payments strategy forum

Financial Crime, Data & Security Working Group report

Draft for discussion 7 April 2016

New version uploaded 8 June 2016

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

payments 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:

Many of the weaknesses of the payment system, which are exploited for financial crime, are related to the identity of the parties involved. Current solutions and rules are not applied consistently across payment types, across payment service providers (PSPs) and within the whole payment lifecycle. Criminals exploit these deficiencies to attack the weakest links in the financial supply chain, harming both individuals and organisations.

This proposal looks to establish a standard 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. By establishing basic, end-to-end standardisation, which is matched to business and risk model, each payment service provider will be required to document, and in some cases augment, its approach to each of the key capabilities, protecting both payment service users and the integrity of payment systems. Approaches to compliance will vary between payment service providers, with smaller organisations having typically a smaller scope and therefore a smaller burden.

This may result in the benefit of stimulating the UK economy by supporting FinTech, challenger banks and new entrants whilst allowing existing, large players to be more innovative and agile

This paper also recognises the need of the payment systems for ancillary solutions, both commercial and collaborative, which will give PSPs improved capabilities to manage identity risk in payments.

PROBLEM STATEMENT:

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 this include setting up direct debits on third-party accounts, terrorist financing, payments to 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.

Among the detriments identified by the Forum and Working Group which are solved by this solution are the following:

- Fraudulent or criminal opening of payment accounts
- Criminals misuse of third-party's accounts for receiving payments (UC-10) and for direct debit

- Difficult to know whom you are paying
- Consumer friction caused by security mechanisms prevents them making payments
- Payment systems inability to convey names of beneficiaries completely or reliably

SOLUTION DESCRIPTION

This proposal looks to establish a standard 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.

Technical Standard for Identity in Payments

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 in mid-2016.

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:

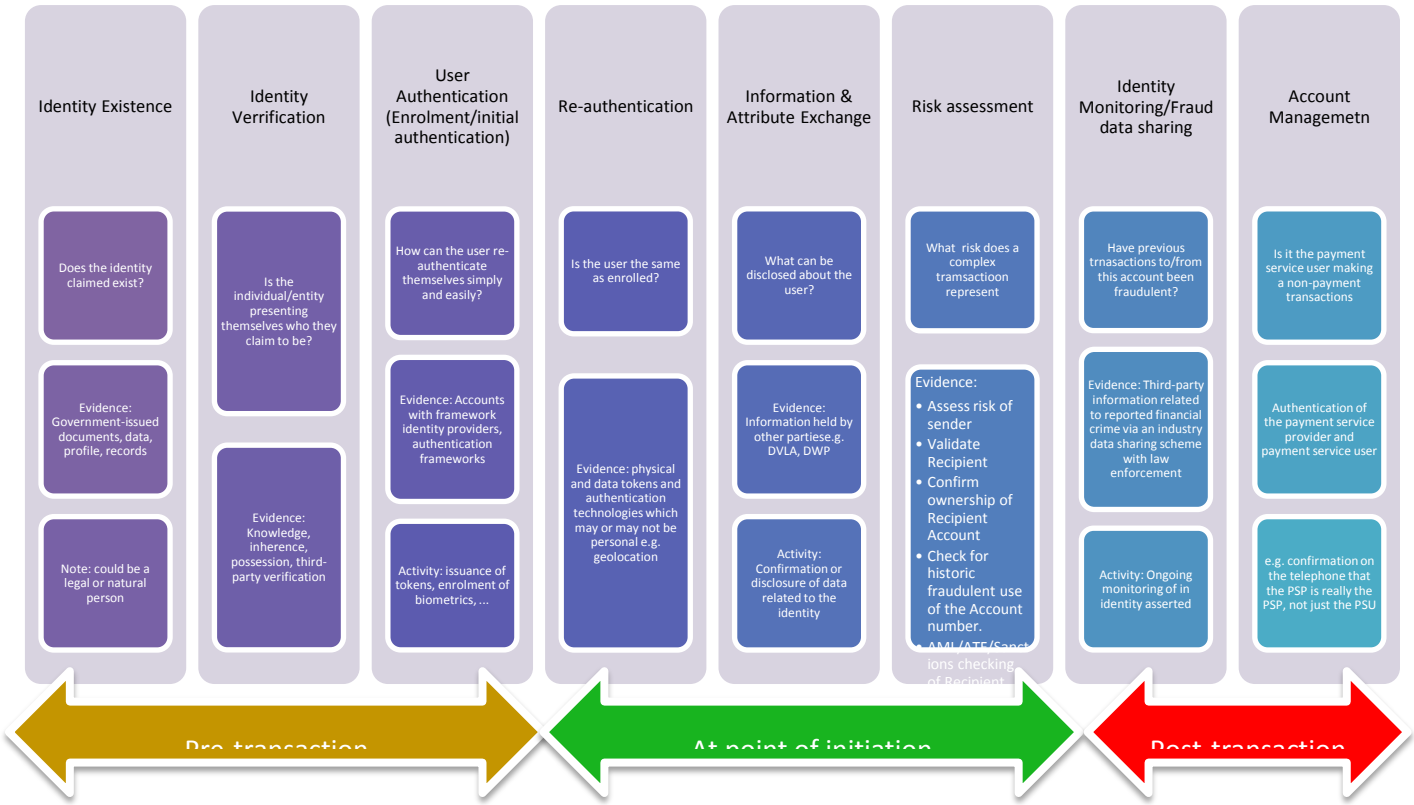
	Capability	Description
1	Identity Validation	Estimate confidence in whether a natural or legal person exists
2	Identity Verification	Confirm the (natural or legal) person presented matches the validated identity provided
3	Enrolment and Issuance	Issue, capture and/or enrol tokens, biometrics, knowledge-based security information
4	Authentication	Using one or more methods, authenticate the user presented is the user whose identity was verified on a previous occasion; also, where necessary, authentication of the payment service provider (or 3rd-party service provider) to the user
5	Information and Attribute Exchange and Confirmation	Confirmation and/or disclosure of key information related to the identity and transaction
6	Payment Risk assessment	Quantification of the risks presented by the identity-related components of a payment transaction
7	Identity Monitoring and Reporting of Financial Crime	Detection of financial crime payment transactions and subsequent notification to prevent potential or inform active transactions
8	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

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:

- 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

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.

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
Validation of the identity of the receiver of a payment instruction	Many financial crimes relate to the inability of PSPs to check the account details of the recipient of the payment transaction (including payment cardholder, direct debit payer/debtor and cheque paying accountholder). Some commercial solutions exist for some payment types however these are impaired by lack of engagement by PSPs or customers	Commercial/ Competitive
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[1] 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

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

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 Technical Standard • Establish how PSP supervision will occur
Payment Services Provider (PSP)	• Following publication of the Technical Standard, assess existing operations against the Technical Standard and ensure identity and risk assessment methodologies of each PSP meet the Standard
Solution Providers, Government	• Continue to develop solutions for each capability requirement to meet the Technical Standard

LEADERSHIP

A competent independent authority is seen to be the body to establish technical 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 Standard by consultation
- Mandate the Standard as part of UK regulation of PSPs or via primary legislation if necessary
- Monitor and enforce the Standard 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 a Technical Standard for payment service providers will overlap with a number of other pieces of existing and proposed legislation and rules[2] 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 not enforced by regulation or 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 a potential that some change to the process of regulation of payment services 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 standard 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

[2] See Appendix for a list of some relevant regulations, legislation and standards

organisations with fewer payment mechanisms and simpler business models will be faced with a less onerous workload.

COST BENEFIT ANALYSIS (HIGH-LEVEL)

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	Payment Systems Regulator/ FCA and payment service providers	
Maintenance of Technical Standard	Payment Systems Regulator	BSI would maintain in conjunction with industry collaboration

The 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

Estimates of the cost of developing a standard are £150,000-£250,000 if using an external agency in addition to the cost of consulted and consulting organisations.

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

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

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.

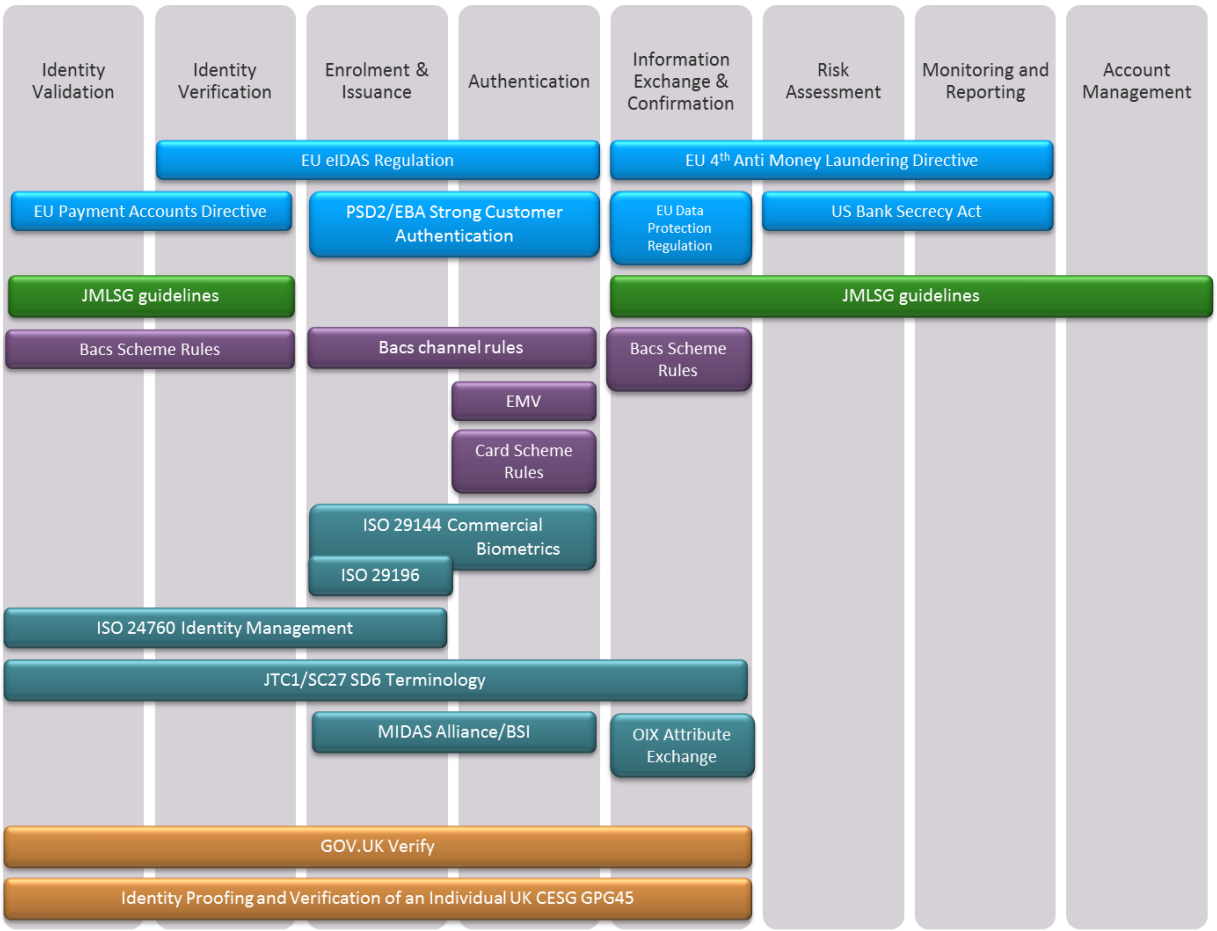


Diagram showing mapping of some rules, legislation and standards to capabilities (not exhaustive)

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.

1. *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.

2. *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

3. *Identity Verification*

   f) The individual presenting him/ herself 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.

4. *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

5. *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.

6. *Information and Attribute Exchange and confirmation*

p) 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

7. *Payment Risk assessment*

q) 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

8. *Identity Monitoring and Reporting of Financial Crime*

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

s) 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

9. *Account Management*

t) 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

u) 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.

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. *Identification of a Payment Service Provider to a Payment Service User*

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. This is particularly important where contact is made over the telephone or internet. It is vital that payment service users can trust communications with their payment service provider; this is currently an area targetted by criminals to defraud consumers.

2. *Confirmation of identity of a recipient*

When a payment is being made to or a collection made from a payment account, it is necessary to confirm the owner off the account is as expected. A solution is therefore require to confirm ownership of account receiving transactions e.g. Direct Debit payee, card account holder, recipient of credit transfer/RTGS payment. This would, as a minim, confirm the name and address 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). Commercial solutions exist for some payment types but not all.

3. *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.

4. *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 Verify, be undertaken to utilise work already under way in this area. It is also possible that commercial schemes may exist

2. Payments Transaction Data Sharing and Data Analytics

SUMMARY

The UK payment industry creates a very large and high quality data set as a by-product of processing payments through the BACS, FPS and LINK transaction networks. This data set has the potential to provide a multitude of powerful insights that can be used to address many types of financial crime, however to date this opportunity has remained relatively untapped. The emergence of 'big data' analytical capabilities has opened up the potential for the industry to better leverage this data set in the interests of combatting financial crime.

This solution assessment summarises how this high-quality payments transaction data can be capitalised on, using 'big data' capabilities, to address Financial Crime and Anti-money laundering.

This paper is not intended to consider the merits of including additional data in the payments transaction message; this is a topic covered by a separate Solution Assessment (see section 3).

We note there are significant legal questions to address in this solution, for example on privacy and data protection, as the vast majority of the data being pooled would not be related to criminal activity.

The meaning inferred by the term 'data sharing / pooling', is intended to reference the activity of individual PSP's submitting data into a secure data warehouse (central or distributed), where it is collectively analysed for the greater good of identifying actionable insights to address financial crime.

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 BACS and Faster Payments payments systems, 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 'big data' capabilities to extract actionable insights:** the storage of shared data in a secure and compliant data warehouse(s), provision of 'big data' advanced analytics capabilities (e.g. machine learning models) and skilled industry-relevant data scientists to extract 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, both existing players 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.

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

The core problems the working group has addressed are:

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

Key customer issues and detriments addressed:

- The sharing of payments data and application of 'big data' capabilities provides the ability to address a wide range of financial crime issues such as identification of money mules, funds repatriation and a risk-based approach to intervention. Furthermore big-data capabilities are flexible and can be applied to an ever-changing range of financial crime use cases, addressing ongoing changes in fraud activities and other financial crime risks.
- This additional protection and detection can be provided without increasing obstacles in account opening and account access / operations.

PEOPLE INVOLVEMENT AND ACTION

Who needs to do what to make this solution a reality?

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;
- agree rules and standardised approaches for victim contact;
- 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 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 (centralised or distributed), 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).

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

Who should own implementing this solution and what are their key actions

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.

SYSTEMS AND PROCESSES

What systems and/or processes will need to change?

- Process: data owners will need to agree the data sharing compliance, rules and controls – for example standards approach to data syntax and lexicon;
- System: data owners will need to physically move data to the organisation that is storing and analysing the data. The effort on the data owners in this regards can be reduced if the existing payments processor is leveraged as they are well placed to physically access the payments data once appropriate data owner permissions have been provided.
- System/process: a standardised approach will need to be agreed to confirm how PSP's can consume the data insights that are extracted from the sharing of the existing transaction payments data (e.g. how will a PSP's fraud operations teams can best leverage the data insights).

DEPENDENCIES

Are there other things that need to change to enable this solution to work?

- 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, e.g. whether customers would need to opt in, under the existing law.

EASE OF IMPLEMENTATION (OVERALL)

Overall views on how straightforward/ complex to deliver: technology, processes, stakeholder commitment.

- Agreeing rules and controls around data permissions: data owners to commit legal/data compliance resources. Based on existing industry initiatives, this is believed to be relatively straightforward once all data owners are supportive and aligned around a common goal.
- Collation of data into secure data warehouse(s): could be complex and be PSP resource-intensive dependent on who is collating the shared data. For example, if an existing payment processor is used the effort for data owners is materially reduced due to the payment processor's ability to access the majority of required data (subject to obtaining the appropriate permissions from the data owners).
- Extracting data insights: relatively complex due to need for secure data warehousing, 'big data' analytical tools and teams of sector relevant data scientists. These capabilities exist within 3rd parties for the industry to leverage. A centralised model will ensure that not only are the data insights being created for the benefit of the industry, but that the most efficient model is adopted.

Some views in the working group sessions centred on the overhead, legal issues and potential high cost this solution would bring, and suggested an approach levering PSPs' existing fraud detection engines. Another consideration for data sharing is the development and impact of the Open Banking initiative to develop open APIs in banking – and whether solution(s) around information sharing could be deliverable in a faster, cheaper way than historical, larger scale infrastructure projects. This would be a hypothesis to be tested, potentially as part of detailed design.

COST BENEFIT ANALYSIS (HIGH-LEVEL)

Benefits to customer (consumer, business, government dept, charity etc)

- Victim protection: provides capability and framework to address financial crime within consumer, business and government to help protect victims and potential victims of fraud.
- improved ability to trace funds that have been lost, and to repatriate funds to the underlying victim.

Benefits to industry

- By creating greater transparency by pooling payments data between all/most PSPs, the industry can collectively force targeted criminal activities out of the UK payments systems. This will reduce the opportunity to execute financial crime, benefitting all PSPs – as well as customers and society overall.
- Quick wins: Opportunity to secure 'quick win' due to the existence of existing industry initiatives

- Flexible: provides data sharing framework and advanced analytics capabilities that are flexible and so can be applied to address multiple financial crime use cases now, with the flexibility to adapt to address changing fraudster tactics.

Costs to deliver/ to operate

- To be determined once relevant parties have been engaged
- Proof of Concept: relatively low cost to run a proof of concept to test the concept

SECURITY

Security is based on ensuring the organisation that holds the shared data has all the necessary security and data protection systems, rules and controls in place. Liability for data breaches is a key concern.

IMPACT: SUCCESS METRICS

For each fraud use case or method, a set of analytical success criteria would be set (e.g. identify x% of frauds with Y level of false positives).

The solution approach also requires target metrics for identifying money laundering and terrorist financing.

COLLABORATIVE OR COMPETITIVE

This require collaboration across the data owners in order to share the data. It also requires collaboration across the industry to confirm the use cases to be addressed and how the insights extracted will be consumed.

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

QUICK WIN VS SUBSTANTIAL PROJECTS

Quick wins are possible by leveraging the Money Mules proof of concept being discussed between VocaLink, FFA-UK and 12 UK PSPs.

3. Enhanced Payment Transaction Data

PROBLEM STATEMENT IN RELATION TO ENHANCED DATA

Today's financial payment messages follow a number of formats for processing payments for validation, routing and settlement, for both inbound and outbound. FIs are required to process these varied formats and their related metadata to define both the attributes and the data flows required for the payment. The data in the current standards enables the processing of payment transactions – and also can be used to reduce financial crime (fraud, money laundering, terrorist financing) through pre-transaction, transaction processing and post-processing analytics.

However, there are a number of challenges in the current payment message standards:

- Referencing the account for payment in a payer request is for the intended payee;
- Referencing the purpose of the payment is as expected by the payer;
- Ability to refund monies from fraudulent or criminal activities to the originating payer;
- Restrictions in data attributes available in fixed length message formats;
- Reference of customer payer and payee data inclusion;
- Reference data fields used by FIs for processing data are open to error or fraudulent use.
- Sharing of Risk data in payment messages;

The working group has assessed the opportunity to enhance the data in these payment message formats to enable the PSR to ensure payment systems that provide superior service to their end-users, are secure, adhere to standards and produce a reduction in financial crime while ensuring new entrants and innovation are also enabled.

SOLUTION DESCRIPTION

A variety of formats has evolved across the different systems both in the UK and internationally, including the following.

Message Standards	Usage	Platform Services	Data Observations
ISO 8583	Inter-Bank, Cards	FPS, Visa, Mastercard, Link, Amex, Diners Club	Messages tend to have fixed length fields Note was modified for FPS
Standard 18	Inter-Bank	BACS	Bulk Credits , Debits, fixed length Reference Data Limited
SWIFT MT and MX	Inter-Bank , Business to Bank, Swift Messaging	CHAPS, Settlements	Number of different message types Widely used MX is ISO2002 standard
ISO 20022	Inter-Bank , Business to Bank	CASS, SEPA, ISA transfers	Framework – Recognised internationally, Many Message Types XML Single and Bulk handling

To enable transaction data sharing and analytics to prevent financial crime by enhancing the data in payment messages would require the following:

- Identification of payer and payee added to the payment instruction;
- Use of digital identities in payment messages;
- Identification of both credit and debit account numbers. For example, by addressing the Account Number structure the use of reference data by some FIs could be avoided;
- (to address use of Reference data by some FIs today);
- The use of the identification, account numbers to set a minimum process authorisation;
- Use of digital identities in payment messages;
- Geo location data;
- Purpose of Payment or Remittance Data;
- Standards for Reference Data.

Many FIs and PSPs are investing in IS02002-based messaging, mainly in the high-value payment world. Swift Messages are migrating from MT to MX which is an ISO20022 standards based set of messages.

The Working Group considered a technical framework payment message standard and its adoption by the FIs in the UK payment industry.

- Its goal is to enable the sharing of data across PSPs and greater collaboration to combat financial crime.
- The addition of existing data in payment messages to enable migration to a common standard.
- The use of a technical format that enables straight-through-processing (STP), secure payments and supports analytics and the use of data science for the prevention of financial crime.
- Allows new entrants to the payments industry and enables innovation and competition.

Concerns were raised about the cost of changing a large number of payments systems to accommodate enhanced data. Alternative approaches could place the additional data in a repository available 'in the cloud' for example, and keeping the payment systems as they are.

BENEFITS IN RELATION TO SPECIFIC DETRIMENTS

The analysis has captured a number of customer detriments and other issues which this Enhanced Data solution can address. These are listed here, together with the ability of this solution to address it.

- Tipping off law prevents co-ordinated AML and CTF protection - Partially met; more information provided will empower addressing detriment, empowers people to act on suspicions.
- Unnecessary Bank Secrecy Enhances Money Laundering - Account details for returned payments - Met: End to End data flow through the chain, combined with data sharing will address i.e. the enhanced data flows all the way through the payment system.
- Real time payment risk assessment (e.g. for DWP, HMRC payments) – Met, if we have central capacity. Enhanced Data needs to be combined with analytics to address.
- Data-limits on the extent of input and output data and no third-party reporting – Met, directly.

- Criminals use mule accounts to receive payments into seemingly valid PSP accounts – Partially met: Enhanced Data will help identify unknown mules
- Anti-money-laundering provisions are paper-based and react too slowly to new information on accounts and accountholders - Partially met by Enhanced Data and shared transaction data
- Difficult to know who you are paying leads to misdirected payments and fraud - Met
- Criminals use third-party accounts in their control to make and receive payments – Partially met
- PSPs cannot make reliable risk decisions on third-parties because they cannot be 100% sure of the identity of the counterparty and hence information about them – Partially met
- PSPs and businesses/government cannot reliably check ownership of all payment accounts: Partially met: Enhanced Data can be linked to LEI (legal entity identifier

OTHER BENEFITS

In addition to the above, we have identified other benefits delivered by enhanced data and a new payment message technical standard for the UK.

- Opportunity to reduce the number of payment message types formats and reduce the cost for existing FIs through more systems consolidation.
- The cost of entry for new PSPs would be greatly reduced with simpler IT and Operations processing.
- It would enable an improvement in AML compliance due to enhanced data.
- Enhanced data showing the whole transaction and compliance to a technical standard would help drive down the Operational costs of processing.
- Adopting a technical standard framework would make integration into the wider global payment ecosystem easier, enabling more cross-border collaboration to address financial crime (e.g. terrorism funding). Although some data privacy implications will also need to be addressed to realise this fully.
- Enhanced data will also help determine where liability lies in transaction processing errors and refunds.
- Overall the use of enhanced data should see a reduction in mule accounts.
- The use of enhanced data would allow the funds to be returned to the right owner when monies are seized due to criminal activities as the entire chain of flow would be more easily determined.
- The adoption of an enhanced data and technical standard and framework would allow BACS and FPS to be simplified.

Overall a technical standard and enhanced data, combined analytics of shared existing payments data, would have significant impact on fighting financial crime while reducing costs and maintaining innovation.

PEOPLE INVOLVEMENT AND ACTION

In order to take the solution for enhanced data forward the following actions are required.

Creation of a Technical standard and framework for enhanced data will require further analysis. This could be achieved through a period of consultation and setting of the technical standard. (IS020022 is considered as a potential foundation to build the new UK standard.)

The technical infrastructure of the UK payments industry is complex and also its impact of the UK economy is significant. Therefore, deeper analysis of the movement to single technical framework is required in order to develop a migration approach and any required regulatory changes.

The technical standard for enhanced data needs to link to new digital identification and authentication mechanism (see Identification solution option). This will require analysis and a working party to drive this deeper and look at the wider government digital identification plans. Additionally, features such as geo-location data should be built into the standard.

The creation of the technical standard and framework should deliver a recommend migration standard and path to support legacy formats. This approach would allow the creation of migration tools. A migration approach would allow the change to be managed by FIs without an unnecessary IT cost burden. Regulation impacts such as the EU's 2nd Payments Services Directive (PSD2) should be leveraged as an opportunity to drive the standard in UK forward. We also are mindful that the EU is pursuing an open-standards approach in its public procurement guidelines[3].

A number of proofs of concept should be undertaken by a consortium from within the UK payments community to address the technical feasibility of an enhanced data framework.

[3] https://ec.europa.eu/digital-single-market/en/open-standards

4. Financial Crime Intelligence Sharing

SOLUTION NAME: FINANCIAL CRIME INTELLIGENCE SHARING

PROBLEM STATEMENT:

While all the individual Payments Service Providers (PSPs) are actively implementing various measures to combat fraud and money laundering 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, proceed of crime act among others.

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

- What type of data are we sharing? What do we consider to be intelligence sharing? Have we completed due diligence on this data? Is this data worth sharing and valuable?
- Financial crime sensitive data also needs to be addressed. Can we rely on other parties information? What are the regulators' expectations?

SOLUTION DESCRIPTION

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

- Typology / trends level sharing between various PSPs
- Transaction/ customer level sharing and actions between various PSPs

There are different implications of the two scenarios depending on the type of financial crime prevention activity. Potential industry solutions could evolve as follows:

1) Typology / trends level sharing for AML and fraud

While there are significant regulatory barriers in sharing customer/ transaction level information, there do not appear to be any hurdles to share fraud or AML typologies between various PSPs. In order to make this happen, there are a few components that will need to come together

- Agreement on the typologies (both AML and fraud) that will be beneficial for the industry to share
- Definition of the standard/ format/ materiality in which the PSPs would share the information
- Central repository (light infrastructure) to hold and share these typologies
- Rules/ mandates for sharing to avoid the situation of some organisations only benefitting without contributing

2) Fraud event response

In case of a transaction fraud event reported by a customer, there appear to be lack of standard rules/ governance for the organisations to work together to stop the money leaving the system. While the efforts are on best endeavours basis, better guidelines and processes will improve the effectiveness of the industry against fraudsters. In the solution, there are a few components that will need to come together:

- Liability rules in proceeding with the fraud reporting
- Clear contact points and authentication mechanism for inter-PSP communications
- SLAs for responding to/addressing the fraud enquiry
- Standard formats for data sharing (to not get caught in data privacy act)

3) AML suspicious activity

The hypothesis behind this solution is that the combination of suspicion across various PSPs will make a stronger case (or not) to assess the money laundering risk of an individual or entity. 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.

The industry will need to agree at which point and format would there be data sharing and how will it not impede data privacy. There will need to be a consideration around what information/ data is shared within the regulated sector vs non-regulated entities.

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.

PEOPLE INVOLVEMENT AND ACTION

WHO	WHAT
TBD	• We are already sharing a lot of data under the legal framework; we don't want to create something where we are duplicating efforts. Thus, we need to be aware of what law enforcement are doing, 3D view of all the working groups in payment space.
TBD	• TBD
	•

COST BENEFIT ANALYSIS

There are a number of detriments (identified by PSF working groups) that are addressed/ positively impacted with these solutions.

Ref #	Detriment	Solution Solves?	Notes
UC-1	Tipping off law prevents co-ordinated AML and CTF protection	Yes*	Partially met as this entails a dependency.
UC-9	Unnecessary Bank Secrecy Enhances Money Laundering (…Account details for returned payments)	Yes	Clarification of this detriment is needed of information shared.
UC-13	Remitting payments to more than one bank to defeat monitoring payments by remitting institutions (Monitoring of payments)	Yes*	Partially met, should apply when at least two payments have taken place.
IS-16	Criminals use mule accounts to receive payments into seemingly valid bank accounts	Yes	
UC-2	Banks do not respond to money laundering reports from third-parties for a specific bank account	Yes*	Partially met.
IS-3	Customers, who become suspicious of having become a victim of fraud, cannot easily get banks to freeze recipient accounts (e.g. 'mule' accounts) to prevent money being paid away	Yes*	Partially met as more checks and balances are needed. E.g. governance, industry standards.
UC-14	Crediting consumer originated local payments to non-resident accounts held by foreign FIs with UK Banks	Yes*	Partially met.

In addition to addressing these detriments, a number of other additional benefits are likely

- Reduction in false positives – With better intelligence, 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.
- 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.

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 in the table below.

Participants	Set up/ Implantation Types of cost				Costs			Ongoing Benefits		
Bank	Infrastructures	Standard Cost	Project/Delivery	FTE	Subscription	IT	Legal	Scale for new entrants	Less False Positives	Less Fraud costs and losses
Non Bank										
New Entrants										
Regulator										
Trade Body										
Consumer										
Govt/ DWP										
LEA										

QUICK WIN VS SUBSTANTIAL PROJECTS

The 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 would take longer to gain consensus but still going to be significantly faster than some of the other substantial projects like enhanced data.

5. Trusted KYC Data Sharing and Storage Repository

SOLUTION NAME

Trusted KYC Data Sharing and Storage Registry (DSSR)

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

It is a regulatory requirement that financial institutions (FIs) have to collate and validate KYC information for each customer relationship (correspondent, corporate, individual etc) in order to help address AML and Fraud risks. 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.

Within an FI the extent of the KYC information collected and validated will vary depending upon the business relationship at hand and the KYC policy within the FI. This data 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. In effect there exists a many-to-many repeated work-task (where Customers will provide KYC information to many requesting FIs and different FIs will ask the same customer for KYC information). This problem persists as there is no mechanism to share KYC information and the implementation of the CASS Account Switching Service compounds this problem.

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 both the on-boarding and on-going BAU 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 can delay genuine business activity.

The logical case thus exists for a Data Sharing and Storage Registry (DSSR) style initiative to reduce KYC efforts for both FIs and customers, to provide greater transparency and thus risk reduction, and to increase the speed of customer on-boarding and transaction execution. Such an initiative has broad applicability for fraud and AML and spans both the domestic and international dimensions.

SOLUTION DESCRIPTION

A KYC Data Sharing and Storage Registry that would provide real-time sharing of KYC information between FIs, customers and Data Providers in order to help mitigate the Financial Crime Risks of all parties. The main capabilities of the solution are listed below:

- A single registry or exchange mechanism (*central or distributed*) where KYC information may be submitted, exchanged and re-used many times.
- Provision of an API gateway where KYC information can be sourced, collated and aggregated from a variety of sources both within our outside existing geographies.
- Implement a relationship model based on Government<>Corporate<>Citizen.
- Implement controls to ensure data privacy and security whereby the owner of the KYC information maintains control over who may have access to it.
- Implement standards in collaboration with FATF, JMLSG, Basel and Wolfsberg to facilitate adoption, innovation and competition.

BENEFITS

- The benefits of a shared KYC service or repository from a customer perspective 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.

The DSSR solution concept aims to provide a registry to help 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 on-boarding and transaction execution to the benefit of the FI and customer alike.

EXISTING OR IN-DEVELOPMENT SOLUTIONS

Sharing of KYC information 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.

PEOPLE INVOLVEMENT AND ACTION

In order to take the solution for DSSR the following actions are required.

Creation of a Technical standard and framework for KYC will require further analysis. This could be achieved through a period of consultation and setting of the technical standard.

The cost of such a shared service will require the economic rationale to be developed. This could be as simple as large financial institutions transfer the cost of infrastructure ownership and maintenance to the central service and pay a flat fee annually or based on usage volumes, sharing costs across the industry. However as KYC will still require to be carried out by FIs transfer is unlikely. It is more likely DSSR adopted by FIs' Corporate and Retail services would provide a better approach. This latter approach could be implemented iteratively and bring incremental benefits.

It is not clear that all FIs will wish to share data for KYC purposes as some of this risk assessment may provide client or FIs competitive advantage. Therefore, development of a standard will have to consider the type of risk data to be shared and the efficiencies of the shared service do benefit particular clients.

A new standard for KYC sharing could be broadened to Non Financial Service players.

The technical standard for KYC needs to be linked to new digital identification and authentication mechanism from T1. This will require analysis and a working party to drive this deeper and look at the wider government digital identification plans.

Analysis of the following main legal areas is needed in order to ascertain how viable the registry is now and what needs to change in order to make it viable:

- The data items needed and their use to achieve the benefits
- The storage and exchange methods between participants
- The data protection legal frameworks that exist on an international basis

In conclusion while the benefits of sharing KYC data are significant more analysis of how to address the challenges is required at this time.

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.

COMMUNICATION

TBC.

SYSTEMS AND PROCESSES

- On-boarding and periodic CDD processes for FIs to enable information to be both contributed and consumed from the DSSR.
- Transaction risk mitigation for both AML and Fraud where additional information may be consumed from DSSR.

DEPENDENCIES

Are there other things that need to change to enable this solution to work?

- Data protection legal frameworks. Regulatory consent to implement and use DSSR.

COST BENEFIT ANALYSIS

TBC.

SECURITY / RESILIENCE

High security and high resilience.

EASE OF IMPLEMENTATION (OVERALL)

The following areas of complexity are seen at present:

- 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 DSSR to function.
- Design of DSSR 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 DSSR information.
- Adoption of DSSR in order that information is contributed and available in sufficient volumes that can be consumed by others for benefit.
- Financial model of DSSR to cover design, build and on-going operational costs.
- Regulatory support for a registry and usage of a trust based model.

SECURITY

From a consumption angle the solution is secure since the information consumed can be done on a 'trust' basis; how much does the FI trust the information based on the risk, who submitted it and who

else trusts it. Whilst this does not prevent invalid / incorrect information being contributed, it does provide the mechanism to identify such cases and thus 'not trust' such sources in the future.

From a technical perspective there are two main deployment models; centralised and distributed. The centralised model is well known and design patterns exist regarding trusted access and security. The distributed model is worth further investigation to determine value of Distributed Ledger technologies / design patterns (these may also provide some help with some data protection concerns).

IMPACT: SUCCESS METRICS

How would we know this solution has worked? What measures and targets do we define for judging this?

- For both FIs and customers; cost of compliance and reduction in fraud losses.

COLLABORATIVE OR COMPETITIVE

A collaborative / cooperative model. KYC registry initiatives have been introduced within the last few years but with a somewhat smaller scope – for example SWIFT KYC Registry for AML risks in Correspondent Banking.

6. Enhancement of Sanctions Data Quality

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

The quality of the entries on Sanctions Lists directly correlates with the number of alerts raised by Sanctions screening systems. 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.

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.

SOLUTION DESCRIPTION

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 in this context is for HMT to adopt the Advanced Sanctions Data Model.

BENEFITS

Adopting this data model for HMT Sanctions 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.

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.

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)

7. Customer Education and Awareness

SOLUTION NAME: CUSTOMER EDUCATION AND AWARENESS FOR FINANCIAL CRIME

PROBLEM STATEMENT:

A priority issue in Financial Crime is the ability of end-users to identify and understand the methods by which criminals seek to exploit end-users in order to obtain or launder money, and the steps end-users should take to reduce the risk of becoming a victim or unwitting participant in financial crime.

Obtaining personal data about customers is the most valuable asset in financial crime market as it enables access to customers' financial relationships:

- directly through social engineering over the telephone to provide further data or undertake payments
- placing malware on customers PC to acquire information
- sending emails to end-users asking for information, e.g. to vulnerable customers, or small-company CEOs ;
- hacking into organisations' databases to obtain bulk card, account and personal information data.

All attacks play on human vulnerability/weakness. Whilst awareness and education will not totally resolve this issue, when placed alongside other measures they will have a substantial impact on the ability to mitigate the risks.

SOLUTION DESCRIPTION

It is clear that the Forum's approach to Education and Awareness will be informed by the End-Users Needs working group alongside our perspective on financial crime.

An education and awareness programme on financial crime risks for end-users should include:

- How to protect themselves from becoming a victim of financial crime;
- The risks from becoming involved in financial crime and fraud, for example by becoming involved in mule-account activities;
- How the payments system can protect customers from financial crime.

The Education and Awareness campaign will need to target customers in many different groups/ segments: consumers, businesses, charities, public sector organisations. In consumers, key groups (among many) are vulnerable customers, students at school & college, young people using payment services for the first time. For example, the Group sees a strong need for information security and fraud awareness to be in school curriculums, to equip young people for whom digital channels and services will be the mainstream method of engagement with PSPs.

The programme should be broken down into two elements:

Immediate

Provide a programme of regular consistent joined up messages to educate consumers and businesses about the risks of financial crime and how to protect themselves against them.

The solution should enhance, strengthen and expand the breadth of topics covered within the existing Financial Crime arena E+A programmes.

This should be co-ordinated through the Multi-Agency Campaigns Group which is currently facilitated by The City of London Police and consists of public and private sector organisations (list set out below) that regularly deliver fraud and scams awareness messages to consumers and businesses. Engagement with CoLP is required to make them aware of the Payment Services Forum and this programme of activity.

The group:

- Provides visibility to participants and their members of planned awareness activities by means of a regularly updated cross-sector awareness calendar;
- Seeks and drives opportunities for collaborative campaigns and messaging and to support one another's campaign activity;
- Looks to ensure consistency in messaging and aligned activities.

Attendees include: Home Office, CoLP, Met Police, Cifas, FFA UK, BT, FCA, NCA, NFIB, Crimestoppers, Trading Standards, Citizens Advice, Age UK and Get Safe Online.

In addition to this the group have access and the opportunity to influence two of the larger scale awareness initiatives currently being driven by the Government and banking industry

Be Cyber Streetwise is a cross-government campaign, funded by the National Cyber Security Programme, and delivered in partnership with the private and voluntary sectors. The campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills and the Cabinet Office. It aims to measurably improve the online safety behaviour and confidence of consumers and businesses.

Take Five to Stop Fraud, an awareness initiative and umbrella brand, led by FFA UK working with its partners, including Government and law enforcement, will launch in 2016. This step change national awareness initiative on fraud and scams will call on Britain to Take Five – to simply have the confidence to stop and think when faced with a potential fraud, whether it be a an unsolicited approach by telephone or by e-mail. If everyone remembers they have the right to Take Five, we'll stop fraud in its tracks.

Longer term

Develop a programme of awareness about the protection provided by using the payments system infrastructure.

This should take place once enhancements have been delivered across the PSF programme of activity.

PEOPLE INVOLVEMENT AND ACTION

- The Multi-Agency Working Group will have oversight, manage and maintain an up to date centralised repository of all planned awareness activities.
- The planned activity forms a communications diary of key messages throughout the year on key vulnerabilities being targeted by financial criminals.
- The group will look to ensure alignment, co-ordination and delivery of those awareness activities identified as requiring a collaborative focus.
- Contributors to the communications diary have a seat at the forum and agree voluntarily to input to it to provide visibility of their awareness plans.
- For collaborative activities a set of measures must be place with agreed baselines against which to determine the success.

The approach to Customer Education & Awareness is directly relevant to the End-User Needs Working group as well as Financial Crime working group.

Within the Financial Crime working group we are working to develop a set of priority topics/ messages for public awareness campaigns. When we have produced this list, we will engage closely with the End User Needs WG in order to develop a joined-up set of priority campaign topics for the Forum to endorse and pursue.

LEADERSHIP

From the perspective of Financial Crime WG, the Forum will need to work with the following organisations to deliver coherent national campaigns.

- Cyber Streetwise will continue to be led by the Home Office.
- Take Five will be led by FFA UK with engagement with its Members and other partners through appropriate working groups.
- Each organisation on the Multi-Agency Campaigns Group will provide visibility of plans and dates for their awareness activities with others on the group by means of a calendar maintained and shared regularly by CoLP.

The PS Forum should look to support existing initiatives such as Cyber Streetwise and Take Five and identify any other key areas of fraud that require collaborative awareness activity.

COMMUNICATION

PSF should point any participants to the Multi Agency Campaigns group and encourage them to provide details of current and future planned E&A activity.

COST BENEFIT ANALYSIS (HIGH-LEVEL)

- Benefits to customer (consumer, business, government dept, charity etc)
- Reduction in the numbers of victims especially vulnerable customers

- Benefits to industry
- Reduced operating costs from having less victims
- Increased consumer confidence in payments systems
- Enhanced reputation from being seen to be doing something to educate customers
- Costs to deliver/ to operate
- Costs can vary dependent upon the level of campaign and awareness required. If further funding can be achieved, improved campaign tactics can be applied

SECURITY

Education and awareness are only one part of an anti-crime strategy, running alongside other industry initiatives to protect and prevent fraud.

Education and Awareness require ongoing consistent messages supplemented by the latest Modus Operandi being used by the criminals.

IMPACT: SUCCESS METRICS

- This is difficult to measure in terms of outcomes as the may be a number of factors which can impact the reduction in fraud losses and therefore it is not easy to directly attribute any reduction to E&A.
- Not all outcomes are readily measurable in terms of absolute numbers, e.g. the number of mules, the number of victims of scams. In addition there will be other mitigation being put in place
- The only measure will be to measure input by undertaking sampling surveys of whether people have seen the E&A and their understanding of the campaign message.
- Education and awareness is not applicable for deterring terrorist financing or bribery and corruption as this is done either with intent or coercion.

COLLABORATIVE OR COMPETITIVE

- Collaborative working is the best outcome ensuring the messages are aligned and using the same logo/ branding. This will therefore enable consistent and regular messaging without the burden of costs falling to one organisation
- There have been a number of campaigns by different organisations covering a wide range of topics however these have not been organised under one banner and the effectiveness potentially sub -optimised

8. Looking forward: Recommended next steps

This section sets out the next steps for the Financial Crime Working Group for the period between the Forum meetings on 14 April and 30 June.

FOR WORKING GROUP'S PRIORITY SOLUTION AREAS

For the six solution options covered in this report, developed in detail in the period since February's Forum, the Working Group recommends a further phase of detailed analysis to move from a potential approach towards practical recommendations:

- Identity Verification, Authentication, and Risk Assessment
- Payments Transaction Data Sharing And Data Analytics
- Enhanced Payment Transaction Data
- Financial Crime Intelligence Sharing
- Trusted KYC Data Sharing and Storage Repository
- Enhancement of Sanctions Data Quality

This phase of analysis should address:

a. Solution definition
    - Iterate and make more robust.
    - Check on proposition - is this solution a valid model, what returns or benefit will it bring.
    - Engage wider stakeholder group/ working group (including legal working group).
    - Further prioritisation.
    - Check inclusivity across all PSP players
    - Address other elements such as solution security and resilience, governance details, assumptions and dependencies analysis, collaborative vs. competitive analysis and landscape review, plus performance metrics/ KPIs
b. Phasing
    - Timeline, dependencies, roadmap, quick wins, fit in with horizon scanning, other industry initiatives.
c. Net Benefits
    - More measurement of detriments resolved?
    - Econometrics for end user pricing.
d. Costs
    - Transfer drivers into order of magnitude.
    - More quantitative analysis.
e. Requirements for engagement with other authorities and industry bodies (external environment)
    - financial services sector authorities and industry bodies involved directly in reducing financial crime and fraud

f. Further impact assessment analysis & surveys around the Forum's questions on innovation

FOR CUSTOMER EDUCATION AND AWARENESS

The Forum's approach to Education and Awareness will be informed by the End-Users Needs working group alongside the perspective from the Financial Crime Working Group.

Within the Financial Crime working group we are working to develop a set of priority topics/ messages for public awareness campaigns. When we have produced this list, we will engage closely with the End User Needs WG in order to develop a joined-up set of priority campaign topics for the Forum to endorse and pursue, building extensive engagement with organisations setting campaign objectives and priorities across the financial services sector.

ALIGN APPROACH ACROSS THE FORUM'S WORKING GROUPS

In the next phase of the Forum's work, we propose that the working groups should identify common issues and work closely, across the Working Groups, on developing the next level of analysis and proposal. Issues that require a common approach include:

- Identity and authentication of payer / payee in payment systems, both for UK and international payments: we understand is a common interest with End User Needs, and will link to Horizon Scanning;
- Customer Education and Awareness: common topic with End-User Needs
- Enhanced Payments Transaction Data is a common interest with End-User Needs (e.g. for corporates and government departments) and leads directly into discussions on payment systems standards, which is a link to Horizon Scanning.

OTHER FINANCIAL CRIME WG WORK-STREAMS

Plan activities and deliver next-phase outputs for four other work-streams in the Working Group:

- Consistent Control & Reporting obligations across all payment/ money-transfer providers;
- Profiled control of payment initiation for all customers;
- Legal work-stream: to pull together an understanding on the existing legal issues or constraints which would need to be addressed in order to enable aspects of these solutions to be viable;
- External Environment work-stream: to identify all the public authorities, industry bodies and industry initiatives, across the financial services arena, that are addressing issues of financial crime (fraud, money laundering, terrorist financing, bribery and corruption).

ENGAGING WITH OTHER FINANCIAL SERVICES AUTHORITIES AND BODIES

A number of issues addressed by the Financial Crime Working Group are also of direct interest to authorities, regulators, and industry bodies across the financial services sector. As the Forum moves to confirm a set of priority requirements/ initiatives from the perspective of the payments industry, there

will be a need to engage with other industry authorities and bodies to join up the approach and, for example, assess the best delivery approach and funding model.

9. Appendix

MEMBERS OF THE FINANCIAL CRIME, DATA AND SECURITY WORKING GROUP

(as of 03 April 2016)

The working group comprises a number of members with a diverse set of interests and specialisms relevant to working in finance. These include payment service providers, infrastructure providers, software providers, management consultants, credit reference agencies, and industry bodies/ associations. See below for a full list of who has been involved.

This diversity gave the group a multitude of perspectives and expert points of view, and enabled it to reflect 'in the round' on the issues and solutions it explored. This also worked well when assessing whether or not the solutions it was developing solved specific problems and represented a value proposition.

Attendee	Business
Russell Saunders (Chair)	Payments Strategy Forum
Neil Lover (Deputy Chair)	Coventry Building Society
Lana Abdullayeva	Experian
Charles Bennett	VocaLink
Nick Davies	Department for Work and Pensions, HMRC
Graeme Donald	Lloyds Banking Group
Robert Dooley	Virgin Money
Andrew Fone	Financial Fraud Action UK
Luisa Grey	Eazipay
Laura Hanna	HiFX
Ian Horobin	Swift
Lisa Hullah	Clydesdale & Yorkshire Bank
Ali Imanat	FFA-UK
Gail Jones	FFA-UK
Andrew Kaye	Transpact
Cate Kemp	Lloyds Banking Group
Harshan Kollara	FastENcash
Andrew Laidlaw	Financial Conduct Authority
Louise Lamb	Hogan Lovells
Charles McCready	TISA
Ruth Mitchell	Electronic Money Association (EMA)

Isabelle Moeller	Biometrics Institute
Mick Paisley	VocaLink
Olivia Randell	Barclays
Richard Ransom	Bottomline Technologies
Catherine Robert	Hogan Lovells
Martin Salter	Nationwide
Georgios Samakovitis	University of Greenwich
Peter Seymour	Laurasia
Mark Stanhope	Faster Payments
Paul Thomalla	ACI Worldwide
Hamish Thomas	EY
Hazel Timbrell	Barclays
Philip Treleaven	UCL
Bill Trueman	Association of Independent Risk and Fraud Advisors
Peter Tully	Clydesdale Bank
Karen Tyler	Santander
Caitriona Whelan	Royal Bank of Scotland
Jonathan Williams	Experian
Tim Yudin	Payments UK
Andrew Ducker	Payments Strategy Forum
Stephanie Mcloughlin	Secretary
David McPhee (Observer)	Payment Systems Regulator
Andy Watson (Observer)	Financial Conduct Authority
Kevin Bridgewater (Observer)	Payment Systems Regulator

ATTENDEES – FINANCIAL CRIME CUSTOMER IDENTIFICATION AND RISK SCORING WORKSHOP

(4 Mar 2016)

Attendee	Organisation
Jon Williams	Experian
Isabelle Moeller	Biometrics Institute
Paul Thomalla	ACI Worldwide
Gail Jones (AM only)	FFA UK
Mark Stanhope	Faster Payments/Paym
Kyra Oattes	Coventry Building Society
Olivia Randell	Barclays
Bill Trueman	Association of Independent Risk & Fraud Advisors
David Paris	Cognizant
Judith Crawford	Electronic Money Association
Mark King	Broadsail
Andrew Ducker	Lloyds
Ali Imanat	FFA-UK
Jon Frazer	Cognizant
Sulabh Agarwal	Accenture
Mayank Bhundia	Accenture

ATTENDEES – FINANCIAL CRIME TRANSACTION DATA SHARING AND ANALYTICS WORKSHOP

(11 Mar 2016)

Attendee	Organisation
Giorgios Samakovitis	Univ of Greenwich
Rob Dooley	Virgin Money
Nick Davies	DWP
David Paris	Cognizant
Olivia Randell	Barclays
Kevin Bridgewater	PSR
Li Yeoh	LBG
Lana Adbullayeva	Experian

Natalie Nunney	RBS
John Fraser	Cognizant
Harshan Kollara	Fast EnCash
Hamish Thomas	EY
Andrew Ducker	Lloyds
Charles Bennett	Vocalink
Gail Jones	FFA UK
Andrew Kaye	Transpact
Alex Bray	Coventry BS
Mark Stanhope	Faster Payments
Sulabh Agarwal	Accenture
Mayank Bhundia	Accenture

ATTENDEES – FINANCIAL CRIME TRUSTED INTERNATIONAL ECO-SYSTEM REGISTRY WORKSHOP

(16 Mar 2016)

Attendee	Organisation
Andrew Ducker	LBG
David Paris	Cognizant
Giorgios Samakovitis	University of Greenwich
Harshan Kollara	Fash EnCash
Ian Horobin	Swift
John Fraser	Cognizant
Lana Abdullayeva	Experian
Louise Piosek	Santander
Paul Eagles	Visa
Paul Thomalla	ACI Worldwide
Sulabh Agarwal	Accenture