payments strategy forum

November 2017

Trusted KYC Data Sharing – Standards Scope and Governance Oversight

Handover Document

Contents

Preface

This document has been produced by the Financial Crime, Security and Data Working Group (FCWG) as part of the consultation paper 'Blueprint for the Future of UK Payments' developed and published by the Forum in July 2017. It describes the preliminary scope of the data sharing standards scope and the required governance oversight.

This document is expected to be of particular interest to those with a role in the prevention of financial crime, including Payment Service Providers (PSPs), trade bodies, solution vendors, regulators, law enforcement agencies and the government.

The establishment of a data sharing framework is recommended (see Figure 1) to provide a method of sharing a core set of SME[1] customer data between organisations acting as data providers where the customer already has an account (e.g. a bank or insurance company) and other organisations who use that data with the customer's consent (data consumers).

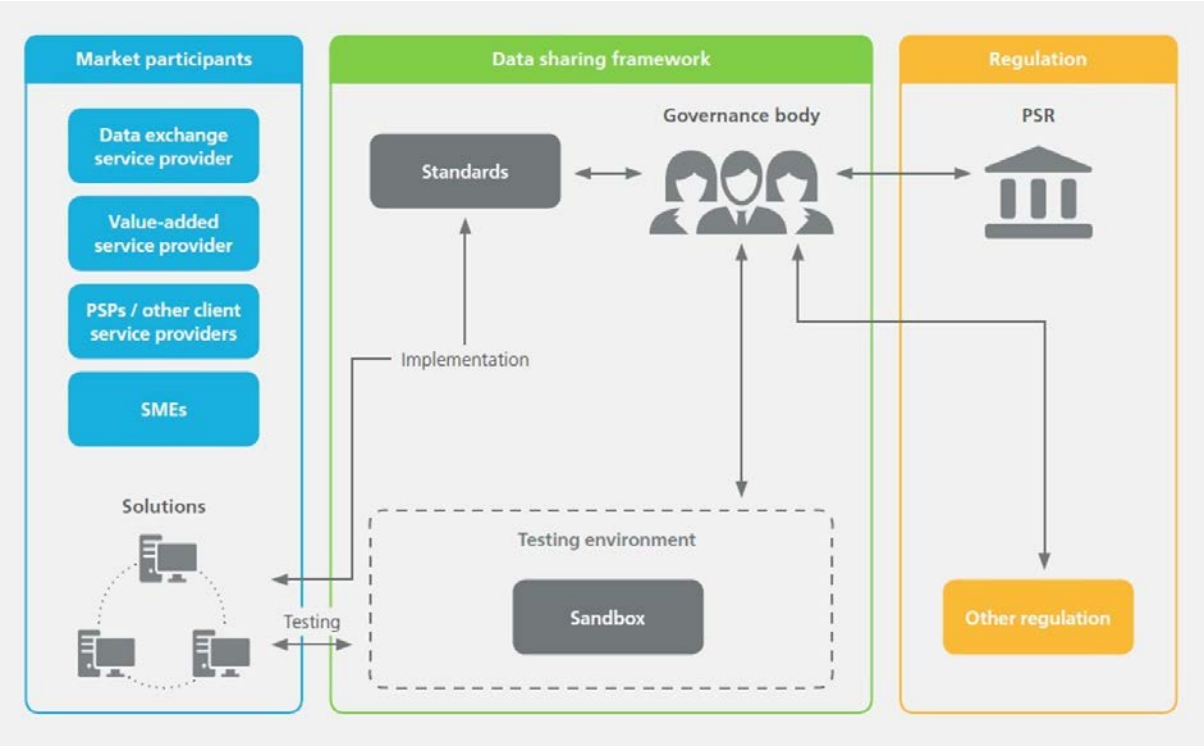

Figure 1 Schematic picture of data sharing framework

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

Data sharing is intended to be on a point-to-point basis between PSPs, or via data exchange service providers which offer a single point of connectivity between data providers and consumers. Data will only be shared with the customers' consent. For example, an insurance company (data consumer) can only receive customer data from a bank (data provider) about a customer (data owner), with that customer's consent. In this example, the insurer could also purchase services from a data analytics company (KYC service provider) to

[1] Small and Medium sized Enterprises (SMEs)

further enhance and validate the data being shared.

The whole network and the wider public will benefit from improved (i.e. corrected, verified and timely) customer information through updates during each interaction. Results will include improved customer experience, reduced KYC operational costs and increased ability to identify 'bad actors'[2] and reduce financial crime.

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

Consultation input

As part of the Forum's Blueprint for the Future of UK Payments consultation in July 2017 (July 2017 Consultation), respondents commented on the potential benefits of the solution if applied to other market segments beyond the sharing of a core set of SME data.

The Forum feels that a starting point is required to help develop an effective addressable market to promote long term competition for services and offerings in a wide variety of market segments. Given the focus on SME's in the CMA report 'Retail Banking Market Investigation' and a lack of existing commercial offerings for SME customers, the Forum feels that an initial focus on the SME market segment will provide the most significant benefit to a currently unserved population.

As the solution progresses over time, with increasing levels of adoption and innovation, it is envisaged that use cases and service offerings will emerge that look to extend the range and focus, and if required further standards developed, to provide benefit to a variety of markets, including but not limited to KYC.

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

Overview

1 Objective of this Document

The 'Trusted KYC Data Sharing' solution introduced in Section 6.3 of the consultation document is further detailed in two documents (see Figure 2).

This document defines the suggested scope of the data sharing standards to be developed and enforced by the governance body. These standards will be reviewed and validated with representatives from the financial services industry, SMEs and service providers, before being verified in a testing environment.

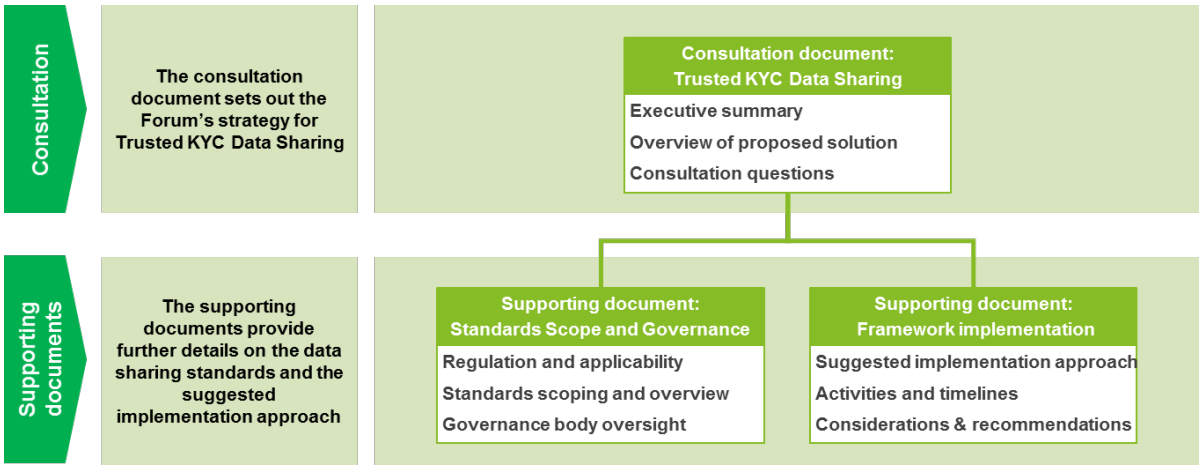

Figure 2 Schematic picture of document structure

2 Key Regulations, Legislation and Guidance

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

The introduction of the General Data Protection Regulation (GDPR) in May 2018, together with industry-specific regulation including Payment Services Directive 2 (PSD2) in Europe and the Competition and Markets Authority (CMA) remedies in the UK, mean that a tipping point has been reached which is compelling the industry to identify new ways to interact with their customers.

In particular, the CMA 'Retail Banking Market Investigation' report of November 2016 recommended a 2018 review by the Treasury with regards to secure data sharing for SMEs between PSPs and third parties, which allows them to manage their accounts with multiple providers.[3] These changes will potentially have a significant impact on the KYC processes of PSPs operating in the UK.

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

As a minimum, the following regulations, topics and guidance are recommended to be taken into account when defining the data sharing standards (see Figure 3).

Regulations, topics and guidance with impact on KYC data sharing standards

- 4th Money Laundering Directive (MLD4)
- Payment Services Directive 2 (PSD2)
- EBA PSD2 SCA Regulatory Technical Standards (EBA RTS)
- Joint Money Laundering Steering Group Guidance (JMLSG)
- UK HM Government guidance (GOV.UK)
- FCA Financial Crime Guide (FCAFCG)
- European Electronic Trust Services Regulation (eIDAS)
- EU Funds Transfer Regulations (WTR2)
- UK Data Protection Act (DPA)
- EU General Data Protection Regulations (GDPR)
- UK Money Laundering Regulations 2017 (MLR)
- UK Payments Accounts Regulations 2015 (PAR)
- EU Payments Accounts Directive 2014 (PAD)
- UK Current Account Switching Service (CASS)
- CMA 'Retail banking market investigation' report

Figure 3 Regulations and guidance with impact on KYC data sharing standards

3 Applicability of Standards

This section will define the applicability of the standards by topic (see Table 1) and participant type including: PSPs and other client service providers, SMEs, data exchange service providers and value-added service providers. Two scenarios for sharing data between PSPs are supported:

1. Peer-to-peer data exchange
2. Data sharing through data exchange service providers

The KYC data sharing solution will not standardise PSPs approaches to validate customer data. The set of standards created will focus on defining the characteristics of the data sharing i.e. data fields that will be shared; some components of 'The standard information set' developed by CMA for Business Current Account opening might be taken as a baseline.

The data sharing framework must enable the co-existence of a range of potential business propositions that could leverage the data exchange capability provided to offer additional services to PSPs, and thus drive adoption of the service (see Appendix 1).

The initial implementation of the standards is recommended to cover only the sharing of a core set of SME customer data between PSPs and with data exchange service providers depending on the chosen data sharing scenario. Every PSP will still be required to perform their own due diligence processes; liability will not be placed on the originating PSP sharing the data. However, customer authentication or data quality services, could be offered by the entities providing the customer data as additional value-added services.

The scope of the standards will evolve incrementally as the solution offerings expand and new regulatory requirements emerge (e.g. extensions to the data model and additional security requirements). The baseline standards should cover the following topics (see Table 1).

Topic	Content
Sharing capabilities and interoperability (Section 1)	Defining the sharing mechanisms between the data provider and the data consumer, e.g. consent process and cooperation recommendations to ensure that both provider and consumer contribute data.
Data model (Section 2)	Defining the data model building upon some components of 'The standard information set' developed by CMA, including completeness requirements and data access rights. A minimum set of fields will be defined that ensures flexibility for different KYC processes and regulatory requirements.
Security and privacy (Section 3)	Providing technical details for encryption by cross referencing to Open Banking, PSD2, GDPR and ISO. Also defining reporting requirements for participants if they experience security and data breaches.
Governance body oversight (Section 4)	Activities include evolving and enforcing the defined data exchange standards as well as identifying which service providers are not compliant with these standards and taking appropriate actions.

Table 1 Data sharing standards topics

Each section will cover three categories:

- Behavioural principles to be followed by participants for the appropriate operation within the data sharing environment.
- Requirements to be met by the service providers and PSPs to enable the secure sharing of data between the participants.
- Degree of oversight required to track adoption rates and ensure compliance with the data exchange standards.

These topics may have been addressed already for the purposes of Open Banking and PSD2. The governance body will draw on the progress made in each of these areas. Other standards related to sharing data are available (such as OAuth 2.0 and the Open ID Connect protocols), but are not specifically designed for use in association with KYC services. The proposed KYC Data Sharing standards are complementary to these and it is anticipated that all standards will develop over time to meet the needs of the evolving market place.

1 Sharing Capabilities and Interoperability

The drafted standards are intended to cover the sharing capabilities of multiple data exchange solutions, co-existing in the data sharing environment (including the characteristics and features of the environment), to enable the exchange of data between all participants.

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

This environment will only be successful if network participants are willing to share their core set of SME customer data with other PSPs and client service providers. While data consumers will directly profit from receiving the data, there is currently limited regulation requiring data providers (in most cases larger PSPs) to share their valuable customer data. More details are provided in Appendix 2.

1.1 Data Sharing Behaviour Principles

PSPs have heterogeneous customer due diligence processes and data requirements; the data sharing environment must offer flexibility for PSPs to perform their KYC processes. Data exchange service providers should establish access models to allow connectivity with PSPs and other data exchange service providers (operating for other PSPs). Every PSP will be able to request and receive information from other peers through the network established between the different data sharing solutions.

The scope of the data model defined by the governance body will not be restrictive. PSPs which have not aligned their data fields to the model will not be precluded from using the environment. Participants should be able to share additional customer information exceeding the defining minimum set if relevant for the execution of the KYC processes.

Collaboration from all participants will be required for the successful operation of this KYC data sharing initiative. PSPs will be required to respond to all data requests that they receive from other PSPs; this is subject to legal constraints and the customer's consent to share the customer attributes. PSPs will be required to draw their own conclusions on the customer assessment based on their own risk appetite. No liability will be placed on the originating PSP.

Consultation input

As part of the Forum's July 2017 Consultation, respondents commented on the need to develop a clear liability model associated with use of the solution.

The Forum agrees that the solution delivery body will need to work with stakeholders to develop and clearly define the liability model associated with the data sharing framework.

Regulations are envisaged to remain such that they require institutions to validate the data they hold and receive on a customer before providing services; therefore, the liability for this solution will be limited to ensuring that data is not corrupted or altered during data exchange without the customer's permission. The framework will not therefore include the liability associated with decision making made by organisations based on data that they have not validated themselves beforehand (e.g. based on information supplied to them direct from their customer). Participants will retain their requirement to ensure the accuracy of the data they received, and may look in future for data verification service providers to supply this service. However, the liability associated with decision making based on data verified by other parties does not fall within the scope and remit of this solution.

The solution delivery body will need to work to develop this model, and ensure all participants have a clear understanding of its implications.

1.2 Data Sharing Mechanism Features

The data model used to exchange information must be concise and easily understood by PSPs and third party service providers (TPSPs).

All PSPs will be provided with access to the whole end-to-end environment by their respective data exchange service providers, regardless of size or magnitude. Thus PSPs with limited budget (and who may be using small third party providers) will be able to share customer information. This end-to-end data sharing process will be achieved through interoperability agreements established between service providers co-existing in the data sharing environment.

PSPs and TPSPs will be able to register their participation in the data sharing environment. This registration will contain information about the services supported by the PSPs and service providers and the relationship of the providers and users.

1.3 Degree of Oversight Required

The governance body must ensure that the standards evolve on an ongoing basis to cover the needs of the whole range of participants (SMEs, PSPs and TPSPs). In addition, the governance body will supervise the vendor's certification process in order to ensure compliance with the data sharing standards. Participant certifications may be revoked if participants are no longer meeting the required standards.

A consultation process will be carried out by the governance body to monitor the issues experienced by the involved PSPs and TPSPs in the reception/transfer of the data (including interoperability issues in the data exchange). A central registry will be used to monitor the number of participants and the services they provide.

2 Data Model

It is recommended that the governance body will define a data model including a minimum set of data fields and the data exchange format (e.g. XML).

2.1 Data Sharing Behaviour Principles

Certified PSPs and data exchange service providers will ensure that the data fields exchanged are aligned with the agreed data model; covering completeness (e.g. provision of the right amount of information) and formatting (e.g. provision of the date of birth data field in the right format: dd/mm/yyyy). To protect their customers PSPs and data exchange service providers will have to establish/maintain controls on the personal customer information that they are holding and/or exchanging.

The data sharing standards will be expanded over time. Future versions may require the participants to provide timestamps at a field level to facilitate ongoing due diligence by reducing the number of additional data checks. On the other hand, SMEs will be required to keep their personal information updated (through the channel provided by the PSP that is holding its customer account) to avoid duplication of effort when collecting customer information.

2.2 Data Sharing Mechanism Features

The data exchange environment must be able to provide access to a wide range of participant SMEs who provide consent to share their personal data. Full access to the data sharing environment will be granted to the participants through the interoperability agreements established between the different TPSPs co-existing in the environment.

2.3 Degree of Oversight Required

To raise awareness of the importance of keeping personal data up to date it is recommended that a series of educational sessions and communication material be provided by the governance body to the SME community, through trade associations and PSPs. The governance body will need to consider how these sessions will be run in order to achieve maximum benefit for SMEs.

3 Security and Privacy

The standards must define security and privacy rules for personal customer information shared within the data sharing environment to protect SMEs from fraudulent actors.

3.1 Data Sharing Behaviour Principles

With the objective of keeping a safe environment, participants will be required to report any kind of confirmed or suspected data or security breach. SMEs will be notified in the event that their personal data may have been compromised. PSPs and TPSPs will be required to encrypt information shared with other participants. This will be key to ensure the security and privacy of data transmissions within the environment.

Explicit customer consent is required before their data can be shared. Customers must remain fully aware about when their data is shared, to whom and for what purpose. These principles will increase the trust in the data sharing environment and drive the adoption of the solution among the SMEs.

3.2 Data Sharing Mechanism Features

To protect customer personal data from access by ‘bad actors’, participants within the environment will be certified to guarantee that their data exchange service offerings are compliant with the defined security and privacy standards. The standards will be aligned with and cross-referenced to other regulations/initiatives like GDPR, Open Banking and PSD2.

All data exchange solutions within the environment must provide SMEs with control over their data. SMEs will decide on which data they want to share and with whom. PSPs must be able to provide a regular data sharing report about their data usage on a field level.

Consultation input

As part of the Forum's July 2017 Consultation, feedback confirmed that emphasis should be given in the development of the framework on ensuring: the SME customer is at the heart of the standards; consent is obtained to sharing of their data between institutions; and they understand their rights and responsibilities in relation to how data is managed.

As such, during the definition of the standards, the solution delivery body should work with stakeholders to give detailed consideration to the process by which customers give their consent for their data to be shared and processed; that customers understand their rights and obligations with regards to their data; and the governance body oversees the way in which all data is only used for the purpose consented by customers.

The solution delivery body will be required to perform a GDPR assessment of the solution and the standards to maintain alignment through its development.

3.3 Degree of Oversight Required

Prior to participating, PSPs and service providers must be certified by the governance body to ensure compliance with privacy and security requirements. On a yearly basis, the governance body will:

- Decide on required updates to the security and data standards to comply with regulatory change, mitigate emerging financial crime trends and to incorporate feedback gained from participants through usage of data and security protocols.
- Assess data exchange service offerings provided by the service providers to grant, review, revoke, or reinstate certifications to the participants within the environment.

4 Governance Body Oversight

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

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

4.1 Evolution of the Environment

The amendment of existing standards and/or the inclusion of new standards by the governance body will ensure the environment evolves on an ongoing basis to cover the needs of the whole range of participants (SMEs, PSPs and TPSPs). The continued evolution of the standards will be key to ensure coverage of participant future regulatory requirements and adoption of the solution by PSPs and SMEs. It will also maintain an open data exchange environment with no barriers against small participants (both PSPs and TPSPs) joining.

A large number of TPSPs must be able to co-exist together in the open data exchange environment. It is key that this environment does not impose any restriction that may limit the competition in the market.

The governance body, will go through a consultation process on a yearly basis, engaging with participants to ensure that the data exchange standards are appropriate, accepted and understood.

4.2 Compliance and Correct Interpretation

The different participants in the data exchange environment may interpret the drafted standards in different ways. Therefore the data sharing standards must be written clearly and with a high level of detail. Additionally, the governance body must oversee that the standards are understood and respected by all the PSPs and service providers.

For the correct interpretation and accurate understanding of the standards, educational sessions will be provided to the different range of stakeholders. The governance body will define the strategy and methodology for the provision of these sessions. Sessions will be held before the solution goes live and when a significant change is made to any of the existing standards.

Continuous feedback will enable the governance body to answer questions raised by the participants and make further enhancements.

Consultation input

As part of the Forum's July 2017 Consultation, we asked for feedback on the expected roles and responsibilities of the Governance Body when overseeing the data sharing standards and testing environment. Following the consultation responses, the following roles and responsibilities have been added on the theme of ensuring compliance and correct interpretation. The governance body will be required to:

- Define, manage and periodically update (as appropriate) a liability management model covering:
  - non-compliance with the standards
  - losses incurred from errors in spite of compliance with the standards
  - the consequences for non-compliance with the standards
- Take appropriate steps that participants only use the data for the purpose(s) that the SME customer gave consent.
- Maintain alignment of the standards to regulatory and legal requirements.
- Provide guidance to solution participants on the topics of regulatory compliance, effectively capturing KYC data, and mitigations against the risk that data is shared that is found to be incorrect at a later date

4.3 Management Information

A number of metrics must be monitored by the governance body on a periodic basis through service providers to track:

- Level of adoption of the KYC data sharing initiative.
- Any key issues reported by the different participants.

These metrics will be key to ensuring that the environment is meeting participant expectations and is achieving the right level of adoption across the industry.

Consultation input

As part of the Forum's July 2017 Consultation, we asked for feedback on the expected roles and responsibilities of the Governance Body when overseeing the data sharing standards and testing environment. Following the consultation responses, the following roles and responsibilities have been added on the theme of information management. The governance body will be required to:

- Publish and maintain a list of participants that have been 'accredited', including an annual renewal of this publication to ensure clarity as to which participants are adhering to the standards
- Oversee customer education initiatives, including the commissioning of customer education materials if necessary, and overseeing industry customer communications
- Maintain awareness of complaints that arise from the application of the standards by participants, such that appropriate action can be taken as necessary

Appendix

Appendix 1: Value-Added Service Providers

The focus of the data sharing framework is to provide a data sharing environment as described in the section above. A range of potential business propositions have been identified that could leverage the exchanging capability provided by the environment to offer additional services to PSPs, and so drive adoption of the service (see Figure 4). These have been grouped into three broad categories:

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

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

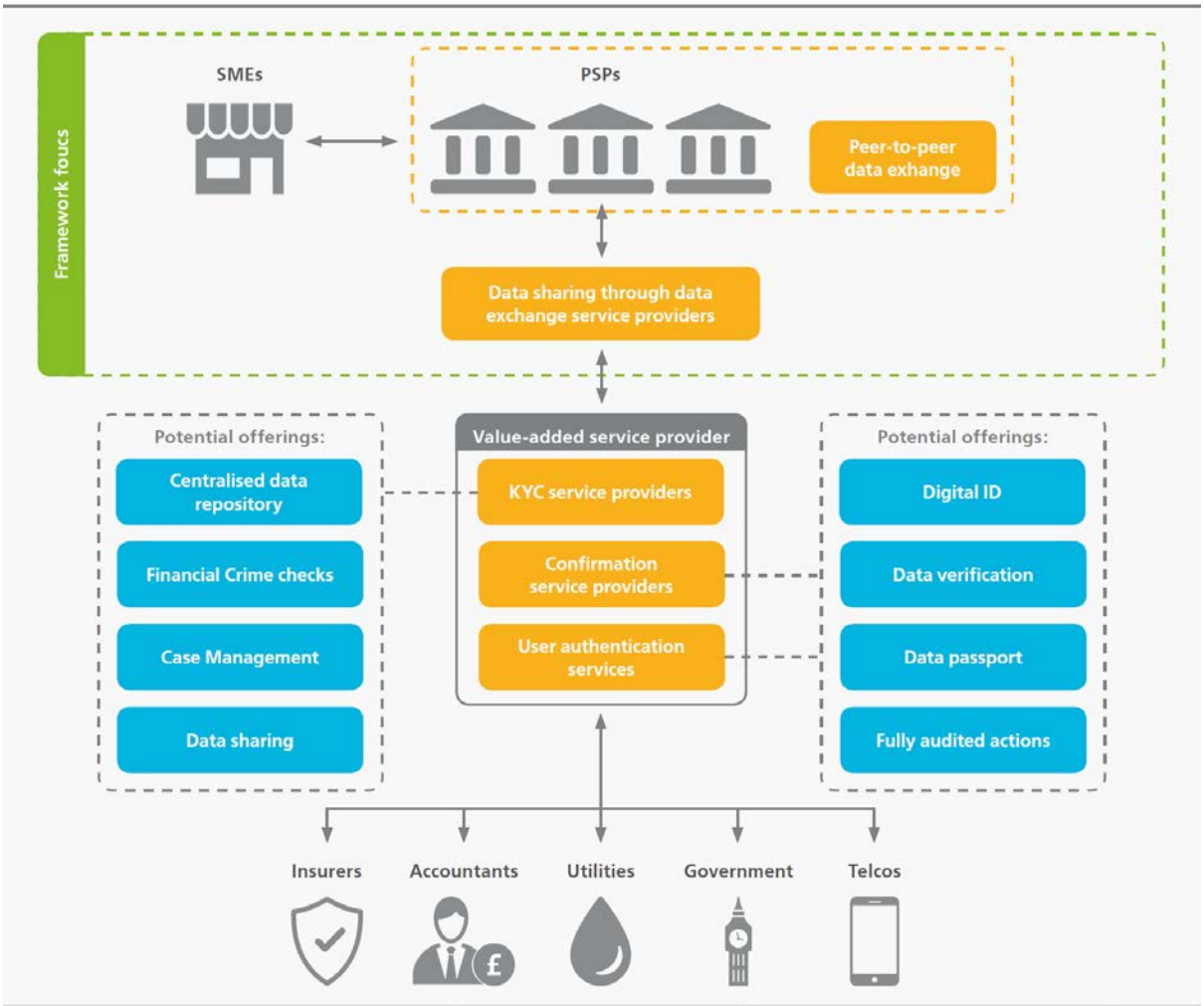

Figure 4 Overview of business models enabled by the data sharing framework

KYC Service Providers

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

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

Confirmation Service Providers / Digital ID

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

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

User Authentication Services / Data Passports

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

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

Appendix 2: Data Consumers and Data Providers

The sections below illustrate the requirements and advantages for both net consumers and net providers.

Benefits for Net Data Providers

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

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

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

Benefits for Net Data Consumers

Net data consumers will receive direct benefits from the exchange of the data through the environment. The received core set of SME customer data from other entities reduces the operational work required to obtain the

data and supporting evidence and will lead to lower cost and a faster on-boarding process. This enables them to provide a better customer experience and potentially increased revenues due to increased customer interest.

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