2016, and look to extend for non-remote payment channels and authentication of PSP's when contacting a customer.

Many of these capabilities are currently delivered in a number of different ways for some payment mechanisms by different providers, commercial and otherwise, to payment services providers and payment service users.

The result of the risk assessment framework may include one or more of:

- Expected (mean) loss for a given transaction based on information held by the PSP;
- Probability that a transaction breaches one of the appropriate rules for (e.g. AML, counter terrorist financing, sanctions, account ownership, account takeover, scheme rules …);
- Suspected fraudulent payment requests potentially to be shared;
- PSP remedial activity including referrals and investigations.

There are a number of areas for clarification as part of consultation: for example where the scheme rules mandate some parts of the authentication must be completed by the payment service user; in the case of paperless electronic Direct Debit the obligations to identify the payer (debtor) is placed on the originator; it is proposed that while this transfers the action, the payment service provider is still accountable for ensuring that these identification and authentication processes are completed, as is currently the case for all sponsoring banks.



Example of how a Technical Standard might define the capabilities required

SOLUTION RECOMMENDATIONS

Scope

This paper focuses on the first phase solution where a standard is proposed comprising **technical** and **governance** aspects, which PSPs will need to comply with, and demonstrate compliance with. A single technical standard should be developed to ensure that, as an industry, we use the same language when we describe identity and its attributes. A single governance standard should be developed, and enforced through independent audit reviews[2], to establish a common capability framework for managing identity.

These standards will cover:

- both identity validation and verification related to account opening and making payments;
- all payment types;
- all payment channels.

Going beyond the first phase, the Working Group considers that the desired end-state for the payments environment is a single system for digital identity, whether distributed or centralised, as a collaboratively-developed solution. This should be a strategic asset at a national level providing identity services for consumers and businesses. In addition to the immediate benefits, by reducing the instances where separate identities are used and by linking accounts together the industry can substantially reduce the opportunities for identities to be abused. The payments community should further assess opportunities to align with existing national digital identity initiatives to deliver the capabilities required for payments providers.

[2] Similar to PCI DSS assessments

Principle

The question has been discussed of whether the standards should be prescribed. It is the recommendation of the working group that the standards should be proportionate and compliance not strictly prescribed. Overly prescribed standards could result in new detriments for payments users and providers such as:

- *Consumer*: unable to open an account/make a payment as they are unable to provide all of the information in the format defined by the standard;
- *PSP*: unable to enter the market as the cost to implement the standard is too high, and to ensure simplified market access.

An open question remained on liability if a lower standard was used by a PSP and criminal/fraudulent activity occurred. The consensus is to use a similar approach as defined in Payment Service Directive 2 (PSD2[3]). The new rules make the Account Servicing Payment Service Provider ('ASPSP') liable to restore the funds to the payer in the event of an unauthorised payment, even if a Payment Initiating Service Provider ('PISP') was involved. The rules acknowledge that a Payment Initiating Service provider may, as a consequence, owe the account provider compensation. PSD2 attempts to establish a hierarchy of liability to address previous confusion as to where the burden of proof lies.

The implementation of the standard must be assessable if a PSP is to be certified / assured to enable them to participate in the market.

GOV.UK Verify, the government's online identity assurance service, based on Good Practice Guide-45 (GPG45), is seen as a benchmark for how prescribed the standard would be, as it defines minimum requirements that PSP's must adhere to.

See Appendix *A4 – Key Principles*, for further information.

Data Taxonomy

For the solution capabilities to be most effective, a standard set of data attributes and relationships need to be defined. The standard will include a description of data items and relationships as a Standard for Identity in Payments, to enable PSP's to collect and store payment and identity data in a consist manner. (See Appendix A2 – Data Taxonomy for further details)

Additional solutions identified

In addition to the need to establish fundamental standards for identity across all payment types this solution recognises the need for solutions in addition to the standard. These solutions could be developed collaboratively, by engaging with existing initiatives (e.g. GOV.UK Verify) or delivered by commercial services.

[3] The objective of the Payment Service Directive, adopted in 2007, was to create a single market for payments within the EU, it was further revised in 2015 (PSD2) by the European Commission to create a better consumer protection, incorporation of new and emerging payment services into the regulation, integration and improvement of payment efficiency in the EU, and to drive further improvements in payment services so that they will not be rapidly outdated because of the speed of change related to technological and customer service innovation.

Solution	Description	Proposed delivery
Validation of physical identity documents	PSPs need to validate physical documents when proving the identity of an individual or organisation. In many cases this is difficult especially with uncommon documents such as foreign passports. Some commercial solutions already exist	Commercial/ Competitive Collaborative
National/ supra-national digital identity scheme	If a digital identity schemes existed, it would be much easier for a PSP to comply with many of the identity-related rules. In some countries, such as Estonia, such a scheme exists for all residents. In the UK, GOV.UK Verify[4] proposes to do the same for citizens' relationship with government. It is therefore recommended that engagement with existing and potential new schemes, such as the EU's eIDAS regulation, be undertaken Note the TISA Digital ID project is looking at a pan-financial-services Digital ID that will enable consumers to open a new account online. (The TISA project is working closely with Verify.Gov.UK to determine how to optimise a solution for financial services)	Outside payments industry
KYC sharing	PSPs need a mechanism to be able to share and request KYC data from other PSP's where further information is required for account opening and for the counterparty on a payment. The KYC data sharing solution can be used, to satisfy the needs of this requirement.	Commercial/ Competitive Collaborative

See Appendix *A5 – Ancillary Solutions Identified,* for further information.

PEOPLE INVOLVEMENT AND ACTION

An independent authority	• Establish required capabilities by consultation with industry and providers • Establish principles for each of the capabilities by consultation • Publish Standards • Establish how PSP supervision will occur
Payment Services Provider (PSP)	• Following publication of the Technical and Governance Standards, assess existing operations against the Standards and ensure identity and risk assessment methodologies of each PSP meet the Standards

[4] Note also the European interoperability initiative, "CEF eID" solution: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

Solution Providers, Government	• Continue to develop solutions for each capability requirement to meet the Technical and Governance Standards

LEADERSHIP

A competent independent authority is seen to be the body to establish technical and governance standards and to lead the initiative formally. However to be successful, the detail and application of the framework to each of the payment schemes should be contributed to by scheme companies and industry experts.

Proposed key actions to complete are as follows (subject to further analysis of detailed requirements):

- Establish the Technical and Governance Standards by consultation
- Mandate the Standards as part of UK regulation of PSPs or via primary legislation if necessary
- Monitor and enforce the Standards as part of normal operations

COMMUNICATION

The Payment Strategy Forum's (PSF) Payments Community can be used in addition to other channels to communicate the development of the standard. The impacted organisations are all PSPs regulated by the Financial Conduct Authority (FCA) and therefore these dialogues can be used to communicate the requirements.

SYSTEMS AND PROCESSES

Current risk assessment processes will need to be assessed and documented as part of a standardised approach to risk assessment of identity in payments. In some cases, remedial action may be required by each PSP to meet the minimum standard for all payment types. It is possible that there may be some impact on payment scheme rules, although this is estimated to be minor.

DEPENDENCIES

Establishing Technical and Governance Standards for payment service providers will overlap with a number of other pieces of existing and proposed legislation and rules (See Appendix A3 – Related Standards, Rules, Legislation and business practices for further information) which in some cases apply to specific payment instruments. These include:

- Payment Services Regulations (2009)
- Payment Services Directive 2 (2015)
- European Banking Authority Regulatory Technical Standard on Strong Authentication (TBC)
- Financial Action Task Force (FATF) rules
- Joint Money Laundering Steering Group (JMLSG) guidelines on anti-money laundering and sanctions screening
- Related UK Legislation including Proceeds of Crime Act, Modern Slavery Act 2015
- UK Money Laundering Regulations2007 (MLR)
- Wire Transfer Regulations 2006 (WTR)
- the forthcoming 4th Money Laundering Directive (4MLD) and revised WTR (known as the Funds Transfer Regulations)

In addition, there are number of industry or relevant standards which are enforced by contract rather than by regulation or primary legislation, including:

- Bacs Direct Debit schemes rules
- Bacs channel standards such as Bacstel-IP, ETS and STS
- VISA/MasterCard processing rules
- EMV standards
- Open Identity Exchange (OIX) model of Identity Exchange Attribute Exchange
- GOV.UK Verify operating rules

Finally there is potential that some change to the process of regulation of payment service providers will be needed to ensure that this standard is mandated.

EASE OF IMPLEMENTATION (OVERALL)

Development of the standard is fairly straightforward and could be outsourced to an organisation with expertise in this field such as the British Standards Institute (BSI). The key to a successful outcome is the involvement of all stakeholders, including PSPs, regulators/supervisors, solution providers, law enforcement and specified anti-fraud organisations. For this reason the ease of delivery of the Technical Standard is assessed as straightforward if commitment from stakeholders can be obtained.

Implementation by PSPs of the technical and governance standards will take time, but should be incorporated as part of the regulatory review of qualifying organisations. Because of the nature of the risk assessment, those organisations with fewer payment mechanisms and simpler business models will be faced with a less onerous workload.

COST BENEFIT ANALYSIS (HIGH-LEVEL)

Costs

The costs associated with the standard are anticipated to be in line with general development of industry standards. The costs of the supporting solutions are not estimated.

Description	Cost to	Notes
Establish standard	An independent authority	BSI could be commissioned to commercially develop the standard in conjunction with industry collaboration
Implementation of standard	Payment service providers	Documentation of existing processes and remedial activity to address deficiencies
Ongoing supervision, authorisation and regulation of Payment and Banking Institutions	Competent authority; and payment service providers	A 3rd-party to provide assurance/certification to PSPs implementation of the standard
Maintenance of Technical and Governance Standards	Competent authority	BSI would maintain in conjunction with industry collaboration

Estimates of the cost of developing a standard are £300,000 - £500,000 if using an external agency in addition to the cost of consulted and consulting organisations.

Work by the Forum is ongoing to assess the cost for all PSPs to implement the standard.

It is assumed that third-parties would be used to provide assurance/certification to PSPs implementation of the standard. The estimated cost is still being researched with third-parties who have performed similar activities for similar technical standards.

Benefits

To justify the proposed spend on the solution, a number of quantitative and unquantifiable benefits are highlighted.

The unquantifiable benefits to the customer are:

- improved protection from account takeover, identity theft, account misuse and other financial crime
- high confidence in payments processing
- ability to assert identity and ownership of accounts

The benefits to the industry are:

- consistent standard for risk scoring and data sharing, resulting in the ability to procure and consume common services from a number of providers
- clear principles of operation for identity proofing, verification, authentication and risk scoring

The benefits to the UK are:

- reduction in funding of criminals and terrorists;
- high confidence in payment instruments and systems;
- Overall reduction in fraud levels;
- Support for the UK's competitive position as a centre for financial services;
- Support for the UK Governments and Law Enforcement's economic crime initiatives, including those on cyber crime.

As part of the analysis of the working group, a number of use case were identified which maps to the detriments from the 25th February Forum Triage and Prioritisation Report. Use cases were also identified and prioritised (low 1 to high 10) by the working group. By mapping the detriments against the use cases, and then further mapping to the proposed solution capabilities, we are able to demonstrate how the technical standard can help to mitigate the risks identified.[5]

Further analysis is taking place to identify the gaps in industry which map to the detriments.

#	Priority	Use case Headline	Solution addresses detriment
1	10	Open payment account	✓
2	10	Set up Direct Debit	✓
3	10	Remote card payment (CNP)	✓
4	8	Contact Customer	✓
5	8	Issue authentication token	✓
6	9	Change payment account address	✓
7	9	Make one-off remote banking payment	✓
8	6	Initiate payment in branch	✓
9	5	Make recurring remote banking bill payment	✓
10	10	Issue change of account details	✓
11	8	Enrol biometric security details	✓
12	9	Change payment account details	✓
13	8	Make e-money transaction (P2P)	✓
14	8	Open Third-Party Provider account	✓
15	9	Switch customer / charity / small business account	✓
16	7	Make Subject Access Request	✓
17	7	Make payment via e-banking	✓
18	8	Change payment account business information	✓
19	7	Request refund, return	✓
20	8	Open new business payment account	✓
21	8	Request additional KYC information	✓

See Appendix A1 – *Use Case Mapped to Detriments and Solution Capabilities*, for more information on the mappings.

Using data taken from FFA UK 2016 report, fraud cases can be used to demonstrate benefits that the proposed solution can potential achieve, by reducing the fraud loses seen in the industry. This report does not claim that by adopting the proposed standards the fraud will not reduce to zero. This is only a demonstration that by taking the appropriate measures and following the standards/ guidelines fraud can be managed and further fraud can be prevented.

The following fraud types and associated costs to the UK economy show examples of where the solution can help to reduce costs historical incurred.

- *Remote purchase fraud (internet, telephone, mail order also known as Card Not Present) (2015: £398.2m +20%)*
    - The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, digital attacks such as malware and data hacks, or through unsolicited Emails or telephone calls. The card details are then used to undertake fraudulent purchases over the Internet, phone or by mail order.
- *Application Fraud (2015: £14.1m +38%)*
    - Application fraud occurs when criminals use stolen or fake documents to open an account in some else's name. For Identification purposes, criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeit documents.

- *Online Banking Fraud (2015: £133.5m +64%)*
    - Online banking fraud refers to the fraudulent act of surreptitiously accessing and transferring funds from an individual's or a company's online bank account for the

purposes of financial gain. In some cases, an individual may even be duped ('socially engineered') by a criminal into making a fraudulent money transfer themselves. Criminals use a variety of cyber-related tools and techniques such as malware and phishing to commit this type of fraud, some of which are used to mask the true identity of a person or company. The proposed solution can create a more difficult environment to achieve success for the criminals, costing them time and money.

- *Lost and Stolen Fraud including Courier Fraud (2015: £74.1m +24%)*
    - The courier scam is when fraudsters call and trick you into handing your cards and PIN numbers to a courier on your doorstep.
- *Telephone Banking Fraud (2015: £32.3m +92%)*
    - Telephone banking fraud refers to the fraudulent act of accessing and transferring funds from an individual's or a company's telephony bank account service for the purposes of financial gain. A criminal will use a variety of ways to acquire information about an intended victim such as social engineering, phishing, and vishing (by pretending to be from a trusted organisation such as a bank or the police).

SECURITY

The approach taken in developing a framework that allows payment services providers and technical solution developers to create and deploy innovative capabilities will help to ensure the technical standard will support the on-going progress in the prevention of fraud and financial crime. As techniques improve, the standard will allow PSPs to evolve their strategies and deploy a flexible set of countermeasures.

IMPACT: SUCCESS METRICS

The success can be measured in the value and volume of payments that reach criminals or terrorists. Key metrics would be:

- Volume of third-party account opening and account takeover frauds;
- Volume and value of payments detected as part of money laundering, terrorist financing, fraud or other financial crime;
- Volume of cases of fraud shared by payment services providers under commercial data sharing schemes;
- Volume of payment fraud cases reported to FFA, CIFAS, UK Police (Met and National Crime Agency);
- Total UK losses to financial crime;
- The number of resulting intelligence packages generated for Law Enforcement from intelligence sharing and reporting.

Reduction targets in volume and value could also be set on a per-payment mechanism basis; analysis and collaboration would be required to determine these.

COLLABORATIVE OR COMPETITIVE

What is proposed is an industry-wide, collaboratively developed framework into which competitive and innovative solutions can be developed. This mandated approach for any organisation facilitating payments allows it to define how it delivers its services for its own business needs and those of its clients.

Since many competing solutions deliver capabilities referred to in this, a single collaborative procurement is likely to stifle competition and prevent innovation. This approach allows innovation to flourish and creates a defined framework into which new providers can position their services and techniques. It is unlikely that a single provider could deliver a centralised service which could keep up with best practices across the number of payment schemes required; therefore the onus should be placed on PSPs to make their own decisions based on this framework.

Finally this approach allows payment service providers to meet industry standards for identity and authentication, to interact with other providers on a common basis and to make UK payments secure and trusted.

EXISTING OR IN-DEVELOPMENT SOLUTIONS

While there are many solutions in development which would fit into this framework, the development of a standard does not preclude their inclusion, or the future inclusion of new products and services.

Current initiatives in this area include (but not limited to)

- MIDAS alliance
- TISA financial services digital ID initiative
- Implementation of eIDAS, a European regulation on electronic identification and trust services for electronic transactions in the internal market.

QUICK WIN VS SUBSTANTIAL PROJECTS

The area of establishing principles of data sharing and confirmation of account ownership are important capabilities to prioritise in order to minimise direct debit fraud, invoice fraud and Card Not Present (CNP) fraud on card transactions.

INTERNATIONAL INSIGHTS / BENCHMARKS

There are currently no similar international standards with the proposed breadth of scope - although, as previously mentioned, there are applicable rules and regulations in other countries (e.g. Basel, FATF), and more are being developed, such as the EBA RTS on Strong Customer Authentication.

APPENDIX - TECHNICAL STANDARDS FOR IDENTIFY VERIFICATION, AUTHENTICATION, RISK ASSESSMENT

This section contains 5 appendices for this Identity Standard solution proposal.

A1 - Use Cases Mapped to Detriments and Solution Capabilities

A2 - Data Taxonomy

A3 - Related Standards, Rules, Legislation and business practices

A4 - Key Principles

A5 - Ancillary Solutions Identified

A1 - Use Cases Mapped to Detriments and Solution Capabilities

The following use cases where identified by the working group to provide real life scenarios on the detriments identified in the 25th February Forum Triage and Prioritisation Report.

By further mapping to the proposed solution capabilities, we are able to demonstrate how the technical standard can help to mitigate the detriments.

Further analysis is taking place to identify the gaps in industry which map to the detriments.

#	Priority	Headline	Mapped to Detriment	Mapped to Key Capability	Initiating Actor	Impacted Actors	Notes
1	10	Open payment account	1. An identity can be used by a criminal (3rd party) 3. A payment is made to a wrong account 4.c. Application is declined due to ID checks 8. Current ID solution may not be sufficient for proof of identity in criminal cases 10. At account opening, where customers are seeking access to payments instruments understand who is the applying customer	1 .Identity Validation 2. Identity Verification 3. Enrolment and Issuance	Customer / Criminal	PSP, Consumer	Online, in person, via post
2	10	Set up Direct Debit	3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 7. Understand who is the payment recipient (payee) and the beneficiary account	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 6. Payment Risk assessment	Customer / Criminal	PSP, Business, Consumer	Online, Post / In person
3	10	Remote card payment (CNP)	1.An identity is used successfully by a criminal (3rd party) 4.a. Online payment verification checks (e.g. a 3D Secure retailer) 7. Understand who is the payment recipient (payee) and the beneficiary account	2. Identity Verification 4. Mutual Authentication 6. Payment Risk assessment	Customer / Criminal	PSP (Issuer), Business (Merchant)	MOTO / Online / Mobile

4	8	Contact Customer	1.An identity is used successfully by a criminal (3rd party) 4.b.Point-of Sale card payment declined by PSPs fraud systems (as false positive) 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account 9.Know who are vulnerable customers	2. Identity Verification 4. Mutual Authentication	PSP / Criminal	Consumer / Business	Telephone, e-mail
5	8	Issue authentication token	1.An identity is used successfully by a criminal (3rd party) 4.a. Online payment verification checks (e.g. a 3D Secure retailer) 8. Current ID solution may not be sufficient for proof of identity in criminal cases	2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	PSP	Consumer / Employee / Business	Remote or in person
6	9	Change payment account address	1.An identity is used successfully by a criminal (3rd party) 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Consumer / Criminal / Employee	PSP, (Consumer), (Business)	Telephone, online, in person
7	9	Make one-off remote banking payment	1.An identity is used successfully by a criminal (3rd party) 3. A payment is made to a wrong account 7. Understand who is the payment recipient (payee) and the beneficiary account	2. Identity Verification 4. Mutual Authentication 6. Payment Risk assessment	Consumer / Employee / Criminal	PSP, Consumer / Business	Online
8	6	Initiate payment in branch	3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 8. Current ID solution may not be sufficient for proof of identity in criminal cases	2. Identity Verification 4. Mutual Authentication 6. Payment Risk assessment	Consumer / Employee / Criminal	PSP, Consumer / Employee	In person

9	5	Make recurring remote banking bill payment	3. A payment is made to a wrong account 7. Understand who is the payment recipient (payee) and the beneficiary account	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 6. Payment Risk assessment	Consumer / Employee / Criminal	PSP, Business	Online
10	10	Issue change of account details	1.An identity is used successfully by a criminal (3rd party) 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account 9. Know who are vulnerable customers	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Business / Criminal	PSP, Business, Consumer	Invoice Fraud
11	8	Enrol biometric security details	1.An identity is used successfully by a criminal (3rd party) 4.c. Application is declined due to ID checks 10. At account opening, where customers are seeking access to payments instruments understand who is the applying customer	2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	PSP	Consumer / Criminal / Employee	In person / Online
12	9	Change payment account details	1 .An identity is used successfully by a criminal (3rd party) 2. Day to day concern about the risk of identity theft, risk of fraudulent activity on an account 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account 9. Know who are vulnerable customers	2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Consumer / Criminal / Employee	PSP, Consumer / Business	Telephone, in branch, online
13	8	Make e-money transaction (P2P)	2. Day to day concern about the risk of identity theft, risk of fraudulent activity on an account 3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification	2. Identity Verification 4. Mutual Authentication 6. Payment Risk assessment	Consumer / Criminal / Employee	PSP, Consumer / Business	Online / Mobile

14	8	Open Third-Party Provider account	3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification	1. Identity Validation 2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Consumer / Criminal / Employee	PSP, Consumer / Business	PSD2 AISP / PISP. Online / Mobile
15	9	Switch customer / charity / small business account	2. Day to day concern about the risk of identity theft, risk of fraudulent activity on an account 3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification	1. Identity Validation 2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Consumer / Criminal / Employee	PSP, Consumer / Business	Online / Mobile of Open payment account
16	7	Make Subject Access Request	1.An identity is used successfully by a criminal (3rd party) 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account 9. Know who are vulnerable customers	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	Consumer / Employee/C riminal	PSP	GDPR, via post, online
17	7	Make payment via e-banking	3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 7. Understand who is the payment recipient (payee) and the beneficiary account	2. Identity Verification 4. Mutual Authentication 6. Payment Risk assessment	Consumer / Employee / Business / Criminal	PSP, Consumer / Business	Online
18	8	Change payment account business information	3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 7. Understand who is the payment recipient (payee) and the beneficiary account	1. Identity Validation 2. Identity Verification 3. Enrolment and Issuance 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 6. Payment Risk assessment 7. Account Management	Employee / Criminal	PSP, Business	Via post, telephone, e-mail, online

19	7	Request refund, return	1.An identity is used successfully by a criminal (3rd party) 2. Day to day concern about the risk of identity theft, risk of fraudulent activity on an account 3. A payment is made to a wrong account 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 8. Current ID solution may not be sufficient for proof of identity in criminal cases	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation	Consumer / Employee Criminal	PSP, Consumer / Business	Telephone, online, mobile, e-mail
20	8	Open new business payment account	1.An identity is used successfully by a criminal (3rd party) 5. Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notification 10. At account opening, where customers are seeking access to payments instruments understand who is the applying customer	1. Identity Validation	Employee / Criminal	PSP, Business	Online, in branch, telephone
21	8	Request additional KYC information	2. Day to day concern about the risk of identity theft, risk of fraudulent activity on an account 6. Criminals contacting consumers and fool them that they represent a PSP, an act than can result in risk of identity theft and risk of fraudulent activity on an account	2. Identity Verification 4. Mutual Authentication 5. Information Attribute Exchange and Confirmation 7. Account Management	PSP /Criminal	Consumer, Business	

A2- DATA TAXONOMY

The table below describes the areas and types of data the taxonomy would cover, using GPG45 and ISO/IEC 29115:2013-04-01 as primary sources for the initial analysis.

Term	Definition
Assured Identity	A Claimed Identity that is linked to an Applicant with a defined level of confidence that it is the Applicant's real identity.
Biometric	A measure of a human characteristic that is captured recorded and/or reproduced in compliance with ICAO 9303 or ISO/IEC 19794.
Claimed Identity	A declaration by the Applicant of their current Personal Name, date of birth and address.
Genuine	To be what something is said to be; i.e. authentic not counterfeit.
Identifier	one or more attributes that uniquely characterize an entity in a specific context
Identity	A collection of attributes that uniquely define a person or organisation. The fact of being whom or what a person or thing is.
Identity Evidence	Information and/or documentation that is provided by the Applicant to support the Claimed Identity. Identity Evidence must, as a minimum, contain the Personal Details OR the Personal Name and photo/image of the person to whom it was issued. Identity Evidence must be current,
Identity Evidence Package	Evidence that the Claimed Identity exists
Identity Evidence Package	The Identity Evidence Package is the collection of Identity Evidence provided to support the Claimed Identity. The Identity Evidence Package must contain at least one piece of Identity Evidence that demonstrates address and one that demonstrates date of birth.
Identity Proofing	Identity Validation and Identity Verification
Identity Validation	Validation of the pieces of Identity Evidence in an Identity Evidence Package to ensure the Claimed Identity exists to an appropriate degree of certainty
Identity Verification	A process performed to determine whether the Applicant is the owner of the Claimed Identity.
Knowledge Based Verification (KBV)	Static Where a secret has been previously exchanged between two parties. One party uses the secret to verify that they are the other party with whom the secret was originally exchanged. Also referred to as a shared secret. Dynamic A process where the Applicant is required to provide answers to questions relating to the Claimed Identity.
Personal Details	A combination of Personal Name and at least one of date of birth or address. (Not to be confused with Personal Data as defined by the Data Protection Act.)
Personal Name	A proper name used to identify a real person, as a minimum this contains forename and surname (also known as given name and family name); it may include titles, other/middle names and suffixes.
Valid	To know that something stated is true.
Validation (of Identity Evidence)	A process performed to determine whether a piece of Identity Evidence is Genuine and/or Valid.

A3 - Related Standards, Rules, Legislation and business practices

The area of identity is already covered by a number of relevant artefacts. This includes commercial agreements, legislation, scheme and other rules and national and international standards. The diagram below comprises existing initiatives and to which of the capabilities, required of a PSP by the proposed Technical Standard, each set of rules applies.

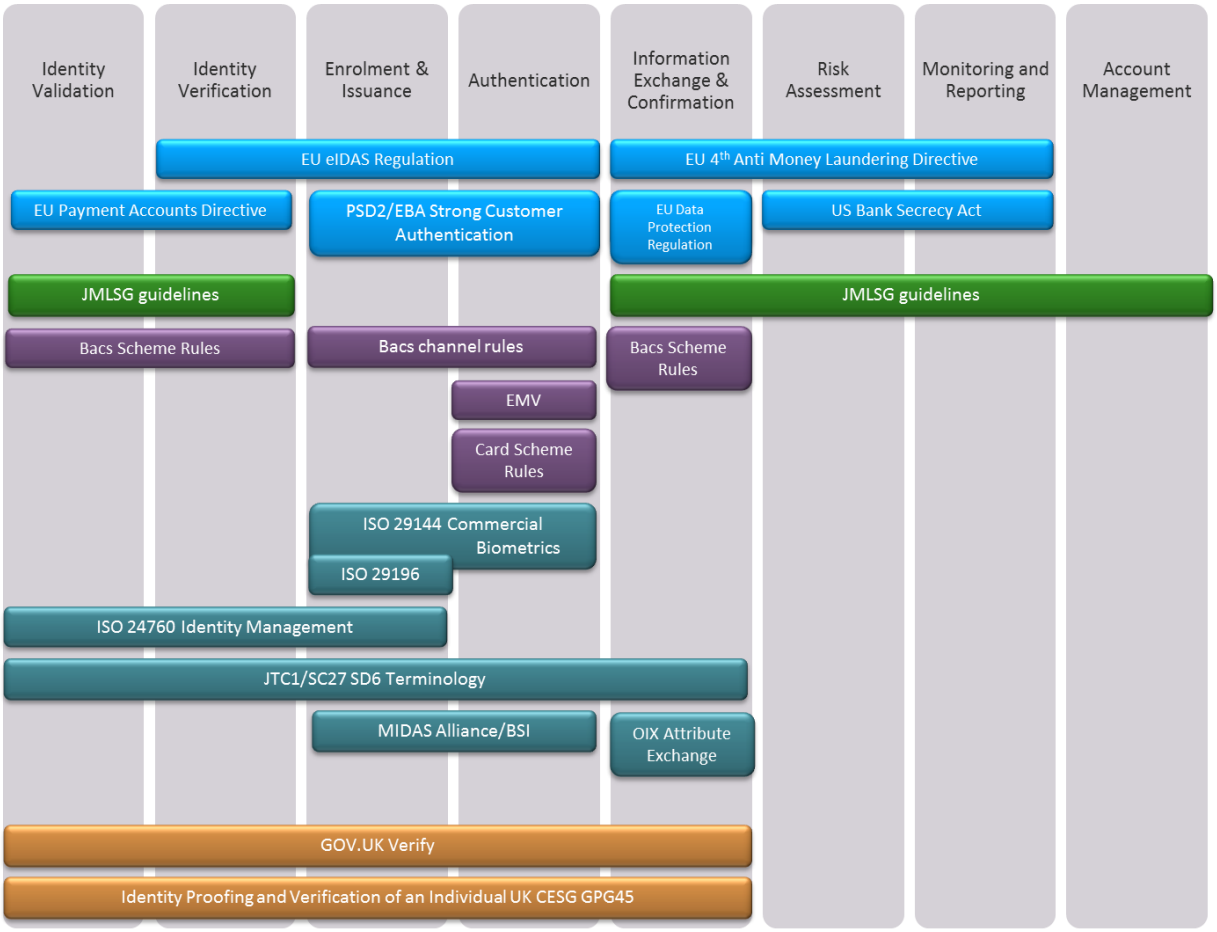


Diagram showing mapping of some rules, legislation and standards to capabilities (not exhaustive)

A4 - KEY PRINCIPLES

The following are candidate principles for each of the capabilities and are intended only to illuminate the potential of principles and for the purpose of discussion. It is likely that these will be superseded during the development of the standard. These candidate principles are therefore indicative of the content of a final standard and, as such, are subject to change.

Core principles

a) Payment service providers must assess the identity-related risk of each transaction to an appropriate level for the value of the transaction, its relationship with its payment service user and in compliance with legislation, rules and regulations.
b) Payment service providers will be required to document how they meet each of the capabilities described, for each of the payment types they support. Smaller payment service providers are therefore likely to be subject to a smaller scope of regulation than larger providers with multiple payment mechanisms.

Identity Validation

c) The identity of an individual (natural person) must be validated using a birth record data issued by or held by a government, or by exception a proxy for a government, or a document derived directly from a birth record
d) The identity of a legal entity (legal person) must be validated using records held and maintained by the competent authority for the jurisdiction in which the legal person is domiciled
e) The individual whose identity is being validated may be living or deceased

Identity Verification

f) The individual presenting him / her to be verified may use a number of methods to verify the link to an identity which is already validated. These may include:
    - Known static data
    - Existing Identity Providers/Identity Schemes
    - Documentary proofs and bearer documents.
g) During Identity Verification, the Individual, whose identity has been validated already, must be checked to a level appropriate for the expected relationship with the payment service provider.
h) Identity verification of a legal person constitutes two part: verification that the legal person is still extant, according to the relevant competent authority, and that the natural person(s) representing him, her or themselves are duly authorised by the legal person to do so.
i) The means of verifying the identity of any natural or legal person must be recorded permanently and held for seven years after the dissolution of any relationship with the payment service provider.

Enrolment and Issuance

j) Identity tokens are issued or enrolled by payment service providers. These may include security tokens (including cryptographic ones) , shared secrets, biometric recordings (both behavioural and static) and device-based recognition technologies
k) A payment service provider must be able to authenticate the individual using multiple factors to at least the level of confidence achieved by identity verification
l) Where tokens are issued to legal persons, they are linked to the identity of a duly authorised, natural person

Authentication

m) Payment service providers must authenticate payment initiators using methods appropriate to achieve the level of risk assessment appropriate to the transaction. In many cases for payments this will be based on the value of the transaction, but ultimately needs to be driven by risk.
n) In the case of a payment transaction initiated by or on behalf of a legal person, the payment service provider may, by agreement, delegate authentication to the legal person.
o) Where a transaction is initiated by the payee, for example payment card, cheque and direct debit transactions, the payee must be appropriately authenticated.
p) When initiating an electronic payment transactions (e.g. Direct Debit payee, card account holder, recipient of credit transfer/RTGS payment, online banking payments.), the initiator should have the opportunity to confirm or be provided a level of assurance that the recipient is the party the initiator is expecting to pay (e.g. seeing the name of the receiving account or a confidence score based on how closely the name entered by the initiator matches the name related to the account and sort code)

Information and Attribute Exchange and Confirmation

q) The sender's payment service provider must use appropriate mechanisms where they exist to verify key data in a payment transaction to an appropriate degree; this includes identity of the counterparty, ownership of the payment account being debited or credited, reference numbers where they are published. A solution is therefore required to confirm ownership of account receiving transactions e.g. Direct Debit payee, card account holder, recipient of credit transfer/RTGS payment, online banking payments. This would, as a minim, confirm the name of an individual associated with a payment account. In some cases it may be possible to provide the name on an account, for example when held by a legal person, or a confidence score based on how closely the name entered by the initiator matches the name related to the account and sort code. . Commercial solutions exist for some payment types but not all.[6]

Payment Risk Assessment

r) The sender's payment service provider must assess the risk of the payment transaction. This will include assessing the following risks:

- identity risk of payment not being initiated by the sending accountholder
- identity risk of the payment transaction not being directed to the real counterparty
- risk of non-ownership of counterparty account
- risk of fraudulent use of the initiating account number using historical data
- risk of money-laundering
- risk of funding terrorists or criminal activity

[6] The initial direction of the working group was for the initiator of a payment to be provided the opportunity to authenticate the recipient.

An alternative point of view proposed that the receiving PSP should have the liability of authenticating the receiver of the payment, based on information entered by the payer. The prevailing view was that this would cause significant challenges to existing high volume payment mechanisms (e.g. Faster Payments), and would cause significant increases in PSPs operational costs (i.e. costs of screening and authenticating every payment received).

Identity Monitoring and Reporting of Financial Crime

s) Both sending and receiving payment service providers must monitor their clients' accounts for criminal or fraudulent transactions using an appropriate mechanisms

t) Where a payment service provider finds criminal activity linked to payments transactions, as well as informing the appropriate law enforcement body it must inform the payment service provider of the counterparty unless specifically directed not to by law enforcement or the competent authority. In addition, where a PSP operates a financial or eCrime intelligence capability, appropriate trust forums should be utilised to share trends, methods and emerging threats on an intelligence basis only.

Mutual Authentication (Account Management)

u) When an legal person as payment service user or representing a legal person contacts its payment service provider, the payment service provider Is required to use one or more means of authentication appropriate to the risk of the operation being attempted

v) A payment service provider must re-verify a payment service user when that user reports that his or her account has been compromised or taken over. This verification will typically use different mechanisms to assess the identity of the individual from those used to open the account.

w) When a payment service provider contacts its client, it must identify and authenticate itself to its client or provide a means by which the client may verify its identity before initiating a transaction or providing any sensitive details. This is particularly important where contact is made over the telephone, as well as the internet. It is vital that payment service users can trust communications with their payment service provider and has the proper means to authenticate their PSP across all communication channels (telephone, internet & SMS). The telephone and SMS channels are currently heavily targeted by criminals to defraud consumers, and are main contributors to the record increase in banking fraud losses. This capability is already required based on the 1998 Remote Banking Principles but need to be firmed up. This area can be more prescriptive than the overall Identity and Verification Standards as the public need a simple consistent message on what to expect and it shouldn't be too complex/restrict access to smaller PSPs.

A5 - ANCILLARY SOLUTIONS IDENTIFIED

A need has been identified for a number of solutions which either do not exist, are not widely adopted, are incomplete or not as efficient as required. This solution recognises that these solutions are necessary for the proper implementation of identity standards.

1. Verification of physical identity documents

A solution is needed to verify the identity of a natural or legal person using physical documents, in situations where such documents are required such as when the client is physically present. Some commercial solutions exist to verify existing documents to a limited degree; however it may be that change to the physical documents is more beneficial, such as incorporation of a cryptographic, printed code which could be verified.

2. Digital Identity

A digital identity solution would be a significant benefit in order to minimise duplication, increase robustness and ensure consistent identity information. It is not proposed that the payments industry create a national digital identity scheme but it is recommended that engagement with existing schemes, such as GOV.UK[7] Verify, be undertaken to utilise work already under way in this area. It is also possible that commercial schemes may exist.

3. KYC Data Sharing

A mechanism for sharing KYC data including Identify and Verification would be a significant benefit to minimise duplication between PSPs, and improve efficiency when a PSP can rely on other organisation's verification of the customer, if they have processed the contact to the highest standard, doesn't come through strongly.

[7] Verify.gov.uk applies a high standard of identity validation and this currently results in an issue of higher fail rates than a mass market payments system may need. TISA are currently looking at the level of security currently applied by financial services, which is compliant with KYC / AML rules and also eIDAS as the foundation of proving a digital ID. TISA hope to have initial industry feedback on this approach in the near term, after which they are considering an emulation to test the use of this data with financial service firms and organisations that provide identity assurance services. TISA continues to work closely with government (GDS) to seek alignment of their solution and a version that is better suited to financial services.

2. Payments Transaction Data Sharing and Data Analytics

SUMMARY

The UK payment industry creates a very large, high quality dataset as a result of processing that takes place through interbank, retail and, currently to a lesser extent, electronic money (e-money) payment systems. This processing shares data from the payment service provider to the payment system using different message technologies.

While this data set has the potential to provide a multitude of powerful insights that could be used to address many areas of financial crime, this opportunity has remained relatively untapped to date. The emergence of more sophisticated ways to handle and query large amounts of data has opened up the potential for the industry to better exploit this data set in the interest of combatting crime.

This solution assessment summarises how this high-quality payments transaction data can be capitalised on to address Financial Crime. This paper is not intended to consider the merits of including additional data in the payments transaction message; this is a topic covered by another part of the Forum's work. We note there are significant legal questions to address in this solution, for example on data privacy and data protection, such as the need for customers' consent or facility to opt out.

There are a number of approaches that the UK industry could take to build a capability for transaction data sharing and data analytics. Each of these approaches will impact people, processes and technology across the industry and could raise significant legal questions in areas such as privacy and data protection. As a result of these far reaching impacts, the implementation of this capability will be built and will evolve over time.

SOLUTION DESCRIPTION

To enable transaction data sharing and analytics to address financial crime, the UK industry needs to establish the following capabilities.

- **Collaboration and data sharing:** greater collaboration between users of the inter-bank payments system e.g. BACS and Faster Payments, and/or the data owners, to share or pool their existing payments data in the interests of combatting Financial Crime. A pooled data set will open up new opportunities for identifying and preventing Financial Crime.
- **Data sharing compliance and controls:** establish the data sharing and data protection related rules, controls and considerations (for example syntax and lexicon for pooled data).
- **Application of analytical capabilities to extract actionable insights:** Analysis and extraction of the appropriate actionable insights that address each of the priority financial crime use cases.
- **Distribution of insights:** once extracted, make the insights available to relevant industry participants in a standardised usable format that is consumable by all types of PSP; large and small, established and new entrants. It is intended the insights are used in a manner to augment and leverage PSPs' existing fraud management capabilities, rather than replace existing capabilities.
- **Real-time vs batched:** Over a period of time it is anticipated that the intelligence will be able to provide real-time notifications to participating PSPs. In the initial phases it would likely be batched analysis providing after-the-event insights.

PROBLEM STATEMENT: SUMMARY OF THE ISSUES THIS ADDRESSES, AND THEIR PRIORITY

The core problems the working group has addressed are:

- How can greater clarity be provided around the data sharing/ pooling and using it for the purpose of addressing Financial Crime?
- Can the industry embrace an advanced analytics capabilities to make better use of the existing payments transaction data in order to address Financial Crime?

The solution delivers significant benefit by addressing the following issues:

- Identification of money mules accounts
- Funds repatriation to victims of crime – e.g. trace back funds that have been laundered
- Macro-scale: force particular types of criminal activity out of the UK payments system
- Flexible to be applied to an ever-changing range of criminal activities – ongoing changes in fraud activity, money-laundering activity

Furthermore the solution addresses issues and detriments addressed identified in the Triage report in February:

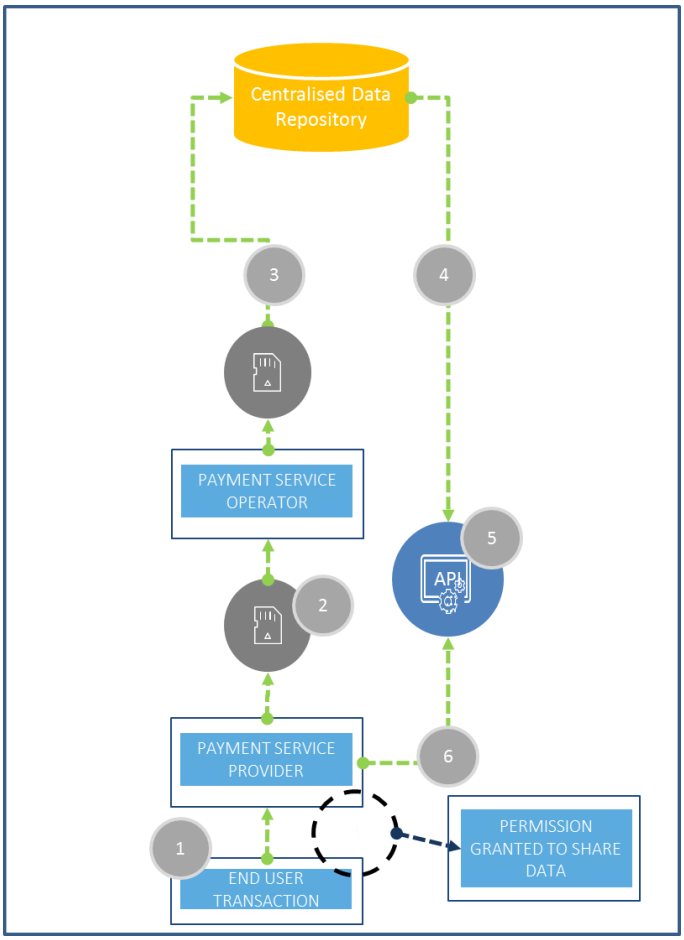
- Day-to-day concern about risk of identity theft, risk of fraudulent activity on an account
- Insufficient reference data and lack of knowledge share results in gaps in preventing financial crime: fraud, money laundering, terrorist financing, bribery and corruption
- Real-time payment risk assessment is limited, reducing the capability 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.

SOLUTION OPTIONS

The Working Group has identified two possible solution to create and maintain data sharing and analytical capabilities:

1. Central database, devolved analytical capability
2. Central database, centralised shared analytical capability (collaborative)

SOLUTION OPTION 1: CENTRAL DATA RESPOSITORY, DEVOLVED ANALYTICAL CAPABILITY



This solution proposes a centralised data storage facility while the analytical capability resides locally with the Payments Service Providers.

As message format data flows from Payment Service Providers and is processed by a Payment Systems Operator, the transaction data is captured. All of the fields that are collected should be stored in a centralised data storage facility and made available to Payment Service Providers via API functionality (preferably using Open API Standard as recommended by *Data Sharing and Open Data for Banks, A report for HM Treasury and Cabinet Office).* This will allow the Payments Service Provider to access this data and use for their own local analysis.

The message data would be captured and stored in a central data repository. The data that would be available for analysis via an API to a Payment Systems Provider would include all transactions that belonged to them and all transactions that pertained to them. To illustrate, in the example of Money Mule accounts that are operating across multiple Payments Service Providers, each of the Payments Service Providers affected would receive the data relating to the suspicious transactions, and only those transactions of the other PSPs.

The record stored in the central database would be only the message format data and any outcome data produced by the Payments Systems Operator. The data that is sent to the central data storage facility would not hold any personal data. The data should be anonymous to those who receive and

hold it but contain information or codes that will allow the PSP to identify individuals from it (linked anonymised data). Each Payments Service Provider would be able to analyse the data received and learn more in order to make their approach to Financial Crime more robust. For example, the PSP could combine the data from the API with existing data about complaints, customer service performance or geographical location.

As the solution evolves, there would be additional benefit gained by enriching the message format data with the Payment Service Provider's unique identifier and an outcome field to show whether or not the transaction had been successful and whether or not the transaction was suspected of fraud, or is fraudulent. As a baseline, a centralised data storage facility would be required to store payment transaction data from all payment types (e.g. BACS, CHAPS). Based on a combination of value and volume, Faster Payments, BACS and CHAPS would be the first priority for inclusion, with LINK and Cheques to follow on.

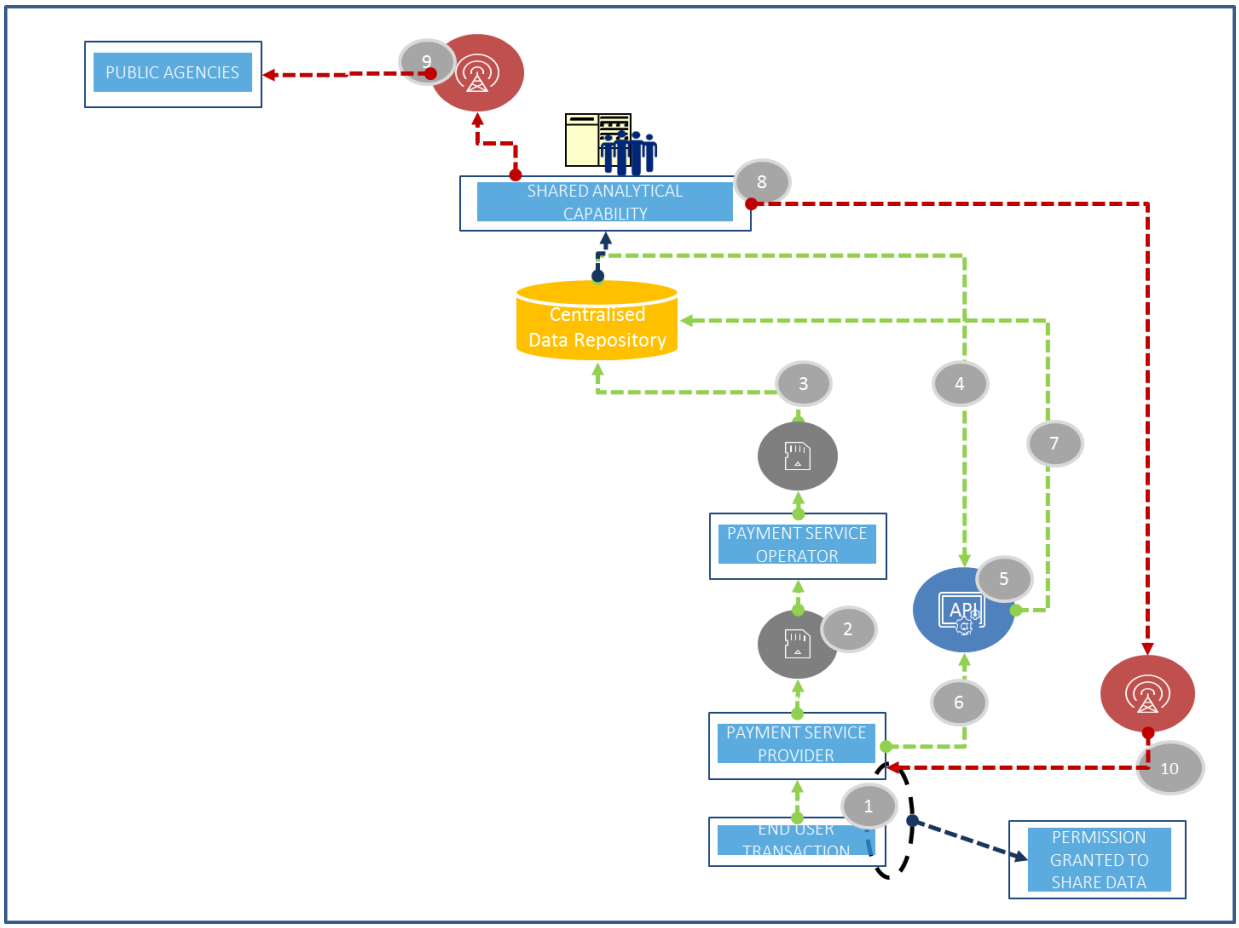
It is recommended that this data storage facility and its underlying data are overseen by an entity independent of the Payments industry. Public authority sponsorship and governance would ensure that robust controls are in place through the adoption of and adherence to a standard like the HMG Security Policy Framework, where guidelines on, but not limited to, Information Security and Personnel Security would ensure that the most sensitive assets are robustly protected. A fully commercial solution to provide this central storage capability is discouraged as it would be difficult to apply and enforce the right level of control and governance, and to ensure ongoing fair access for PSPs, of all sizes and all types.

The onus would still remain with the PSP to make the end-user aware of how their data would be used and to what ends. (A per-PSP delegation of responsibility to inform their client could dis-incentivise the individual PSP to on-board their clients to this process; whilst an FCA-mandated change of personal data use policies for all PSPs would remove this option for the PSP and also introduce a level-playing field across the payments ecosystem.)

Furthermore, this solution will not expect there to be a capability for centralised intervention; the PSP will remain responsible for taking action as a result of the insights produced by the capability – for example to close mule accounts or to proceed with repatriation of funds.

For each individual PSP, there would be internal implementation costs and external costs relating to subscription to the central data storage facility. Participation should be mandatory over time, but initially it would be the recommendation of the Working Group that this approach be piloted with a subset of PSPs to ensure controls and governance are sufficiently robust. After the pilot, participation should take a phased approach and will work towards 100% participation over time. To ensure that this is not cost prohibitive to smaller PSPs and new entrants to the payments market, the subscription model should be based on the size of the organisation and the volume of data that it processes.

SOLUTION OPTION 2: CENTRAL DATA REPOSITORY, CENTRALISED SHARED ANALYTICAL CAPABILITY



This solution proposes a centralised data storage facility and the analytical capability will reside centrally with a public body, taking a collaborative approach.

Similarly to Option 1, as data flows from Payment Service Providers to Payment Systems Operators, data is captured to support the requested transaction. The data that is collected should be stored in a centralised data storage facility. In this Option the proposal is for a centralised, shared analytical capability. This Collective Intelligence Hub would enable the industry to analyse the data received and identify conclusions/ insights based on an industry-wide view of payments activity, seeing more of the whole picture and thereby making the approach to Financial Crime more robust.

The centralised, shared analytical capability consists of shared, dynamic and evolving common industry logic and would be maintained by a centralised team of people. This will be a team of data scientists who will be informing and maintain analysis model, supported by a policy team which will be reviewing the outputs of an otherwise automated 'Black Box', yet still administered by a technical team, to inform or consult with relevant agencies.

As the records stored and analytical models evolve, it should be possible to stop fraudulent transactions at source and there should also be capability to run predictive analysis scenarios. This will allow the industry to take a more proactive approach to tackling Financial Crime. The shared analytical capability will be tasked with producing real-time notifications to subscribing PSPs to allow them to take the relevant action. This team will also liaise across the industry and government agencies, e.g. National Crime Agency (NCA, Department of Work & Pensions (DWP)), to provide data and insights into Financial Crime. It is not the responsibility of the shared analytical capability to intervene at an

end-user level; this will remain the responsibility of the Payments Service Provider or impacted agency. It may evolve over time that the central function will be able to intervene and stop fraud at source, but implementation and embedding of the capability will need to take place before a firm recommendation can be made on this approach.

The volume of transaction data that this solution can aggregate should be considered part of strategic critical infrastructure so it would be the recommendation of the Working Group that the capability should be overseen by a public authority e.g. the Home Office. While delivered through competitive supplier arrangements, public authority sponsorship and governance would ensure that robust controls are in place through the adoption of and adherence to a standard like the HMG Security Policy Framework, where guidelines on Information Security and Personnel Security would ensure that the most sensitive assets are robustly protected.

A fully commercial solution to provide this central storage capability is discouraged as it would be difficult to apply and enforce the right level of control and governance, and to ensure ongoing fair access for PSPs, of all sizes and all types. It is both acknowledged and recommended that the likely evolution of this solution is that permissions would be given to commercial entity or entities to work with the data or outcomes to provide value-add services at a cost to subscribing PSPs.

In parallel with this, each Payments Service Provider would still be able to conduct localised analysis on the relevant central data and learn more in order to make their approach to Financial Crime more robust or indeed understand the needs of their customers better.

Similarly to Option 1, the message data would be captured and stored in a central data repository which would be required to store payment transaction data from all payment types (e.g. BACS, CHAPS). Based on a combination of value and volume, Faster Payments, BACS and CHAPS would be the first priority for inclusion, with LINK and Cheques to follow on.

The data that would be accessible to a Payment Systems Operator would include all transactions that belonged to them and all transactions that pertained to them. This initially would be the message data from all payment types and the implementation priority would be the same as described in Option 1. In subsequent phases of a shared analytical capability, the data set must be widened beyond the current payments transaction data so that sophisticated analysis can take place e.g. geographical patterns and neuro linguistic analysis. However, it is worth noting that the evolution of this data set will lead to a scenario where records are no longer anonymised but coded. Coded data are identifiable personal information in which the details that could identify someone are concealed in a code, but which can be readily decoded by those using the data. This key based encryption will demand increased rigour around Information Security and the personnel involved in staffing this capability.

It remains the assertion that this approach requires the participation of all PSPs and as such PSP delegation of responsibility to inform their client could dis-incentivise the individual PSP to on-board their clients to this process; whilst an FCA-mandated change of personal data use policies for all PSPs would remove this option for the PSP and also introduce a level-playing field across the payments ecosystem.

For each individual PSP, there would be internal implementation costs and external costs relating to subscription to the central data storage facility and the shared analytical capability. As with Option 1, Participation should be mandatory over time, but initially it would be the recommendation of the Working Group that this approach be piloted with a subset of PSPs to ensure controls and governance are sufficiently robust. After the pilot, participation should take a phased approach and will work towards 100% participation over time. To ensure that this is not cost prohibitive to smaller PSPs and new entrants to the payments market, the subscription model should be based on the size of the organisation and the volume of data that it processes.

SOLUTION RECOMMENDATION

It is the recommendation of the working group that the industry adopts Option 2 as its preferred end-state. The shared analytical capability ensures primarily that Financial Crime will be emphasised as a societal issue, not simply a proposition benefit. The data set will be captured across PSPs, rather than intra PSP, which also ensure that the data set will be rich enough to allow the industry to take a more proactive, than reactive approach and have a more joined up approach to Financial Crime. Option 1 will only allow each individual PSP to improve only their approach, and potentially work together on an ad-hoc basis. This will potentially disenfranchise small and new entrant payments providers.

Both solutions require the Payments Service Provider to invest in API capabilities and while it may be an outcome of Option 1, Option 2 assumes changes to the message format or data collected over time which will have cost implications for both the Payments Service Provider and the Payments Service Operators. Nevertheless, the return on investment of a richer data set will allow enhanced ability to reduce the impacts of Finance Crime to the customer and the Industry. This will also allow the industry to be more flexible; enhanced analysis will allow for the development of machine learning models and the progression to an artificial intelligence capability. This type of capability will allow fraud to be stopped at source, and even before it occurs. This is not possible with Option 1, as analytical models will be built up by an individual PSP to serve the end-users of that PSP alone.

Both Option 1 and Option 2 will have initial set up costs but those of Option 2 would be higher given the addition of the shared analytical capability, which would be provided on an industry funded model. Option 2 would also have increased recurring costs; attributable to both the maintenance and running costs of the data storage facility and the costs of the security and personnel of the shared analytical capability. However, given the assumed increased return on investment, over time subscribing PSPs should recoup this investment through reduction in fraud, reduction in manual intervention on an increased scale to that provided by Option 1.

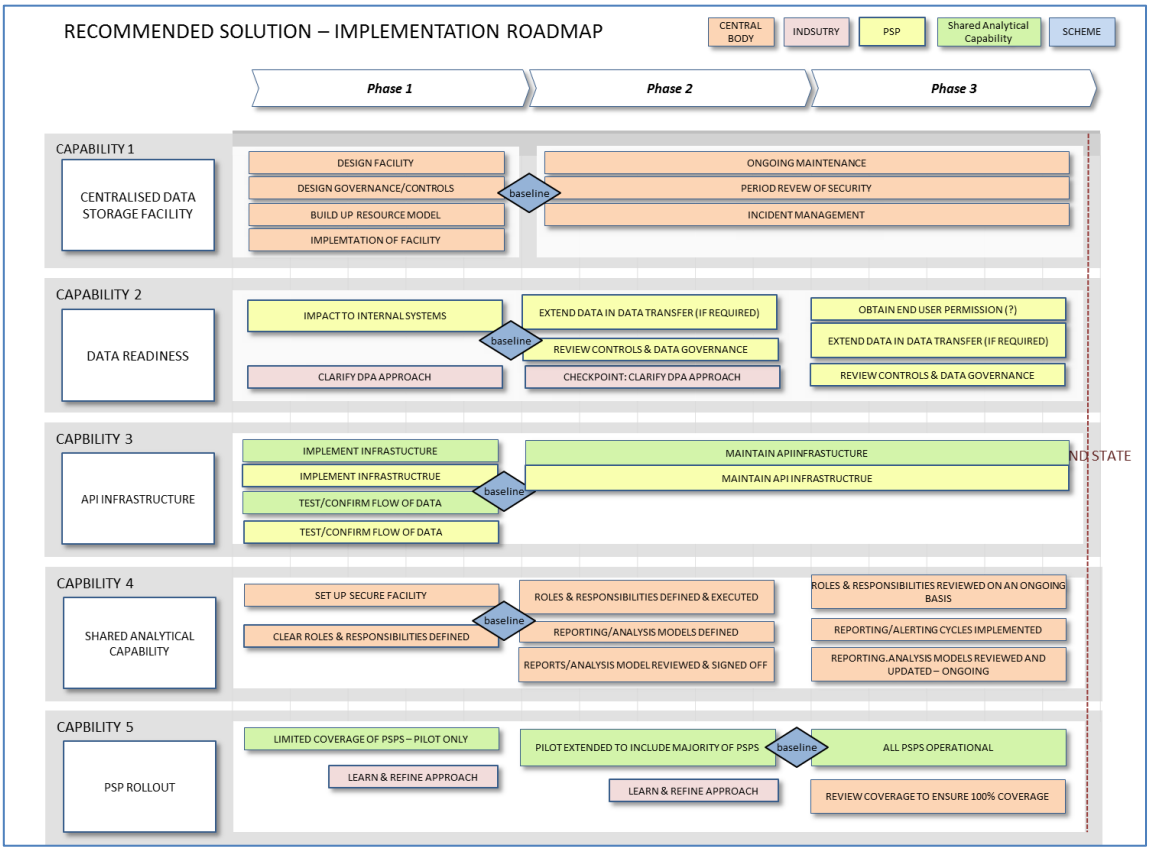
Option 2 increases the richness of data that will be shared from the PSP to the central storage facility, and ultimately the shared analytical capability, will be greater than that of Option 1. This will mean that there will need to increased controls, security and governance to ensure that data is not leaked or breached.

In developing this solution the team highlights that there are legal issues to address in respect of, for example, the Data Protection Act. One consideration is the volume of data being collected and processed compared to the volume of criminal transactions that are being identified. The benefits of this solution depend on access to the large dataset of payments transactions.

Finally, given the maturity of the industry and some of the players within it, it will be necessary to develop the solution over time, taking a phased approach. Rather than discarding Solution Option 1, this could be the starting point from which the industry can baseline itself and continue to build towards the desired end-state as set out in Solution 2.

IMPLEMENTATION APPROACH

The business capabilities are used to illustrate the solution maturity across the three maturity levels through five business capabilities.



- **Centralised Data Storage Facility:** Collation of data into secure data warehouse(s): could be complex and resource-intensive dependent on who is collating the shared data.
- **Data Readiness:** Agreeing rules and controls around data permissions: data owners to commit legal/data compliance resources. Based on existing industry initiatives e.g. VocaLink, this is believed to be relatively straightforward once all data owners are supportive and aligned around a common goal. There may impacts to the internal technology structures and systems of the subscribing PSPs over time.
- **API Infrastructure:** Development of open APIs in banking –information sharing is anticipated to deliver in a faster, cheaper way than historical, larger scale infrastructure projects. Each PSP would need to implement an API Infrastructure and this does presume a level of investment from the PSP.
- **Shared Analytical Capability:** Extracting data insights: relatively complex due to need for secure data warehousing, analytical tools and teams of sector relevant data scientists.

PEOPLE INVOLVEMENT AND ACTION

Users of the UK Payments networks/ payments data owners will need to:

- Provide access to payments data (e.g. Bacs and Faster Payments), to enable data sharing;
- Define how the fraud-based actionable data insights will be 'consumed' in order to combat crime and provide a more informed intelligence picture;
- Agree rules and standardised approaches for how the relevant PSP contacts the victim;

- Agree the rules and controls around how the payments data will be shared in order to comply with data protection considerations.

An organisation is required to operate and govern the data operations, analytics, modelling, and insights. This organisation will need to collate and aggregate the data, understand the fraud use cases, provide advanced analytics, secure data storage, and skilled data scientists to define and apply appropriate models and advanced analytics to extract appropriate data insights (real time or otherwise) that will successfully address each fraud use case.

This organisation would also engage with other authorities active in this area – for example there could be an opportunity to work with the National Fraud Intelligence Bureau (NFIB). There would also be regular engagement with the industry through the Payments Systems Regulator, the FCA and representatives from both the Payments Service Operators and the Payments Service Providers.

Other roles and responsibilities include:

- Payment Schemes: support the usage of data for purposes other than processing payments (i.e. addressing financial crime); both inter-bank schemes and card schemes.
- Public Authorities/ Law-enforcement: to track down the Organised Crime Group (OCG's) identified from this capability.
- Independent authority: to act as necessary to facilitate the effective working of all involved.

LEADERSHIP

Leadership is required in the following areas:

- Strategic direction and data collaboration: should be provided by a body that represents the financial crime related interests of the industry, the FFA for example. Regulatory support/direction would also prove helpful to encourage the participation from a high proportion of PSPs and industry participants.
- Data sharing compliance, rules and controls: should be created and managed by a body that represents the data owners from a data sharing and compliance perspective.
- Big data capabilities: should be provided by a trusted, secure and proven organisation that can provide subject matter expertise, has the ability to securely access and store the large volumes of payments data, is able to co-ordinate the various activities required to enable the data sharing and the extraction and distribution of actionable data insights.

COMMUNICATION

How will this solution be communicated to the people it affects?

- Impacted 'victims' (individuals/businesses) will be contacted by their PSP
- As part of agreeing the organisations that are required to deliver this solution, an appropriate engagement/communications approach will also be agreed.

DEPENDENCIES

The dependencies identified are:

- 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
- Approach in respect of the Data Protection Act for use of customer data in order to tackle Financial Crime e.g. whether customers would need to opt in

- PSD 2: New IT Security Requirements
- PSD2: 3rd Party Access to Payment Accounts and Payment Account Information
- PSD2: Access to Payments Systems – reducing barriers to accessing the Payments Systems need to be removed to ensure 100% subscription
- Open Banking Standards delivery

COST BENEFIT ANALYSIS (HIGH-LEVEL)

Success Metrics

The measurable benefits identified for the customer are:

- Customer satisfaction levels increase due to provision capability and framework to address financial crime within consumer, business and government to help protect victims and potential victims of fraud
- Time to process decreases due to improved ability to trace funds that have been lost, and to repatriate funds to the underlying victim

The measurable benefits identified for the industry are:

- Reduction in volume and value of payments executed as part of fraud or other Financial Crime
- Volume and value of money mule schemes identified and acted upon collaboratively
- Reduction in total UK losses in Financial Crime
- Reduction in volume of payment fraud cases reported to FFA, CIFAS, UK Police (Met and National Crime Agency)

The working group has identified costs to the industry as a whole to support the centralised capabilities and the costs to the PSPs to access those capabilities. The following tables detail the capex and opex cost categories relating to the implementation of Option 2.

Centralised Costs

The anticipated costs are shown in the table below:

Revenue Impact	Increase in end-user satisfaction
	Increase in end-user confidence
	Reduction in manual intervention
Cost Impact	Reduction in fraud losses
	Reduction in internal specialist FTE
	Reduction in processing times/effort
Capex	Site Acquistion
	Site Set Up
	Hardware
	Development Hardware
	Security
	Software - Development Software
	Software - API Management
	Software - Reporting
	Software - CM, QA, Test Manager
	Software - Firewall
	Software - Reference Data
	Software - Entity Extraction Tool
	Software - Others
Opex	Maintenance - Hardware
	Maintenance - Software & COTS
	Vendor Support - Software & Tools
	Vendor Support - Hardware/Servers
	Power
	Predictive Maintenance
	Facility Rent
	Facility Costs
	Staff Recruitment
	Staff
	Telecommunications
	Other Costs

PSP Costs

The costs that the PSP would likely incur are shown in the table below:

Revenue Impact	Increase in end-user satisfaction
	Increase in end-user confidence
	Reduction in manual intervention
Cost Impact	Reduction in fraud losses
	Reduction in internal specialist FTE
	Reduction in processing times/effort
Capital Impact	More robust data model
	Better analytical function without capex spend
Capex	Security
	Hardware
	Software - Development Software
	Software - API Management
	Software - Reference Data
	Software - Entity Extraction Tool
	Software - Others
Opex	Subscription Cost - Central Service
	Changes to Data Model
	Expert IT Staff - API Management
	Other Costs

This model has been informed by the following resources:

- **Oracle Pricing Model** – Exadata April 2016

www.oracle.com/us/corporate/pricing/exadata-pricelist-070598.pdf

- **APIDAYS/BANKING APIS: STATE OF THE MARKET REPORT**

https://www.axway.com/sites/default/files/report_files/axway_report_banking_apis_state_of_the_market_report_apidays.pdf

EXISTING OR IN-DEVELOPMENT SOLUTIONS

If this solution is progressed, we envisage a competitive market to find a provider for the solution, and a delivery roadmap building to an ultimate goal.

This major part of this section provides information on an initiative under way at VocaLink, which will have strengths and challenges in its approach that need to be assessed.

VocaLink has established a data analytics business, 'Payments Data Insight' (PDI). One of PDI's main business lines is the fraud and identity sector, as a result PDI has already established and proven many of the capabilities required to deliver the solution concept outlined in this document.

An example of VocaLink PDI's credentials in the financial crime space is the work done with a Tier 1 bank to identify and prevent social engineering fraud in the business to business sector. Further, VocaLink PDI is currently working on Proof of Concepts to address a number of financial crime scenarios. The capability being established is flexible and lends itself to being able to address a wide range of fraud use cases.

The capabilities established by VocaLink include:

- **Data sharing rules and controls ('Gresham'):** VocaLink has established the 'Gresham Council', an independent body that has representation from the data owners associated with the Bacs and Faster Payments payment networks. The Gresham Council exists for the sole purpose of agreeing the rules and controls around the sharing of the payment data for use cases such as financial crime.
- **Access to payments data**: subject to the appropriate permissions from the data owners, PDI is developing insights and solutions using fact-based data from 11bn yearly transactions, £5trn worth of annual payments transactions, 90% of UK salaries and 70% of household bills. This has the benefit of removing the cost/risk of data owners having to physically move data into a separate data warehouse.
- **Separate secure data warehouse**: capable of managing the very large volumes of data. VocaLink PDI has established the appropriate data security compliance controls, including the use of secure data rooms.
- **Advanced analytical tools**: capable of processing the very large volumes of data, insights are generated using machine learning models, rules based engines and other cutting edge techniques.
- **Industry skilled data scientists**: experienced in applying 'big data' techniques to payments data in the interests of addressing financial crime.

One consideration for in-development/ existing solutions is the approach to in-house ('on-us') transactions, and accessing other account information or activity that would add context to the insights being drawn.

Looking more broadly, there is a wide set of industry bodies, and related initiatives that are relevant to this set of activities. These provide opportunity for collaboration and potential acceleration. Related initiatives and bodies include:

- Solutions in development by industry participants e.g. SWIFT, VocaLink, Experian
- 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

3. 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 not only result in additional work, but can cause operational problems and unnecessarily delay genuine customer business. More importantly however, efforts to tune sanctions screening systems to overcome poor quality list entries increase the opportunity to generate false negatives (failing to stop 'bad' customers).

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; this also correlates to the distribution of names populated on sanction lists. Therefore organisations need 'secondary identifiers' to assist in reducing the number of matches and to help validate who someone is in their due-diligence process. The requirement is to have the integrity of well populated secondary identifiers that help to 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 is imperative when it comes to client on-boarding and payment screening. Compliance teams need this data to aid in their potentially subjective judgement when carrying out customer due diligence (CDD) and investigation of screening hits. Without this data the risk is to slowdown operations. One of the primary reasons for this is that the PSPs will be required to request further information from the consumer or counterparty incurring cost

and time. Worse still, incorrect decisions regarding flagged payments (e.g. wrongly concluding that a flagged payment is a 'false positive') could lead to financial crime.

SOLUTION DESCRIPTION

Principle

An Advanced Sanctions Data Model has been developed by the UN 1267/1988 Security Council Committee. 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.

The solution proposal is for the industry to engage with the PSR to purse an agenda for the HMT to adopt the Advanced Sanctions Data Model.

Scope

The scope of the improved sanctions list will be for all entries i.e. 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 I.e. cater for regardless of size, channel and payment services they provide.

Additional to the implementation of the Advanced Sanctions Data Model, other proposed initiatives for the payments industry to pursue, working with the PSR and HMT to address the detriments identified, are:

A. Data Improvements

- 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.
- Engage with HMT to improve the population of accurate data within sanction lists (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.

B. Process Improvements

- Industry work with HMT to create a single common Sanctions list with consistent format and structure
- 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. Assumptions

- A standard for how data is captured accurately (identity and verification) for PSP consumers, will improve the matching capability against sanction lists

Additional solutions identified

Sectoral and Dual Use Goods List

In addition to the need to improve the HMT list, an additional detriment was identified during the 31st May workshop for which a solution was suggested.

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 Advanced Sanctions Data Model, to create a new list to include these regulatory requests.

COST BENEFIT ANALYSIS (HIGH-LEVEL)

Benefits

Adopting this data model for HMT Sanctions data would not only enable improved detection capabilities for FIs, but also help eliminate the frequent errors that find their way onto the lists.

Promoting the Advanced Sanctions Data 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 on companies of improving the data quality of sanctions would also include:

A. Data Improvement Benefits:

- *Assists in managing risk:*
  - 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.
- *Increases 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.
- *Improves customer experience:*
  - If the CDD process gains more confidence (through improved sanction data) this in turn will increase the turnaround time to on-board a new client and thus the experience for the customer.
- *Fewer false positives:*
  - Speed up and improve efficiency of operations e.g. payments / account opening:
    - Increased sanctions screening detection accuracy and efficiency resulting in quicker identification of matches and a reduction in customer impacts from false positives.
  - Less compliance resource reliance – more manageable workload
- *Reduced risk of false negatives:*
  - Increased accuracy in identifying sanctions
  - Improved protection from Money Laundering and Terrorist Financing

B. Process Improvements Benefits:

- Sharing common best practices and challenges will be a benefit by:
  - Highlighting of existing issues in the data

- Sharing methods on managing matches and CDD, which can lead to better screening throughout the industry

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 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)

4. Trusted KYC Data Sharing and Storage Repository

INTRODUCTION

Know Your Customer (KYC) is the due-diligence and regulations that financial institutions 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 the FIs and the customer.

Indeed a number of initiatives have come to market in recent years offering financial institutions 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 FIs and customers.

The KYC data sharing solution aims to provide a utility to improve management of AML and Fraud risks in the following main ways:

- Reduce duplication of efforts by both FIs and customers where information may be submitted and used many times
- To provide a capability to reduce complexity whereby KYC information can be requested, collected and provided in standardised ways
- To provide greater transparency of FI, customer and UBO (ultimate beneficiary organisation) information in order to mitigate AML and Fraud risks more effectively
- To increase the speed of customer transaction execution and on-boarding, to the benefit of the FI and customer alike
- To standardise the industry approach to AML and KYC

There are a number of approaches that the UK industry could take for KYC-as-a-service. Each of these approaches will impact people, processes and technology across the industry and could raise significant legal and regulatory questions. As a result of these far reaching impacts, the implementation of this capability will be built and will evolve over time.

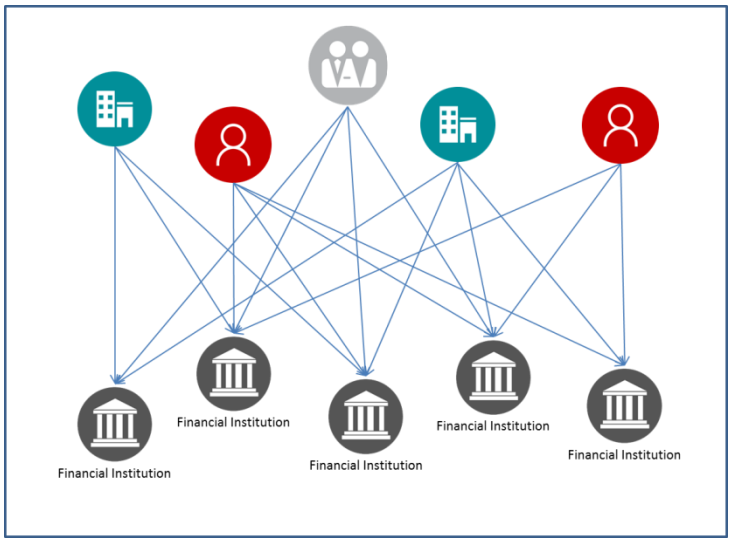
This solution assessment summarises how a 'KYC as a service' utility can address the problems identified. It is recommended that a Central KYC Utility is created that consolidates specific, non-competitive KYC into a shared services utility structure for member institutions. This will improve management of compliance and commercial risk, improve service to customers, and generate efficiencies. The overall objective of financial crime reduction can be achieved if more and more transactions happen with adherence to an agreed standard of KYC, with no exemptions. The payments community should engage with the wider financial services industry and authorities to advocate a KYC utility approach.

The focus of the analysis has been on the business customer (small, medium and large businesses). Following the proposed introduction of a standards-based approach to individual identity & verification, there may be less of a compelling case to include the individual customer in this solution. (This paper is not intended to consider the merits of approaches to identity; this is a topic covered by another part of the Forum's work.)

PROBLEM STATEMENT: SUMMARY OF THE ISSUES THIS ADDRESSES, AND THEIR PRIORITY

Currently, each FI 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 onboarding 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 FIs leads to significant duplication of efforts as KYC information collation process must happen for each FI and customer relationship that exists. A customer will provide KYC information to many requesting FIs and different FIs will ask the same customer for KYC information.



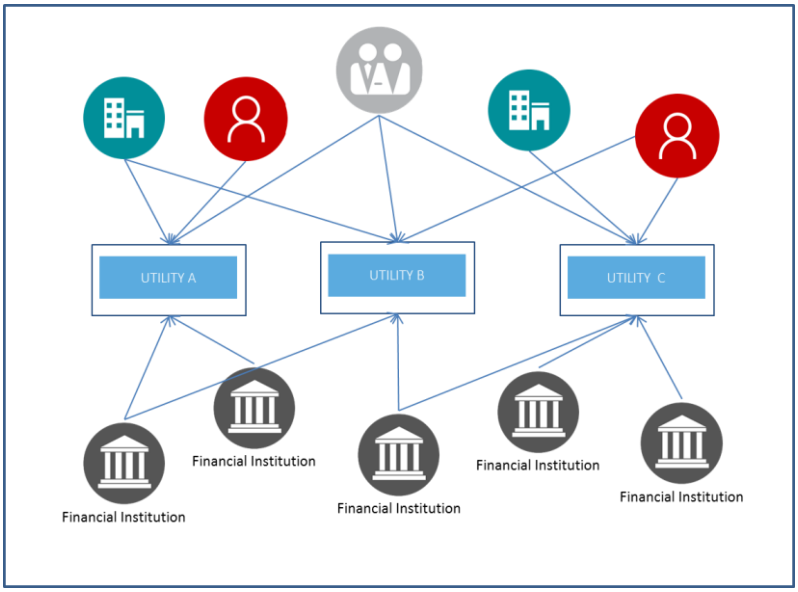
Current state KYC: many FIs to many customers

The problem is compounded further when considering the international domain where KYC information is needed to mitigate an AML or Fraud risk relating to a customer or Beneficiary that originates or is domiciled outside the FI'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.

Whilst the KYC process is clearly complex and costly for FIs to implement, it also has negative impacts on the customer. KYC processes take time for the customer to undertake and unless correct information is available it can delay genuine business activity.

A number of initiatives and utility-based solutions have come to market in recent years offering financial institutions the opportunity for greater industry collaboration and the ability to retrieve customer information related to such activities such as onboarding. There are multiple players who co-exist and compete among themselves. They specialise in specific areas, for example geography, line of business etc.



Current commercially delivered KYC-utility model

While this provides a good service for a subscribing FI, there is a logical argument against having multiple utilities to perform the same function. FIs are also not able currently to satisfy their needs by subscribing to a single utility; they need access to many. And few of the utilities available cater to operations across multiple geographies and jurisdictions.

Furthermore the solution addresses issues and detriments addressed 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 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

SOLUTION DESCRIPTION

The solution required should provide a way of sharing KYC among FIs in way that AML and KYC would become core competencies of any institution. The competencies that should be part of this solution:

- Collect, verify and classify KYC data
- Help support onboarding, compliance and ongoing maintenance
- Maintain Data compliance and controls
- Establish and improve KYC Standards
- Provide access to all FIs, in payments and wider financial services.

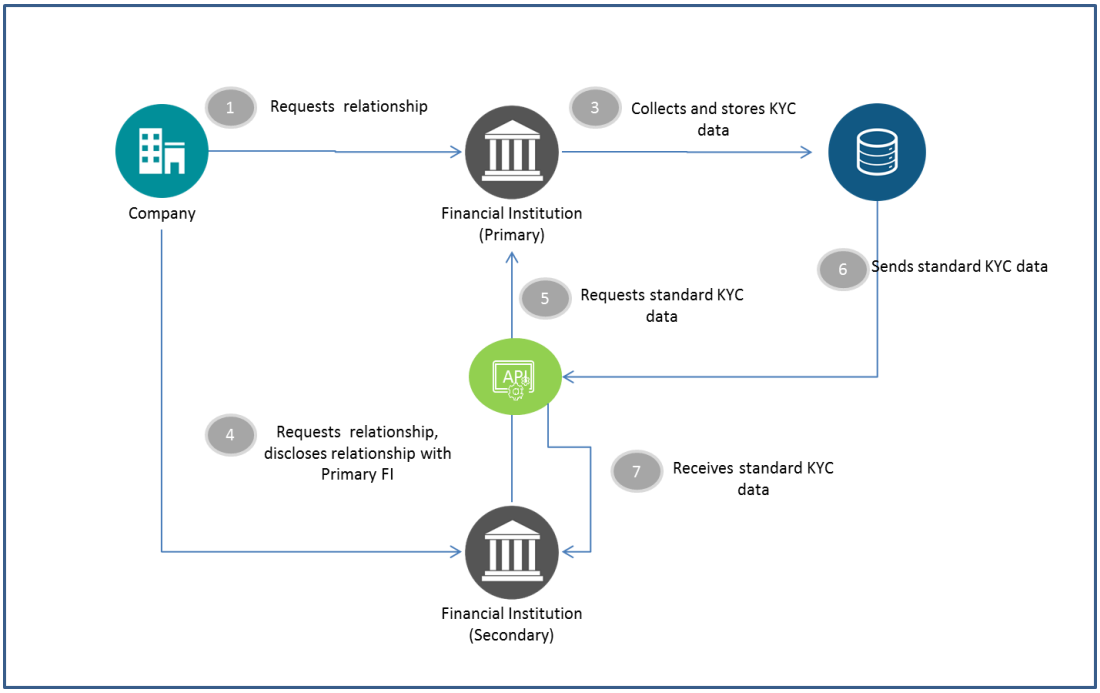
SOLUTION OPTIONS

The Working Group has identified four possible solutions to KYC utility capabilities:

1. KYC Sharing between Financial Institutions
2. Customer to Financial Institution
3. Central KYC Utility Repository Model
4. Central KYC Utility Registry Model

SOLUTION OPTION 1: KYC SHARING BETWEEN FINANCIAL INSTITUTIONS

This solution proposes that institutions share KYC information amongst themselves. When a customer first establishes a relationship with a Financial Institution, the FI should perform collect, classify and verify KYC information based on the nature of the relationship that customer has requested and the type of customer. This institution becomes the primary holder of that customer's KYC data. If the customer instigates a relationship with another FI, this secondary FI can request the KYC data of the customer from the primary FI.

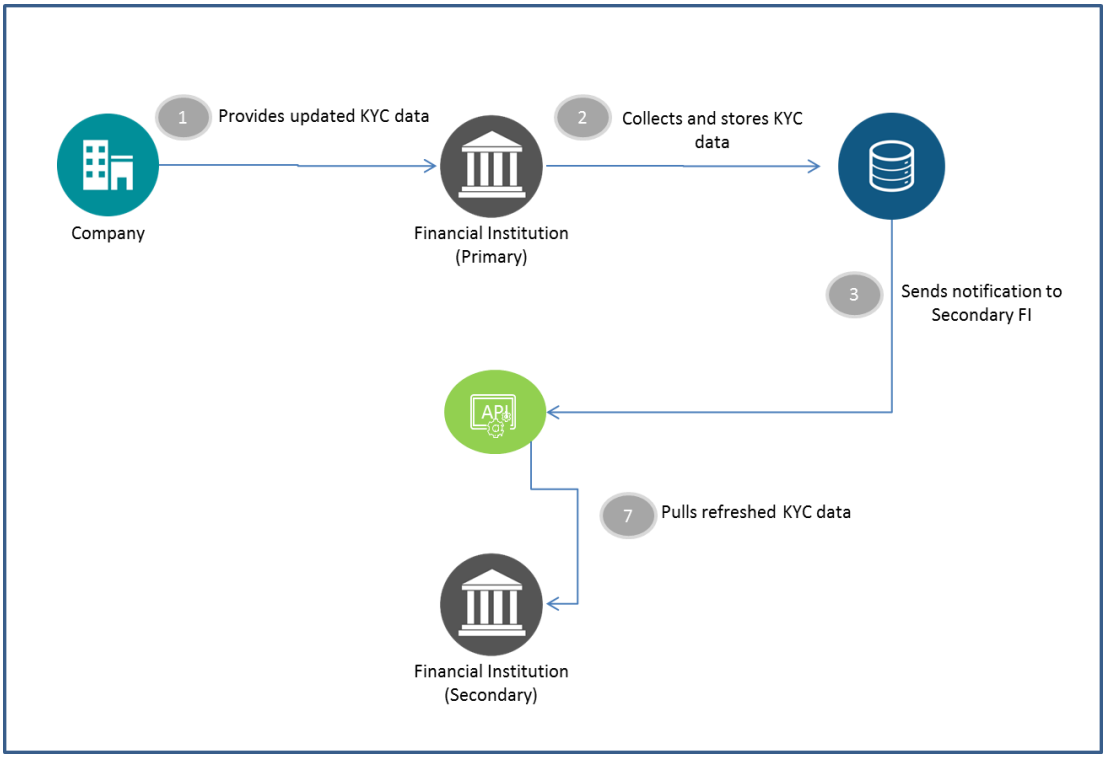


For an individual customer, the benefits of this solution are negligible following the introduction of a centralised identity but for a business customer, there would still be benefit in sharing KYC data.

The data passed will be the regulatory minimum standard of KYC data for that type of customer. Based on the current regulatory requirements, for example, a corporate customer (other than regulated firms) would need to provide full name, registration number, registered office in country of incorporation and business address. Additionally, for private / unlisted companies, they would need to also provide names of all directors (or equivalent), names of individuals who own or control over 25% of its shares or voting rights and names of any individual(s) who otherwise exercise control over the management of the company. The firm should verify the existence of the corporate from either confirming the company's listing on a regulated market, conducting a search of the relevant company registry or obtaining a copy of the company's Certificate of Incorporation

In this solution, each FI would still be able to perform their own risk assessment and potentially capture more data that would not be shared with other institutions. For example, for private / unlisted

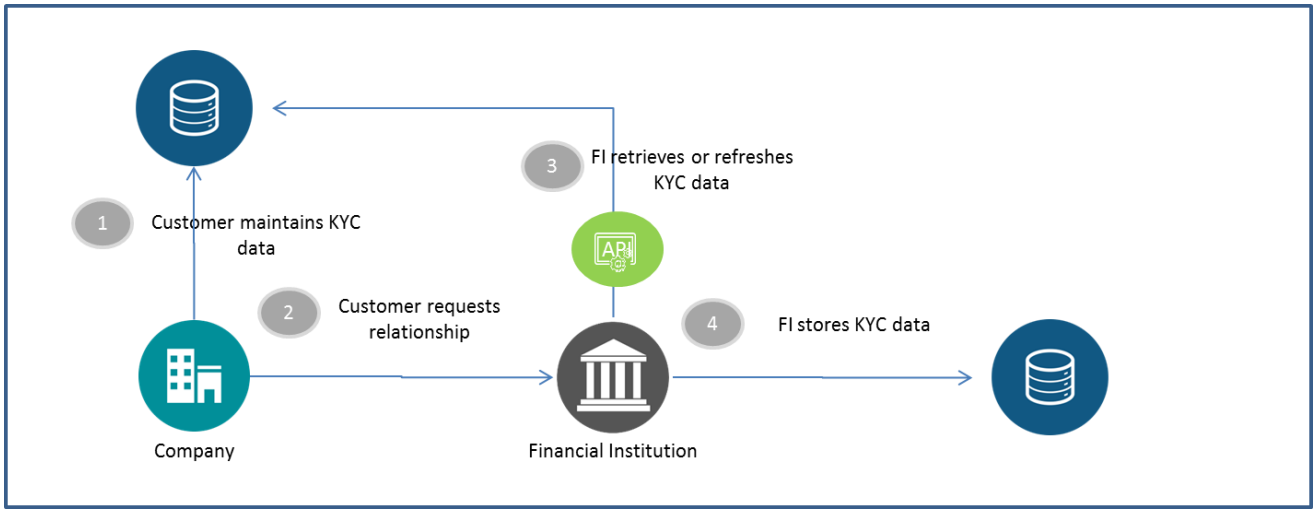
companies, the firm may decide, based on their own risk appetite, to verify one or more of the directors as appropriate in line with the Customer Due Diligence (CDD) requirements for individuals.



For ongoing requirements, if the primary institution updates their KYC data on a customer, a notification is sent to the other secondary organisations to pull the updated documents into their own repository.

SOLUTION OPTION 2: CUSTOMER TO FINANCIAL INSTITUTION SHARING

Solution Option 2 puts the onus on the customer to create and maintain a KYC master record and the FIs pull the information to satisfy onboarding, compliance and ongoing maintenance.



When a customer first establishes a relationship with a Financial Institution, the FI should perform 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 pulled from a central repository that is maintained by the customer.

For an individual customer, the benefits of this solution are negligible following the introduction of a centralised identity but for a business customer, there would still be benefit in sharing KYC data.

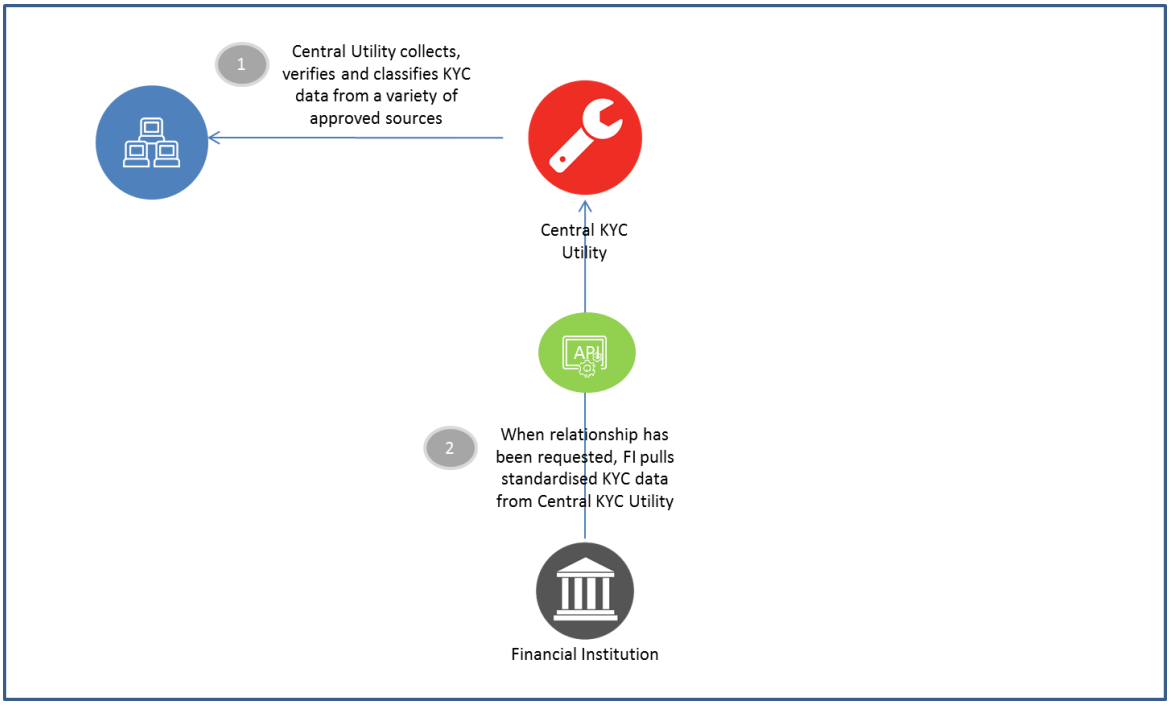
As in Option 1, the data passed will be the regulatory minimum standard of KYC data for that type of customer. In this solution, each FI would also still be able to perform their own risk assessment and potentially capture more data that would not be shared with other institutions.

For ongoing requirements, if the customer updates their KYC data, a notification is sent to the FI to pull the updated documents into their own repository. The onus remains on the FI to review that information and perform any additional internal checks.

This type of mode where the onus is on the company leads to non-mandatory participation and, as such, this lends itself to a competitive, rather than a collaborative approach. There are a number of commercial solutions that currently operate in this manner and it is a service which is provided at a fee. They allow the customer to set permissions to control whether or not, or in some cases how much, data is disclosed to requesting institutions.

SOLUTION OPTION 3: CENTRAL KYC UTILITY REPOSITORY MODEL

Solution Option 3 proposes a central repository that stores the data and documents required to support a financial institution's KYC procedures.



When a business customer first establishes a relationship with a Financial Institution, the FI would request the KYC data from the Central KYC utility. The Central KYC Utility would provide KYC data on that customer that has been classified and verified KYC information based on the type of customer. This utility becomes the primary holder of that customer's KYC data but each subscribing FI should provide any updated information provided by the customer back to the Central KYC Utility. The central KYC capability will also allow the customer to upload the necessary CDD documents and data evidence.

There is a point of discussion that the customer should give the FI explicit permission to retrieve their KYC data from the central utility. However, there is also an argument to say that there would be benefit in an FCA mandated change to data use policies for all FIs. If a customer requests a relationship and KYC data is required, the customer has implied their permission to access their KYC data.

A per-FI delegation of responsibility to inform their customers could dis-incentivise the individual PSP to on-board their clients to this process. However a regulator-mandated change of personal data-use policies for all FIs will remove the option from the FI and introduce a level-playing field across payments providers.

As in previous options, the data passed will achieve at least the regulatory minimum standard of KYC data for that type of customer. Each FI would also still be able to perform their own risk assessment and potentially capture more data that would not be shared with other institutions.

The method of delivery would be through a cooperative solution which will be a more acceptable proposition to international audiences than any Government or for profit structure. Given the diverse nature of payment provider, it is important that the cost implications to payment providers are to be affordable particularly to those at the bottom of the pyramid. The service should be free for the providers of information e.g., asset managers, hedge funds, corporates and the consumers of

information are charged a fee which could be either a flat fee or combination of license fee and variable fee.

SOLUTION OPTION 4: CENTRAL KYC UTILITY REGISTRY MODEL

Similarly to Option 3, Solution Option 4 proposes a central entity but conversely proposes that this is not a repository that stores the data and documents required to support a financial institution's KYC procedures but provides an index to point the FI to where this data can be sourced e.g. from another FI. Once a customer's data exists in the utility, member financial institutions can access and leverage the information for their own individual KYC requirements.

SOLUTION RECOMMENDATION

It is the recommendation of the working group that the industry adopts Option 3 as its preferred end-state. This is primarily because this option consolidates KYC, a non-competitive process, into a shared services utility for member institutions. This approach conceptually underlines that Financial Crime should be emphasised as a societal issue, not simply a commercial/proposition benefit.

It is also recommended that this solution is targeted at the business customer, given the assumption that an identity & verification solution will address this requirement for the consumer customer.

It means that robust KYC data is collected, verified, classified and maintained by a central entity and this ensures that the member financial institutions to adopt a consistent practice for their KYC activities.

Unlike Option 2, the onus is not on the customer to provide data and allow permissions on that KYC data. There are commercial solutions in existence today which allow business entities to use this service. This is dependent on the business entity opting in to this solution. KYC can only become 100% robust if participation in such a scheme is mandatory.

All of the solutions proposed require the FI to invest in internal data transfer capabilities and assume changes need to be made by the FI to receive and store the KYC data. Option 3 would be a higher cost solution to implement in terms of the spend on the Central Utility but the return on investment will allow enhanced ability to reduce the impacts of Finance Crime to the customer and the industry and ultimately justify the set up and maintenance costs of such a service.

It is worth noting that a registry (Option 4), rather than a repository (Option 3) approach, would be less costly to set up and maintain but it would not remove the effort of collection of data from the FI. It would also prove difficult to resolve conflicting entries. For example, if a customer has existing relationships with two FIs and has provided conflicting documentation, a registry could tell the FI where the records exist but does not provide assurance that one is right and one is wrong.

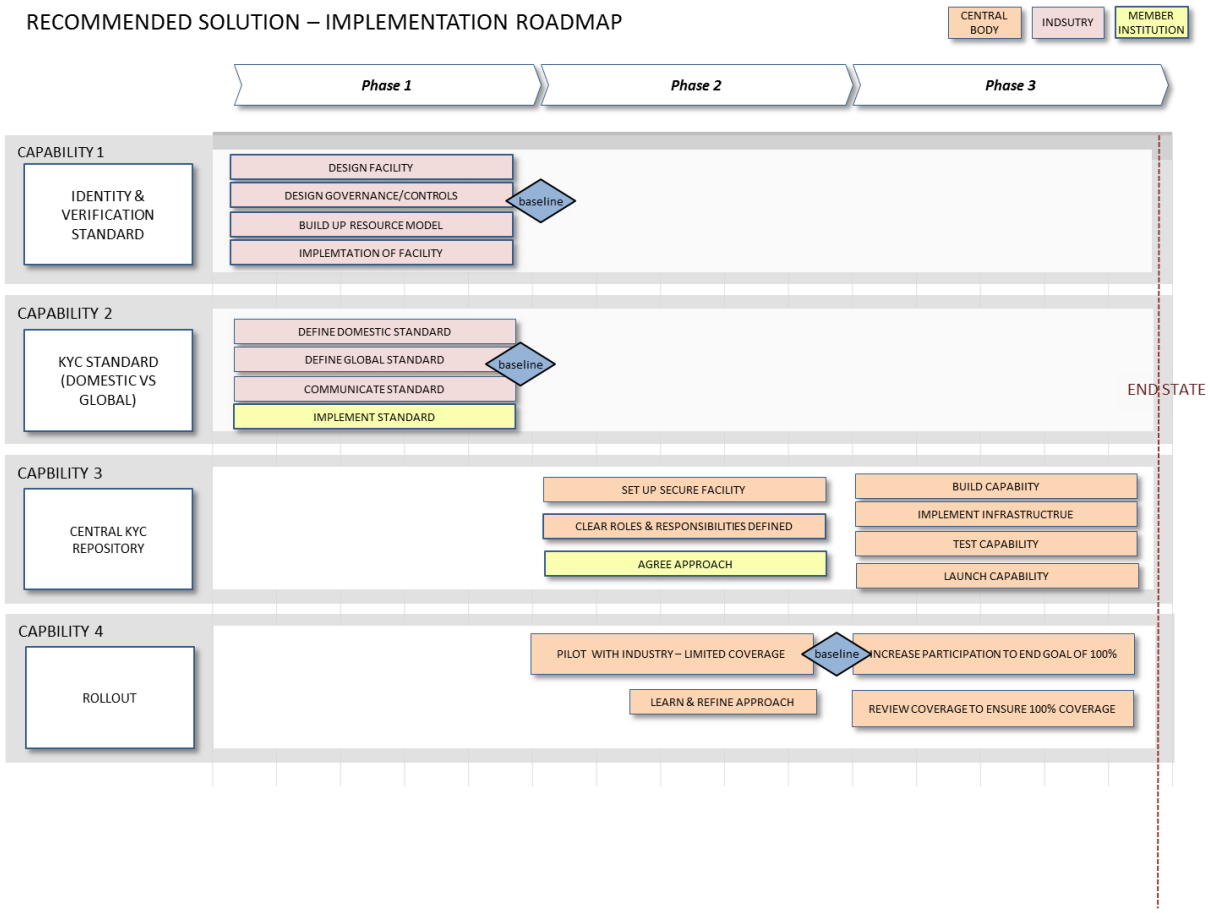
Further consideration of the scope and business case for this solution proposal will be required following the implementation of the proposed identity & verification solution and other dependencies (such as other regulatory/industry initiatives in flight). This should re-assess the approach to sharing KYC information as the implementation approach for this utility is complex, and the timescales involved will not be insignificant.

In terms of approach, a competitive approach could potentially preclude this service being provided as a shared service that is available to all who require it. The method of delivery would be through a cooperative solution and as such this service would become available to all institutions. It is important that when pricing this model, the principles of inclusion are still maintained. Solution 3 ensures that AML and KYC would become core competencies of any institution.

IMPLEMENTATION APPROACH

The following diagram shows the proposed implementation roadmap for Option 3: Central KYC Utility Repository. It looks at how the capabilities will evolve over time. The key capabilities covered are:

- **Identity & Verification Standard:** this must be developed as a precursor for any KYC build to allow business case benefits to be maximised
- **KYC standard:** Define and agree a minimum standard for KYC
- **Central KYC Repository:** Build technical infrastructure to support the utility
- **Rollout:** A piloted approach to be extended to all FIs over time. This will also include collection of existing KYC data via a variety of approved sources.



It is worth noting that there are some implementation challenges:

- Achieving precise definition and standards is difficult in absence of specific regulatory guidelines
- Variations/conflicts between global, regional and local requirements creates additional difficulties
- Requirements keep evolving with little time given to institutions to comply with changing requirements - maintaining the solution on an on-going basis therefore can be challenging
- Information security is another significant challenge
- Sharing of risks and liability between utility provider and financial institutions will require more granular analysis

PEOPLE INVOLVEMENT AND ACTION

The following areas would be required to implement a Central KYC Utility:

- Common agreement within the international community of the detriments and the benefit of the solution
- Comprehension and possible adaptation of data protection laws to enable a Central KYC Utility to function
- Design of Central KYC Utility in order that it addresses the needs detailed within the detriments without breaching data protection / security laws
- System & process changes to enable the contribution, collation and consumption of Central KYC Utility information
- Adoption of Central KYC Utility in order that information is contributed and available in sufficient volumes that can be consumed by others for benefit
- Detailed financial model of Central KYC Utility to cover design, build and on-going operational costs
- Regulatory support for a registry and usage of a trust based model

LEADERSHIP

Ownership of such a registry is likely to be sensitive due to data protection and security concerns. It's unlikely that a government or profit-driven organisation would be suitable to own or drive the core of such a solution. A cooperative approach is the most likely approach.

COMMUNICATION

As part of agreeing the organisations that are required to deliver this solution, an appropriate engagement/communications approach will also be agreed.

DEPENDENCIES

There are dependencies, most of which need to develop further or be delivered to move forward with a Central KYC Utility.

- Data protection legal frameworks. Regulatory consent to implement and use a Central KYC Facility
- Central ID as a utility with which to link the KYC information to optimise any delivery
- Approach in respect of the Data Protection Act for use of customer data in order to tackle Financial Crime e.g. whether customers would need to opt in
- PSD 2: New IT Security Requirements
- PSD2: 3rd Party Access to Payment Accounts and Payment Account Information
- Open Banking Standards delivery

COST BENEFIT ANALYSIS

The benefits of a shared KYC service or repository are:

- Reduced costs for people, process and technology, increased control and consistent client experience
- The use of shared KYC data would improve AML compliance
- Existing PSPs and FIs would be able to realise more systems consolidation and reduce their cost of processing

- Adopting a technical standard framework would make integration into the wider global KYC ecosystem easier and enable more cross border collaboration to address financial crime and terrorism funding. Although some data privacy impacts in this collaboration will also need to be addressed to realise this fully.
- Overall sharing of KYC data would result in reduced costs for the industry and increase the effectiveness for KYC, Fraud, AML and Sanctions processing

A report by VocaLink entitled 'Account Number Portability: A broader perspective (July 2014)' that was submitted to the Parliamentary Committee on Banking Standard, estimates that a Central KYC Utility would cost between £100 - £200m. A copy of this has been requested to provide more granular detail.

IMPACT: SUCCESS METRICS

The success metrics for the recommended solution are:

- For both FIs and customers; cost of compliance and reduction in fraud losses
- Reduction in FTE to support KYC
- Reduction in time taken to onboard a customer
- Reduction in time taken to perform compliance and ongoing maintenance of KYC

EXISTING OR IN-DEVELOPMENT SOLUTIONS

A number of initiatives have come to market in recent years offering financial institutions the opportunity for greater industry collaboration and the ability to retrieve customer information related to such activities such as onboarding. These solutions are:

- Industry collaborations – a utility developed by a specialist venture in collaboration with partner financial institutions
- Utility service providers – a utility or similar 'KYC as a service' offered by a single provider
- Jurisdictional utilities – a utility that is designed to undertake core due diligence on behalf of all the regulated entities within a single regional jurisdiction

The KYC Utility as a service has started with a small number of global services being offered. SWIFT provides a KYC Registry covering the Correspondent Banking domain that is growing rapidly. Reference data for instruments is being shared across a number of investment Banks (J P Morgan, Goldman Sachs, Morgan Stanley) to drive improved KYC. A number of start-ups offering different KYC capabilities have grown up in the last couple of years such as Trunomi, miCARD and iSignthis.

There are currently no solutions in development which aim to create a centralised KYC utility and all of the current commercial solutions have limitations of levels of participation, jurisdiction and cost model.

5. Financial Crime Intelligence Sharing

SOLUTION NAME: FINANCIAL CRIME INTELLIGENCE SHARING

PROBLEM STATEMENT

While all individual Payments Service Providers (PSPs) are actively implementing various measures to combat fraud, money laundering and other financial crime activities, there is limited inter-PSP interaction to work collectively to safeguard the consumers. There are several barriers to making it happen including regulations like data sharing restrictions, tipping off risk, data privacy, data protection and Proceeds of Crime Act among others.

There are questions posed from a PSP perspective around intelligence sharing:

- What do we consider to be intelligence sharing? What type of data are we sharing? Have we completed due diligence on this data? Is this data worth sharing and valuable?
- The nature of the data being shared, for example known crime events or data on suspicions ('black' or 'grey' data) and proportionality for the data being shared.
- Where suspicion exists, can we rely on other parties' assessment and information? What are the regulators' expectations? What are the views from relevant stakeholders (regulators, government agencies, etc.) on PSPs sharing data?
- What should be within the scope of financial crime intelligence sharing, for example should we include fraud, money laundering, terrorist financing, bribery and corruption, sanctions checking, and should this include the attack methods and precursor activity undertaken by the criminals.

There is wide recognition of the fact that increased sharing would very likely lead to an enhanced ability to prevent and detect financial crime. This can be demonstrated by government's the ongoing development of the Counter Fraud Data Alliance which is looking to build a mechanism to share confirmed fraud data between the public and private sector. The sharing of suspicious data (currently constrained by legislation) provides the biggest opportunity to identify hidden financial crime.

DETRIMENTS

There are a number of detriments identified by PSF working groups (extracted from the 25th February Forum Triage and Prioritisation Report) that are positively impacted by the solution proposals set out below:

- 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.
- Legislative constraints make it difficult for Banks to implement KYC, AML, anti-terrorist-financing requirements on their own customers, or on third parties.
- The impact of legal liability creates unnecessary bank secrecy preventing effective control of money laundering.
- The speed of money movements through the payment system, legislative and infrastructure constraints means banks cannot work quickly together to target mule accounts and to prevent funds being paid away when a customer realises a payment is actually fraud (authorised or unauthorised). This results in an inability to repatriate funds to the victim where it has passed through the 1st beneficiary account.

- 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 DESCRIPTION AND RECOMMENDATION

There are two levels of possible industry co-operation to fight financial crime activities:

1. Typology / trends level sharing between various PSPs
2. Transaction / customer level sharing and actions between various PSPs

Single View

A key enabler to achieve the above will be the creation of a single view of the financial crime landscape. The working group proposes a single repository (actual or virtual) to achieve this. It should contain all financial crime data (including articles of financial crime) which can be shared with PSPs to assist in preventing and detecting further financial crime.

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)

Each black or grey data record can also contain an 'articles of financial crime' used by the criminal to commit the crime e.g. malware code, addresses, telephone numbers etc.

Analysis of this information creates the **intelligence** and understanding of typologies. This will ensure the activity is not just about "safeguarding the consumer" but also combating the persistent threat of financial crime on a whole.

Currently, data and intelligence are held in a number of existing data bases focused on specific financial crime types (predominantly fraud). These rarely interface with each other because a number of the data bases belong to suppliers to which PSP subscribe for the value add services they provide.

- In order to produce a single view of an event or entity it will be necessary to gain agreement for suppliers to make their raw data records available for aggregation to enable a comprehensive assessment of risk or;
- The creation of a central point of entry and data pushed to suppliers.

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.

There will need to be a data dictionary that describes the meaning for each data entity held within the each typology.

Typology / trends level sharing between various PSPs

There do not appear to be any hurdles to share fraud or AML typologies between various PSPs. In the fraud world there are already agreed typologies being shared using a standardised methodology. The working group recommends that the industry consider expanding this approach and framework for other types of financial crime. In order to make this happen, there are a few components that will need to come together:

- Agreement on the typologies for AML, anti-corruption etc that will be beneficial for the industry to share;
- Definition of the standard / format / materiality in which the PSPs would share the information;

- The use of existing mechanisms (central repository / light infrastructure) to hold and share these typologies. E.g. BBA FCAS system for typologies;
- Rules/ mandates for sharing to avoid the situation of some organisations only benefitting without contributing.

Intelligence-sharing on the methods, tools and related techniques used in and to support the fraud (e.g. phishing and malware infrastructure) can greatly enhance PSPs' ability to adapt to changes in the threat and add context and information necessary for law enforcement. This includes Intelligence relating to attack methods. This can add in the creation or effectiveness of intelligence operations and criminal investigations, fighting financial crime in the long-term. Where a PSP maintains a fraud intelligence unit, effort should be made to unify the fraud data with related intelligence.

The Working Group believes that the more information that is shared, the higher the chance for PSPs to deter and prevent criminal activity in the payments systems. The Working Group recommends proceeding with the sharing of typologies and trends for AML and other financial crime, extending the existing light registry/ central repository. This should be accessible for consultation at proportionate cost for PSPs contributing in line with their payments volume, SAR reporting and fraud detection levels or other measure deemed more appropriate.

Commencing with Fraud typology sharing, the recommendation is to extend existing arrangements beyond the exclusive memberships of, for example, FFA-UK, CIFAS etc. The sharing of typologies should be done by PSP, channel and payment type using industry-agreed activity codes. In order to define the details of the standard to share the information, further work will need to be carried out.

Transaction / customer level sharing

The working group recommends the sharing of transaction/ customer level data and actions between various PSPs. This is to encompass confirmed, suspected and confirmed attempted crime. In addition it should include compromised card, bank and personally identifiable data which could be used to facilitate financial crime (all subject to a robust legal framework).

The data held within the single repository will be made available to PSPs and to the central payments data analytics capability (see other WG solution proposal).

PSP can use this data to use in assessing risk for:

- On boarding of customers
- Profiling of payment transaction risk
- Assisting in investigations and evaluation of suspicion/ building of evidence
- Funds repatriation.

A central data and analytics capability can use this data for

- Self-learning of decision science models providing predictive insights, alerts and real time prevention. (See solution 2, Payment transaction data sharing and data analytics).
- Once the entire set of fraud data is made available to that industry capability, the ability to stop payments before the money leaves the system will be significantly enhanced. The intelligence produced by the shared analytical capability will need to be specific and targeted in order for it to be reliably used to stop fraud. This will inevitably lead the PSPs to incur cost for digesting the insight received and deciding the best course of action (e.g., require a risk model to choose amongst not notifying the customer, texting them or calling them; and in this case, a call centre to deal with high risk fraud cases).
- The central solution capability will provide the infrastructure to enable the tracing and repatriation of funds subject to the necessary legal framework.

Funds repatriation

Whilst there is an industry gentlemen's agreement and regulatory requirements for the repatriation of funds to victims of unauthorised fraud, there is a lack of standard rules / governance for the organisations to work together to stop authorised funds leaving the system fraudulently (e.g. due to scams, social engineering). This is because this is no legal basis and therefore the infrastructure not utilised to make this possible. Despite this, efforts are made on a best endeavours basis despite the fact a bank risks criminal and civil liability in returning the funds to the victim who has authorised the relevant transfer.

There is existing work being undertaken (by FFA and the Joint Fraud Taskforce) to create a scheme which enables the following of money movements, recovery and repatriation of funds to victims, and has identified the necessary legal changes required. The capability required to enable this to happen is contained within solution 2. (Payments Transaction Data Sharing and Data Analytics solution).

In the repatriation scheme, the following components are being considered:

- Liability rules
- Clear contact points and authentication mechanism for inter-PSP communications
- SLAs for responding to / addressing the fraud enquiry and liability rules associated with SLAs
- Necessary legislative changes to remove barriers for data sharing.

The working group supports the work of the FFA UK and Vocalink, and should further address the removal of regulatory barriers which prevent PSP from repatriating funds to victims.

The sharing of suspicion

The hypothesis behind this solution is that the combination of suspicion across various PSPs will make a stronger case to assess the money laundering risk or fraud risk of an individual or entity or transaction. While there are strict rules around SARs and where they can be shared, there is an opportunity for the industry to share relevant factual data (not intelligence) and let the industry make better decisions where there is suspicion, especially in the case of suspected Fraud.

The industry will need to agree to definition of suspicion and at which point and format would there be data sharing. The solution will need to satisfy data privacy. There will need to be a consideration around what information / data is shared within the regulated sector vs non-regulated entities.

The working group recommend further work to with government to remove the regulatory barriers for sharing suspicion.

One of the critical success factors for these solutions to work is that all participants need to contribute in proportion to their customer base. Unless there is a central mandate for the participants to contribute, this solution may have limited adoption and therefore limited success. Across all intelligence sharing between PSPs, the group advocates a common, standardised approach and to include appropriate authentication for this information.

COST BENEFIT ANALYSIS

Benefits

In addition to addressing the detriments listed above, a number of other additional benefits are achievable from these solutions.

Customer perspective

- Financial inclusion – It is expected that better intelligence will also reduce the number of customer exclusions due to better refinement of models for financial crime detection.

Industry perspective

- Tipping off law prevents co-ordinated AML and CTF protection – The ability to tap into the payments analytics centre provides a means of leveraging data outside the PSP to enhance AML and CTF protection. This use case is partially met as it entails a dependency on the legal framework.
- Banks do not respond to money laundering reports from third-parties for a specific bank account – This use case is partially met by interfacing with the shared analytical capability.
- Criminals' use of mule accounts to receive payments into seemingly valid bank accounts – This will be reduced thanks to the confirmed fraud data collated and brought together providing a holistic view of confirmed fraud which is then fed into the shared analytical capability and accessible to PSPs.
- Remitting payments to more than one bank to defeat monitoring payments by remitting institutions (monitoring of payments) – This is partially met and should apply when at least two payments have taken place.
- Reduction in false positives – The enhanced data set available will lead to better intelligence and, in turn, it is expected that the total number of false positives will be reduced. This will not only improve customer experience but also reduce operational costs for the payments service providers.
- Access to confirmed fraud data – This will benefit smaller organisations that can't afford the cost of common repositories and users who continue to be targeted because link across PSPs isn't made.

Cost

At a high level, there are a number of cost drivers for the solution. More analysis needs to be done to populate the cost estimate detail. We'll use a similar methodology to the one used in 'Payments Transaction Data Sharing and Data Analytics' to specify the CapEx and OpEx cost categories relating to the implementation of the solutions recommended in the section above.

QUICK WIN VS SUBSTANTIAL PROJECTS

The extending of typology / trends level sharing for AML and fraud could be a quick win over the next year as there appear to be limited regulatory hurdles and infrastructure barriers to make this happen. The other solutions involve customer / transaction level data sharing and would take longer to gain consensus, but still going to be significantly faster than some of the other substantial projects.