The Open Banking Standard

Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation

CONTENTS

1. Executive Summary

Context

In the 2015 Budget HM Treasury announced its commitment to delivering an open standard for Application Programming Interfaces in UK banking, to help customers have more control over their data and to make it easier for financial technology companies (FinTechs) or other businesses to make use of bank data on behalf of customers in a variety of helpful and innovative ways. The Government explained that this could help to drive more competition in banking to improve outcomes for customers, and further support the UK's world-leading FinTech industry.

In summer of last year, at the request of the Economic Secretary to the Treasury, Harriett Baldwin MP, the Open Banking Working Group (OBWG) was established to take forward this work. Their objective was to produce a detailed framework for how an Open Banking Standard could be designed and delivered, with a timetable for achieving this. The OBWG comprised industry experts from banking, open data, and consumer and business communities to ensure a diverse range of expert views are represented. This report is the OBWG's detailed framework for delivering an Open Banking Standard in the UK.

Leadership in this area will set precedents across many sectors; a strong data infrastructure will be as important to the UK's economy today, as roads have been to our success in the industrial economy for over a century. Banking as a service has long sat at the heart of the economy because of the need to seamlessly and efficiently connect different economic agents who are buying and selling goods and services. The need for that ease of connectivity only increases in a digitally enabled economy, and the capabilities that underpin it necessitate that connections be made in very different ways.

Trust will remain the single most important factor in determining how those different means of connecting will be made beneficial. Our challenge has been to determine how best to enable high security (a critical foundation to building and maintaining trust) while not impeding development in a rapidly changing world.

The European Union is rapidly advancing legislation that will, upon implementation in the next two years, require UK banks (subject to consent from individuals and businesses) to open access to their customer data and payments capabilities. The UK has diligently fostered a vibrant financial technology environment and stands ready to reap the benefits of that legislation sooner than many other markets. Other markets (in the EU and beyond) have begun to implement aspects of an open banking standard, but none have produced a definitive outline of such a standard, let alone a roadmap for its implementation. There is, therefore, a significant opportunity for the UK economy if we take a lead in this space. This will require that we invest rigorously in development over the next 6-12 months.

Open Banking Standard

Our goal in publishing this Framework today is to enable the accelerated building of an Open Banking Standard in the UK.

It has been developed based on input from an expert group drawn from the banking, FinTech and data communities, building on preliminary work by HM Treasury in the first half of 2015. At its core, the Framework represents a set of foundational recommendations that are intended to allow the process of building the Open Banking Standard to commence immediately. Those recommendations include a broad implementation plan, covering three distinct phases over the course of the next three years.

The implementation plan will, by necessity, need to be flexible over the coming years – both because lessons will be learned as implementation gets underway and because the technology and standards on which it will rely will continue to evolve at a rapid rate in ways that are impossible to anticipate today. Execution of the plan, along with maintenance of the emerging standard itself, will require careful stewardship. Clear and consistent communications will be required to continuously build awareness, understanding and adoption not just with service developers, but also with the individuals and businesses that will benefit.

This latter point is fundamental. Our aim in constructing this framework in the way that we have was to ensure that such an open standard provides the highest quality of service for individuals and businesses, that increases competitiveness, improves efficiency and stimulates innovation. This standard will only be as good as the trust that all of the participants required to make it successful have in it; that will ultimately rely on the trust of individuals and businesses.

Fundamental importance of data literacy

Our work in constructing this framework, as well as more advanced work in other sectors, has repeatedly highlighted the fundamental role of data literacy in supporting the creation of any open data standards. We must align on a common vocabulary – one that cuts across sectors, even if there is sector-specific terminology that must be brought into it.

The Open Data Institute (ODI) has done a tremendous amount of work in beginning to build that vocabulary and we commend it to anyone. To aid that, and ensure that readers of this report interpret its contents consistently, we have included a brief glossary of critical terminology used within this report or related to its contents.

Given the importance of data literacy and a common vocabulary, our working group opened each of its meetings by reiterating a set of core definitions that we used to guide our work; we feel it important to do the same here.

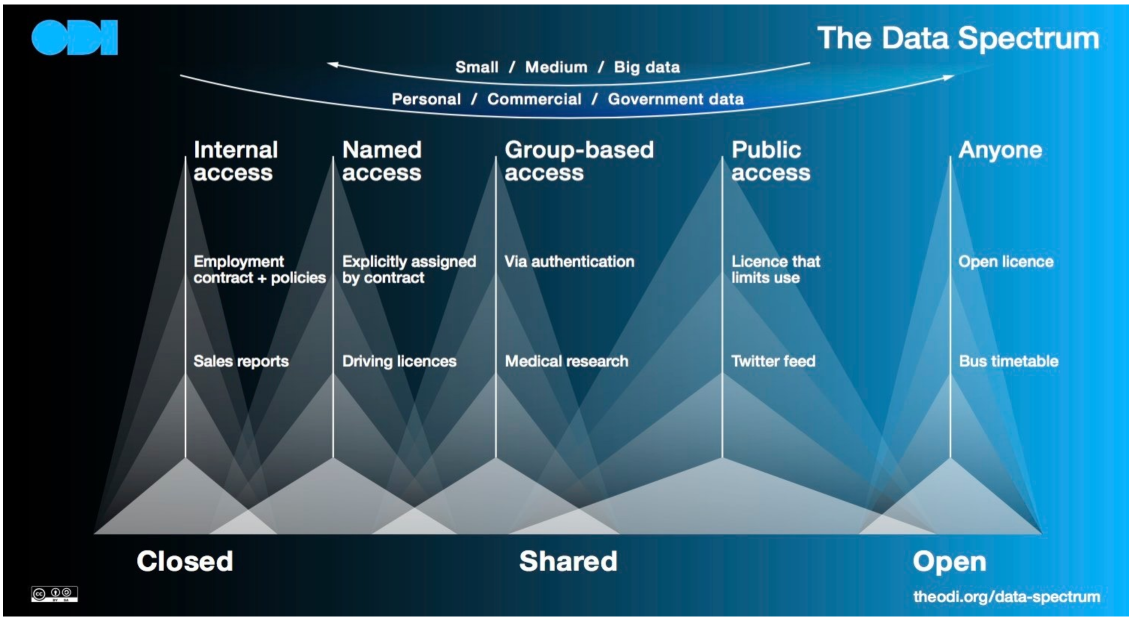
Those core definitions arise from the two important, distinct, but mutually beneficial outcomes that this framework seeks to create:

- an open API for data that is shared, including, but not limited to, customer data; and
- an open data API for market information and relevant open data.

An **open API** is a means of accessing data based on an open standard: it is a public interface.

Data exists on a spectrum of accessibility. The data spectrum ranges from closed to shared to open. The data accessed via an open API may be closed, shared or open data.

Figure 1.1 The data spectrum



* See http://theodi.org/data-spectrum

In fact, it could include data considered to be "proprietary". In that circumstance, the holder of rights to any such "proprietary" data could choose to share (but could not be compelled to do so unless the data was deemed not to be proprietary) that data via the open API, along with stipulations – or licensing terms – related to its use by those with whom it chooses to share it.

Open data is data that anyone can access, use and share. An open data API, therefore, is a public interface that provides access to open data. An example of open data in this context could be financial product information.

Any individual's personal bank details or a company's transaction data are considered **closed** or **shared data**. They will be made available via an open API as a result of the implementation of this work, but access to them would be subject to consent of the individual or business to whom the data belongs and specific governance related to that. Such data **will not be licensed or made public as open data** as a result of this work.

An **open standard** is developed and maintained collaboratively and transparently, and can be accessed and used by anyone.

Key recommendations

There are, of course, significant technical considerations involved in defining and implementing an Open Banking Standard. But the bulk of the work is not technical; there are critical issues to take forward around **governance, security, liability, standards, communications, regulation and legal**. The chapters of this report outline the working group's recommendations in each of these areas. There are a number worth highlighting here because of their relative importance.

- An independent authority should be created, in collaboration with industry, to oversee development and deployment of the Open Banking Standard.
- The Open Banking API should be built as an open, federated and networked solution, as opposed to a centralised/hub-like approach. This echoes the design of the Web itself and enables far greater scope for innovation.
- Customer transaction data (data that is presented to customers in their financial statements, including underlying transaction history, and data that relates to a customer's account through

which payments can be initiated) should be made available, with consent, via the Open Banking API as both customer-related data and aggregated data.

- Protocols will be developed and shared with all participants in the Open Banking Standard to ensure that redactions in data that is shared via the open APIs are truly exceptional, based on specific risk considerations. Further work will be needed to explore the extent of redaction and what alternatives may be available.

- As a principle, existing standards, datasets and structures should be reused where possible and appropriate.

- The Open Banking Standard should be managed within a transparent and open governance framework that will support accessibility, usability and innovation.

- An Independent Authority should be established, whose scope would include consideration of how complaints are handled, how data is secured once shared, as well as the security, reliability and scalability of the APIs provided.

- The Independent Authority would vet third parties, accredit solutions and publish its outcome through a whitelist of approved third parties.

- Customers (individuals and businesses) of services built through the Open Banking Standard will need to understand their responsibility for ensuring their data is protected. When issues arise between participants, third parties and data attribute providers would be expected to resolve these quickly. Where customers are affected they should be able to contact either their third party or data attribute provider to initiate this process. Where issues are not resolved within a specific time period, participants can escalate them to the Independent Authority, which will make a ruling as to whether standards have been breached.

- The Open Banking Standard will have a clear and explicit versioning policy and procedure and use an open repository to maintain and manage changes.

- The Open Banking Standard will be made available under a licence that permits it to be freely used, reused and distributed.

- Permission to access data will only be granted on the basis of informed customer consent, will be subject to constraints (e.g. duration or transaction size) and must be able to be revoked by the customer as easily as they were granted, or, if required for objective reasons, the data attribute provider

- Permission to both “read” and “write” certain data should be granted to third parties via the open API.

- A control framework will be implemented to address the risk profile to set reasonable Open Banking Security Standards in such a way that allows flexibility for future threats and technical flexibility to allow innovation in implementation of the controls.

Key implementation considerations

We believe that the recommendations made in this report should be implemented without undue delay. However, there will not be a single API – there will be many, and the standard envisioned by this report will emerge continuously, through an iterative process, rather than a single event. Following the drafting of detailed design specifications, we expect implementation to broadly follow the release schedule below.

<u>Release 1 – to be completed within 12 months of the report’s publication</u>

Delivery of a “minimum viable product” (MVP) including: 1) the establishment of required governance entities (and their initial scope and processes) and 2) the launch of a tightly scoped Open Banking

API, enabling select, read-access, open data use cases. This release will focus on lower-risk, easily implementable components of the Open Banking Framework.

Release 2 – to be completed by end of Q1 2017

Extension through implementation of select, read-access capability for customer transaction data. By this release's conclusion, third parties will be able to access the midata personal customer data sets via the Open Banking API on a read-only basis.

Release 3 – to be completed by end of Q1 2018

Significant build-out of governance entities and further development of the Open Banking API – to cover the majority of use cases supported by open data and anonymised and aggregated data. Similar functionality outlined in Release 2 to also be provided for midata business customer data sets.

Release 4 – to be completed by end of Q1 2019

All recommendations will be implemented by this stage. In particular, within this release, data and services generally perceived as higher risk will be implemented and will require governance and technical recommendations to have been fully implemented and tested. It will deliver full read and write functionality under the Open Banking Standard as per its target scope.

The implementation section of the report provides more detail on each of these releases.

In closing

The recommendations set out in this report are purposely ambitious. We believe the opportunities to the UK economy – and to the individuals and businesses within that economy – from the successful creation of an Open Banking Standard that will lead the world are enormous. We believe that it is incumbent upon all relevant stakeholders to turn their attention now to starting the important work required to seize that opportunity.

We look to 2016 as the year in which significant momentum must be built. That will require investment to build on open principles, standards and processes to develop the framework into a living Open Banking Standard, continuously iterating to meet the needs of customers and our digital economy. We need to establish a suitable and trusted Independent Authority; to develop and deploy propositions; to create a calendar of events and materials through which we can stimulate action and galvanise the community, especially individuals and businesses; and to develop a long-term business model to make the Open Banking Standard sustainable.

We welcome the support of HM Treasury for the recommendations set out here and its recognition of the importance the level of ambition they represent.

Getting to this stage was not a simple task. It involved the hard work and collaboration of a group of individuals who came together for the first time only a short few months ago. We would like to thank everyone in the team for their support, commitment, challenge and effort – they achieved a tremendous amount in a very short period of time.

We are enormously grateful and privileged to have played a role in helping create this report and look forward to its evolution.

2. Introduction

2.1 Background

In September 2014 the Open Data Institute and Fingleton Associates published a report titled *Data Sharing and Open Data for Banks* (hereafter referred to as the Fingleton Report) at the request of HM Treasury and the Cabinet Office.

The Fingleton Report concluded that "greater access to data has the potential to help improve competition in UK banking" and recommended that banks create standardised application programming interfaces (APIs) that would be accessible by third parties (e.g. FinTechs, developers and other corporates). To facilitate this, the publication recommended that open industry standards be established for data-sharing in banking, thereby enabling the creation of standardised APIs.

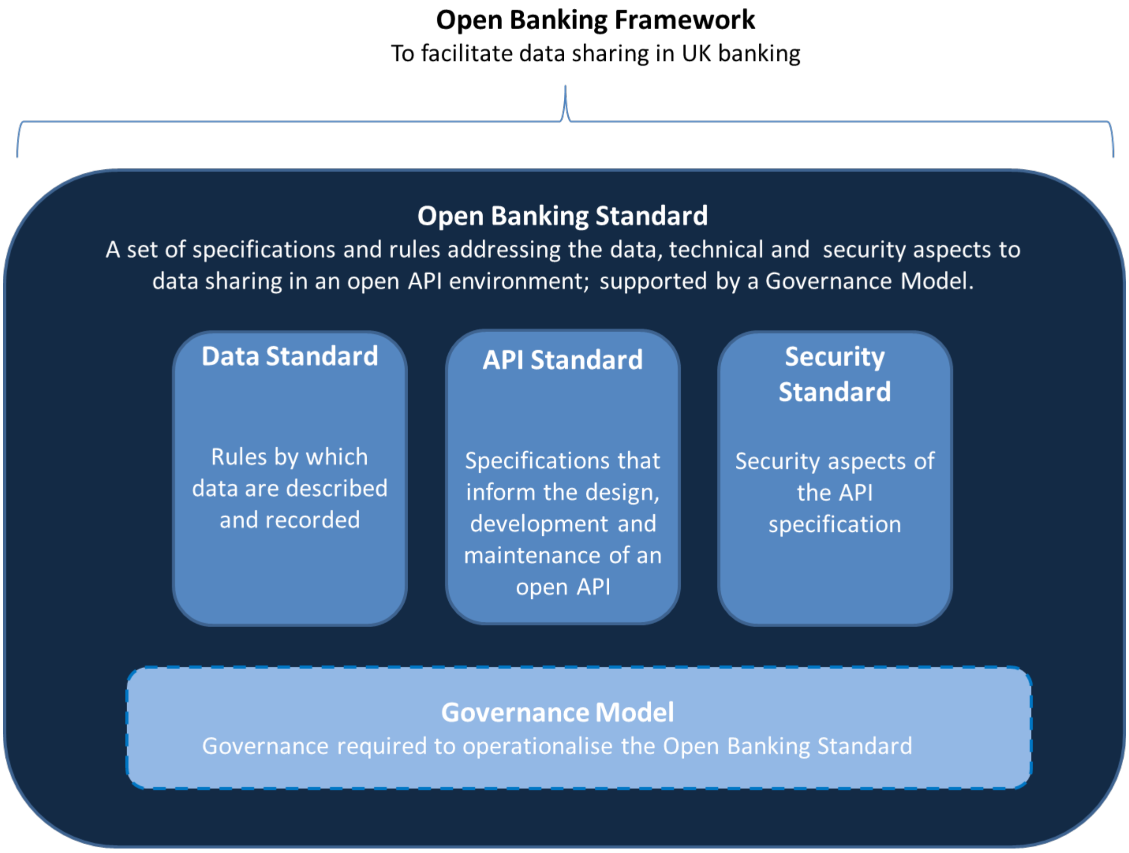
Subsequent to publication of the Fingleton Report, HM Treasury undertook a consultation, sourcing views from across the financial services industry, consumer and business groups and the FinTech community.

The outcome of the consultation was published in March 2015, with many of the respondents supporting the development of open industry standards for data-sharing in banking in the belief it would increase competition and innovation in banking. The consultation also highlighted potential risks around data privacy, consumer education and interoperability, and thus the role the government could play in supporting and standardising the development of an Open Banking Framework.

2.2 Objectives of this Report

Building upon recommendations presented in the Fingleton Report and responses from industry, HM Treasury announced its intention to deliver an Open Banking Framework to facilitate data-sharing in UK banking.

This document provides the framework for adopting these as an open industry standard, hereafter referred to as the Open Banking Standard. There are a number of elements to the Open Banking Standard, which are highlighted below for ease.



Open Banking Framework
To facilitate data sharing in UK banking

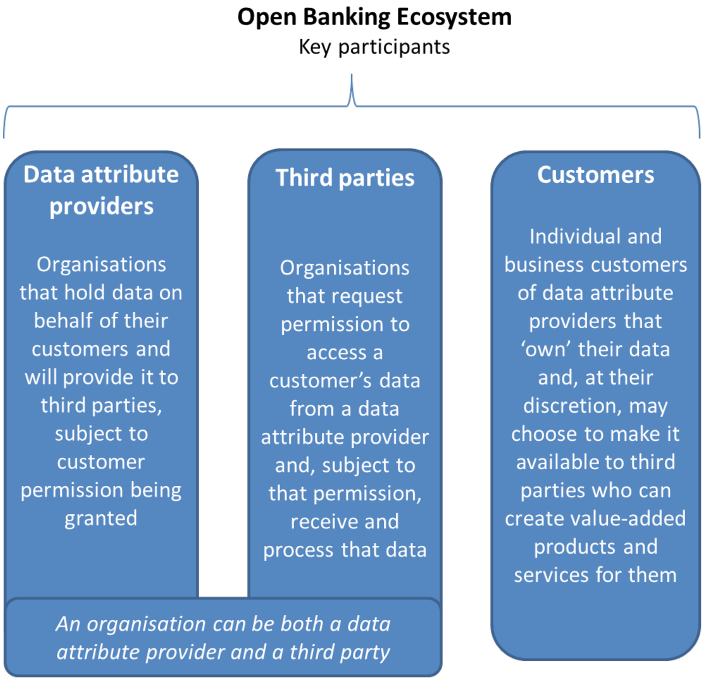
Open Banking Standard
A set of specifications and rules addressing the data, technical and security aspects to data sharing in an open API environment; supported by a Governance Model.

Data Standard
Rules by which data are described and recorded

API Standard
Specifications that inform the design, development and maintenance of an open API

Security Standard
Security aspects of the API specification

Governance Model
Governance required to operationalise the Open Banking Standard



Open Banking Ecosystem

Key participants

Data attribute providers

Organisations that hold data on behalf of their customers and will provide it to third parties, subject to customer permission being granted

Third parties

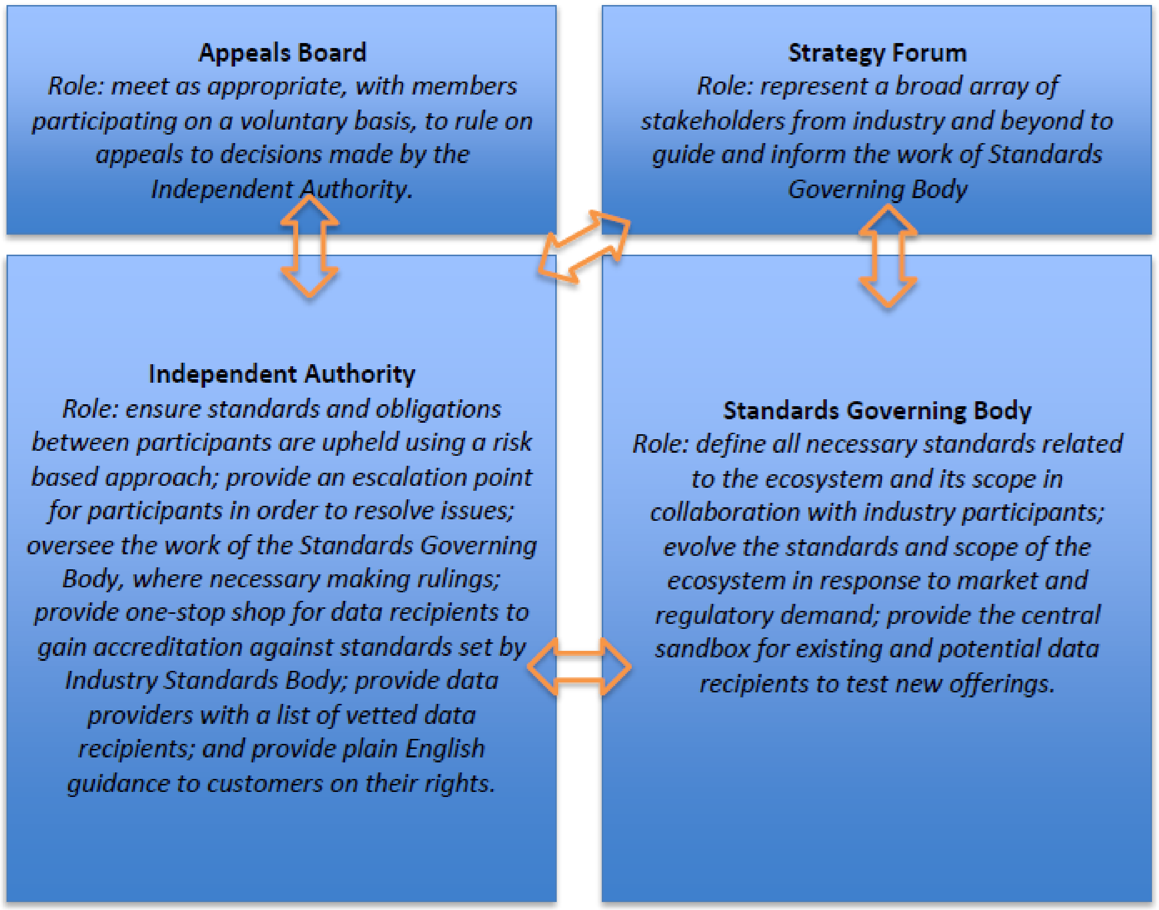
Organisations that request permission to access a customer's data from a data attribute provider and, subject to that permission, receive and process that data

An organisation can be both a data attribute provider and a third party

Customers

Individual and business customers of data attribute providers that 'own' their data and, at their discretion, may choose to make it available to third parties who can create value-added products and services for them

Governance Diagram



Appeals Board
Role: meet as appropriate, with members participating on a voluntary basis, to rule on appeals to decisions made by the Independent Authority.

Strategy Forum
Role: represent a broad array of stakeholders from industry and beyond to guide and inform the work of Standards Governing Body

Independent Authority
Role: ensure standards and obligations between participants are upheld using a risk based approach; provide an escalation point for participants in order to resolve issues; oversee the work of the Standards Governing Body, where necessary making rulings; provide one-stop shop for data recipients to gain accreditation against standards set by Industry Standards Body; provide data providers with a list of vetted data recipients; and provide plain English guidance to customers on their rights.

Standards Governing Body
Role: define all necessary standards related to the ecosystem and its scope in collaboration with industry participants; evolve the standards and scope of the ecosystem in response to market and regulatory demand; provide the central sandbox for existing and potential data recipients to test new offerings.

3. Foundations

3.1 Chapter Outline

This chapter outlines key concepts and terminology referenced throughout this report. These explain what data-sharing entails in the context of banking and financial services, and describe the key mechanisms that are used to share data. They also provide definitions and conceptual overviews of the Open Banking Standard

3.2 Key Concepts and Terminology

3.2.1 Data-sharing

Data-sharing is the process through which access to data is provided from one party to another. The mechanics of data-sharing, including authentication, authorisation and consent, are addressed in more detail in Chapters 7a: Standards and 7c: Security.

In the context of this report, data-sharing is considered from two perspectives:

1. Where an individual or business consents to a third party accessing account-level data stored with a data attribute provider (like their bank or financial services provider), typically on a restricted basis;

2. Greater publication of standardised open data (e.g. bank product data released on money supermarket/price comparison websites).

3.2.2 Application Programming Interface

An API is a method for two software systems to exchange data. A well-designed API allows systems to be loosely coupled such that without any great knowledge of the underlying system or data structure and minimal investment in studying documentation, a software developer can quickly begin to access information.

3.2.3 The Open Banking Standard

Standards in the context of this report describe a set of specifications and rules addressing data, technical and security aspects to data-sharing in an API environment. The Open Banking Standard will be an open standard. It will be developed and maintained collaboratively and transparently, and can be accessed and used by anyone.

Three standards will be considered, which in combination will form the Open Banking Standard:

1. Data Standards: rules by which data are described and recorded, potentially including, among other characteristics, agreements on representation, format, definition and structure. The scope of data to which these standards will apply are detailed in Chapter 5: Scope of Data.

2. API Standards: specifications that inform the design, development and maintenance of an API. This can include guidelines pertaining to architectural design, resource formats, documentation and versioning.

3. Security Standards: security aspects of the API specification A common standard on the underlying data and the mechanism for accessing it will reduce many of the frictions associated with data-sharing and support materially higher customer and third party adoption versus a non-standardised environment based on multiple bilateral relationships.

A Governance Model is also described in Chapter 7d.

3.2.4 The Open Banking Standard

To enable adoption of an Open Banking Standard, recommendations in this report address key considerations in designing, developing and operationalizing the Open Banking Standard

Recommendations will therefore take into account requirements from each participant including:

1. Customers: individuals and businesses who share their data; publishers of open data and

2. Data attribute providers: banks, financial services companies and other organisations through whom data is stored and shared;

3. Third parties: developers, FinTech, and other organisations who use data provided to design and offer new products.

The framework therefore includes:

1. Data, API and Security Standards through which usability of data and APIs will be achieved and customers' data will be protected from malicious actors and access rights can be securely delegated;
2. A governance model, which will develop trust, provide issue resolution mechanisms and oversee the standards;
3. Developer resources, which will enable third parties to discover, educate and experiment.

Chapters 7a-7d outline in detail the aforementioned components and provide guidance on their design and subsequent implementation.

4. Opportunities and Challenges

4.1 Chapter Outline

In this chapter we review the underlying factors that make an Open Banking Standard possible, and highlight the kinds of benefits this can bring to individuals and businesses as well as some of the potential challenges that need to be designed around.

4.2 Opportunities

4.2.1 Driving innovation through data-sharing

The mass adoption of the internet has demonstrated the powerful effect widespread access to data can have.

Collectively, internet companies have collected and organised a vast array of data. This has resulted in the development of a broad spectrum of innovative services ranging from reference sources – including the world's largest encyclopaedia – to the practically useful such as online maps with integrated travel directions, to the niche such as "how to" videos on every imaginable subject.

At first, data was either public, or actively shared by individuals through personal homepages. As the internet became commercialised, businesses began sharing corporate data (e.g. airplane ticket prices, hotel room availability etc.) directly to the public and/or via intermediaries. Furthermore, attitudes of individuals towards data-sharing has also evolved; consumers now use social networks to interface with third-party services and regularly share information to compare prices and receive more personalised services. To date, customers' ability to use their bank data has been limited and restricted to inconvenient workarounds.

4.2.2 GDPR and PSD2 as driving towards an Open Banking Standard

As the collection and use of personal data has increased, individuals, and governments, are seeking more clarity on the basis on which the data is used and their interest safeguarded. The EU is progressing the General Data Protection Regulation (GDPR) initiative in order to fulfil this need. Some basic principles of the forthcoming regulation are to enshrine the individual's rights to:

- data portability – the individual may share their data freely with whomever they choose;
- consent – the individual must provide explicit consent to sharing their data;
- specific usage – the individual's data may only be used for the pre-agreed purposes.

GDPR provides an important framework under which customers' banking data will be assessed and ultimately shared.

The European Commission also issued a proposal for a revised Payment Services Directive (PSD2) in July 2013. Central to its recommendations are requirements for Payment Account Providers to allow third parties – with appropriate consent – to share account information and to initiate payments.

Member states are required to transpose PSD2 into national law and apply the majority of the provisions from two years after publication in the Official Journal (which was published in December 2015). Therefore, transposition at a national level will occur by January 2018.

In order to comply with GDPR and PSD2, many of the components that will enable the Open Banking Standard will have to be built. These components will include technical design and infrastructure as well as an approach to sensitive customer issues such as consent, delegation of access rights, authorisation and authentication, vetting, accreditation and governance.

4.2.3 Leveraging a mature technology in APIs

API technology is the accepted norm for data-sharing and embedding functionality in an online environment. The use of APIs is widespread and today there are more than 14,000 public APIs available.[1] The most popular APIs include familiar names such as Facebook and Google Maps, which are widely used across the Web to embed "like" buttons and maps. Many websites make extensive use of other companies' APIs, which has resulted in a significant amount of innovation and consumer convenience. APIs are a fundamental component of enabling an Open Banking Standard.

Alternative technologies for sharing data exist, but are less robust and less secure than APIs. One of the most common approaches to sharing consumer banking data is through "screen-scraping". In screen-scraping, one system mimics a human user and interacts with the normal webpage. Some objections to this practice include:

- Login credentials are shared directly with the screen-scraping service;
- Access to the host system is uncontrolled and unregulated;
- The technique can fail when web pages are redesigned or new security measures are adopted;
- Consumers are uncertain about the procedure and have little recourse to their bank in case something goes wrong.

4.2.4 Digitising UK banking and strengthening UK FinTech

Customer demand for a digital banking experience is increasing exponentially. Recent BBA research found that 22.9m internet banking apps have been downloaded, an increase of 56% in 2015, and Britons were logging onto internet banking 9.6m times a day in 2015. Meanwhile, branch and telephone banking transactions are falling 6-7% per annum.

In addition, UK consumers are active users of FinTech propositions, i.e. financial products provided by focused, online technology providers such as peer-to-peer lenders, payments providers and personal financial management tools. Forthcoming research by EY suggests that as many as 1 in 6 digitally active consumers are FinTech customers[2] and as many again are expressing a wish to become customers.

Taken together, these trends show that while high street banks are unquestionably digitising, a new group of firms is eager to compete for customers and may be capable of creating a differentiated value proposition. Promoting the sharing of data between banks and FinTechs is an effective means of helping both industries grow, while supporting competition between and amongst them.

[1] See http://www.programmableweb.com/news/telco-apis-offer-huge-revenue-if-carriers-can-handle-disruption/review/2015/09/21

[2] EY FinTech Index

4.3 Challenges

4.3.1 Converting customer interest

Earlier this year, Ipsos MORI was commissioned to conduct research on consumer and small business attitudes to data-sharing. Through a combination of focus groups and online interviews, respondents were introduced to a series of practical use cases based on exchange of financial information between a bank (data attribute provider) and a third party.

While nearly 40% of consumers reacted positively to the concept of sharing financial data, 30% were against the idea, while the remaining nearly 30% were uncertain.

One of the main sources of consumer concern is around security and redress for unauthorised transactions. Generally consumers would expect bank-grade security around their finances, and require some means of financial compensation for security breaches. The Ipsos MORI research finds that consumers expect their bank to be involved in the administration of such claims. Finally, consumers overwhelmingly (77%) believe that third parties accessing their financial data should be regulated.

So while experts agree that data exchange should be able to bring good outcomes for customers, appropriate security and governance safeguards will be needed to develop and maintain trust. In addition, greater customer awareness of the potential benefits and best practice for safely sharing financial information with third parties will be required.

We note the importance of sustained consumer education – this goes beyond raising awareness and helps consumers understand the value of their own personal data and what responsibilities they take on when they share it with third parties. This report considers that the responsibility for consumer education lies with a number of parties including banks, FinTechs, government, consumer and business groups.

Finally it should be noted that this initiative could potentially widen the gulf for two important segments of the UK population, the digital “have-nots” and the unbanked. Research suggests c.8m bank customers do not engage digitally with their bank accounts in any form and a further 2m adults have no bank account. It is recommended that further work is done to assess if the innovative use of bank APIs can be used to actually help in attracting and serving these important groups with products and services that are both relevant and valuable.

4.3.2 Security

Using APIs as a new method for accessing customer data presents cyber-criminals with a new attack vector. Attacks can come in a number of different guises – from those that target technical infrastructure to those that are socially engineered – and capitalise on lack of customer familiarity. The result of such attacks, unless appropriately mitigated, can range from intermittent service provision through to data loss, fraud and identity theft. Therefore it is important to embed best practices in the security field to ensure processes, infrastructure and actors are adequately protected.

In addition to embedding the appropriate structural safeguards including protocols, processes, controls and governance – there is the additional challenge of increasing awareness and “digital literacy” among users (i.e. individuals and businesses). Socially engineered threats (e.g. fake applications) specifically target lack of user familiarity – therefore it is important for customers themselves to adopt a vigilant stance. This will require a general understanding of key processes, safeguards and entities involved in an open banking environment.

5. Scope of Data

5.1 Chapter Outline

This chapter outlines the types of data to be covered by the Open Banking Standard and provides details of their underlying characteristics and associated access rights envisaged (i.e. what third parties will be able to use specific data types for).

In defining this scope, and as a driving principle, this report has sought alignment to products and channels defined by PSD2 (see Appendix 1 for further details). This alignment delivers two key clear advantages should recommendations from this report be acted upon; (1) it simplifies compliance requirements on participating institutions, and (2) it simplifies communications to customers. It should be noted, however, that as of the time this report was written, relevant regulations (such as PSD2 and the EU's GDPR) had not been finalised. As such, subsequent work following this report may further refine or expand the scope as appropriate.

5.2 Data in Scope

5.2.1 Open data

Data that anyone can access, use or share. Examples include product information and ATM locations.

5.2.2 Customer transaction data

Data that is presented to customers in their financial statements (including underlying transaction history) and data that relates to a customer's account through which payments can be initiated. Examples include balance information, transaction history and payment information (i.e. information to facilitate a payment).

5.2.3 Customer reference data

Data about an individual or business that is not directly related to the use of an account, e.g. data that is collected from or generated for a customer as part of an eligibility check, or while being brought onboard. Examples include data relating to Know Your Customer (KYC) processes, anti-money-laundering checks or credit scores.

5.2.4 Aggregated data

Sets of averaged or aggregated data across transactions, balances, other customer data or open data sources. Examples include average number of cash withdrawals per month across a postcode area, successful lending applications by businesses within a SIC code, etc. Chapter 7c.12 covers the need to ensure that any personal data that is released as open data would need to be annonymised and unable to be de-annonymised.

5.2.5 Sensitive commercial data

Sensitive commercial information from data attribute providers: Sensitive information including documents, strategy, price-setting, policies , algorithms and data provided under licence – is not in scope for the Open Banking Standard. At a data subject level, this may include data about profitability that reveals proprietary or competitive insight about a bank's performance, e.g. the average credit score across a customer population, or average margin.

5.3 Permissions and Access Rights

Permissions are rules that grant a third-party access to data within the confines of prescribed functions. The following access rights have been taken into consideration for evaluation against data types.

- Read access – permission that is granted to a third party enabling them to read but not modify a file, set of files, or set of data.
- Write access – permission that is granted to a third party to modify or execute a file, set of files, and set of data. In the context of this report, write access includes payment initiation.

5.3.1 Detailed scope: data attributes by product, channel and access rights

Table 5.1 Scope and boundaries

Scope and boundaries	Customer transaction data	Open data	Open aggregated data
Data granularity	Individual customer/business account level	By design, this should be non-customer data (e.g. product features)	Currently limited to postal district (SW1A) level. There are c.2,500 districts in the UK Limited to at least 10-year age bands
Interaction channel	Online accounts only	Data can describe all channels (but will be delivered online)	Data can describe all channels (but will be delivered online)
Products	Individual & business current accounts Savings accounts Credit cards	Individual & business current accounts Savings accounts Credit cards	Individual & business current accounts Savings accounts Credit cards Loans Mortgages

		Loans Mortgages	
Product availability	All products held by the individual/business as long as the account is open	Only products available for sale on or after 1 Jan 2016	Only products available for sale on or after 1 Jan 2016
Interaction history	25-month history from date of request	N/A – not customer-level data	N/A – not customer-level data
Account status	Open accounts	N/A – not customer-level data	N/A – not customer-level data
Market sectors	Requests from entities only	N/A - open data	N/A - open data
Data transit mechanisms	Read-only API Read/write API	Read-only API	Read-only API
Standardisation	Merchant metadata	Product definitions	Path to purchase definitions (e.g. to allow product applications to be compared across providers

6. Customer Benefits

Standardised bank APIs have the potential to dramatically improve competition and innovation in UK banking to the benefit of individuals and businesses. As financial services are brought into the API economy, it is expected that existing providers and new entrants would compete to dramatically improve existing products by making them more intuitive, personalised, convenient and integrated. In addition, customers would be expected to benefit from a suite of new propositions that are enabled through open APIs. While the breadth of innovation could be vast, this chapter seeks to highlight a small number of the products and services that may arise in this new environment. The basic customer journey, which forms the starting point for all the propositions, is outlined first.

6.1 The Basic Customer Journey

The products and services outlined below are different in nature. However, they all share the same basic customer journey. The journey starts when a customer sees an option to share their data with a third-party for a specific purpose. If the customer wishes to proceed they are directed to their data attribute provider (e.g. their bank) to log on and provide their consent (without sharing their log-in credentials with the third party). Following this, the customer is automatically redirected back to the third-party, at which point it now has access to the specified data for the specified purpose. Some important considerations are built into this journey:

- The customer's consent is attached to specific permissions against specific data.
- The third party may only use the data for the specified purpose.

It should be noted that the customer has the ability to review permissions across all their data attribute providers and third-party applications at any point and revoke them.

Six possible propositions are highlighted below that have the potential to deliver real utility to UK individuals and businesses.

6.1.1 Proposition 1: current account comparison services

The Competition and Markets Authority (CMA) found that UK consumers could save money if they switched to the current account best suited to their needs. Its analysis suggested consumers could save up to £70 a year on average by switching accounts,[3] overdraft users could save on average £140 a year and heavy overdraft users would save on average £260 a year.[4] With 68m active personal accounts in the UK covering 97% of the population, this represents a material potential saving to the UK consumer. Over the past three years only 8% of consumers switched their current account, versus 31% of consumers switching energy providers over the same period.

The CMA concluded that the difficulty in comparing accounts was a particular obstacle and recommended upgrading the midata initiative. Midata was created to help solve the comparison issue

[3] http://www.theguardian.com/business/2015/oct/22/high-street-banks-survive-competition-inquiry

[4] CMA: Retail banking market investigation, November 2015

by allowing consumers to share their transaction data with price comparison websites. However, midata usage has been relatively low as it is hard to use – it requires the consumer to download a CSV file, in Excel, from their bank and then upload it into the price comparison website.

An Open Banking API could eliminate the friction involved in the download/upload model and materially improve the consumer experience. A consumer would simply give a price comparison service permission to access their bank account data and the rest would happen "behind the scenes" and in real time. This service could even be engaged as an ongoing service with regular automatic reviews, or respond to new offers launched into the market. The principle could also be extended to other personal financial products, in particular credit cards and mortgages.

The CMA also recommended making price comparison initiatives available to SMEs, which account for 5.5m active business current accounts in the UK.

Required data:

- Individual transactional (current account usage) data for individuals and businesses.
- Certain data sets available as open data: current account tariffs as a minimum, but could be extended to customer service, branch location, opening hours, digital functionality.
- Further opportunity in credit cards, mortgage and other lending and savings products.

6.1.2 Proposition 2: personal financial management

Personal financial management tools (PFMs) help consumers to budget better and understand their overall financial position, by helping them categorise and manage their spending using visualisation tools and predictive cash flow tools. They often pull information from other financial services products, such as credit cards and savings accounts, to provide an aggregated view to the consumer. PFMs can also help consumers potentially save money in non-banking products by looking at spending patterns in products such as energy, telecoms, groceries or insurance and suggesting alternatives.

PFMs are popular in the US, with 32% of consumers using them to manage their finance, of which approximately three-quarters use third-party solutions such as Mint or yodlee.com.[5]

PFM uptake in the UK has been low primarily because consumers cannot give PFMs access to their transaction and balance data. To date, the typical workaround has been for the PFMs to screen-scrape the data from the banks' online web pages. This forces consumers to share their login details with the PFMs, which makes some consumers uncomfortable and in some cases invalidates banks' own terms and conditions. Under an Open Banking API, customers would be able to grant access to their data securely and efficiently without sharing their password with any party other than their bank.

Should UK consumer uptake of PFMs reach US levels of c.32%, it would suggest 10-15m potential users. A recent UK survey suggested that 39% of consumers felt positive about sharing data via an open API for the purposes of aggregating financial information.[6]

Required data:

- Individual current account data (balance and transactional) for individuals.
- Adding in additional products – credit card, savings, lending.

6.1.3 Proposition 3: access to credit

[5] Novantas, 2014

[6] Ipsos MORI, open API Barclays 2015

Historic transactional data is an important determinant of credit quality and real-time transactional data is a valuable indicator in the ongoing serviceability of loans. Currently this information is only available to the current account provider, which means third-party providers may not be able to offer the best terms to users when they shop around. It is noted that c.90% of SMEs procure loans from their primary banking relationships while c.50% of consumers[7] are likely to purchase new banking products from their current bank. With an Open Banking API, individuals and businesses will be able to share transactional data securely with potential providers of credit to achieve the best possible deal (in terms of rate, quantum and speed).

An additional but related benefit is that consumers could tap third-party credit in real time to avoid paying fees on unauthorised overdrafts. Unauthorised overdraft fees amount to c.£600m per year for UK consumers.[8] With anOpen Banking API, customers would be able to share real-time balance information with credit providers, which would fund the account on pre-agreed triggers using faster payments. This would have the effect of unbundling lending from the current account.

Required data:

- Individual current account data (balance and transactional) for individuals and businesses.

6.1.4 Proposition 4: affordability check

An integral part of the application process for a loan product for individuals and businesses is an affordability check. Lenders typically require applicants to provide bank statements (up to 12 months for businesses and typically three months for individuals). At present, applicants need to provide paper copies of their bank statements, or download them for scanning, then upload or email them to their prospective lender. The credit decision is only determined when all data is collected.

An Open Banking API would allow credit applicants to avoid manually extracting bank data and share it seamlessly by providing one-time permission to review historical data. This would speed up the application process and enable a user to shop around with more potential providers. It could also help with certain identification requirements, such as checking for evidence of active accounts held.

Required data:

- Individual one-time current account data (balance and transactional) for individuals and businesses.

6.1.5 Proposition 5: online accounting

Many businesses are using increasingly sophisticated online accounting packages that are able to import transactional data in order to reconcile the cash book and the general ledger. In many situations this functionality is not supported by the banks and consequently is a manual process, often performed by the business owner.

If an Open Banking API were available from current account providers, reconciliation of payments could be made easier and free up valuable time. All that would be required would be for the business owner to log into their accounting solution; they would choose which bank account/s to link and provide their permission for the data to be shared. There are c.500,000 businesses in the UK with between 5 and 50 employees[9] for whom this could be a compelling proposition.

[7] https://www.pwc.com/gx/en/banking-capital-markets/publications/assets/pdf/pwc-new-digital-tipping-point.pdf

[8] https://assets.digital.cabinet-office.gov.uk/media/53c834c640f0b610aa000009/140717_-_PCA_Review_Full_Report.pdf

Required data:

- Individual transactional (current account usage) data for businesses.

6.1.6 Proposition 6: fraud detection

Fraud costs the UK consumer c.£570m per annum.[10] Currently customers rely on their account providers to notify them of fraudulent activity on their accounts. Some customers may believe that third-parties specialising in security and the detection of fraudulent transactions may offer better quality monitoring and notification services. This may be particularly compelling if the third party aggregates data across multiple accounts or products and can spot patterns that a single product provider would otherwise not see.

Required data:

- Individual transactional (current account usage) data for individuals and businesses.

The six propositions described above were chosen from a long list to highlight the kind of innovative and valuable propositions that Open Banking APIs could enable. Two propositions are notable by their absence: KYC and payment initiation. KYC is a regulatory requirement all financial providers must now undertake when onboarding new clients. In theory, an Open Banking API could be used to port across a customer's KYC profile to a third party; however, this becomes a form of identity that is considered to be out of scope for this report (albeit it could be considered in conjunction with the government's work on identity, particularly GOV.UK Verify). Payment initiation is the ability of third parties to initiate payments on behalf of customers of financial institutions. It offers good utility to users and dispenses with the need to input credit and debit card details multiple times in an online environment. Payment initiation has not been included above, as it is a clear and stated objective of PSD2.

[9] https://www.gov.uk/government/statistics/business-population-estimates-2015

[10] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2015.asp

7. The Open Banking Framework

7.1 Overview

To enable the effective sharing of data between parties, this report will outline a framework for developing and operationalising an Open Banking Standard across UK banking.

7.2 The Role Standards Play in Data-Sharing

Standards in the context of this report describe a set of specifications and rules addressing the data, technical and security aspects to data-sharing in an API environment. Three types of standards will be considered – in combination these form the Open Banking Standard referenced in this report.

1. Data Standards: rules by which data are described and recorded, potentially including, among other characteristics, agreements on representation, format, definition and structure. The scope of data to which these standards will apply are detailed in Chapter 5: Scope of Data.
2. API Standards: specifications that inform the design, development and maintenance of an API. This can include guidelines pertaining to architectural design, resource formats, documentation and versioning.
3. Security Standards: security aspects of the API specification.

By adopting common standards across the banking industry, many existing frictions associated with data-sharing can be reduced.

Data standards will make it easier to create, share and release data by establishing a clear and common understanding of what the data means, how it is represented and what state and quality it will be released or received in. API standards, in addition, will help establish greater uniformity across developer experiences when accessing data through different providers. Security standards help to protect customers from malicious actors (Chapter 7c).

Usability markedly increases in a standardised environment, driven by greater consistency, integrity, accuracy and overarching ubiquity and interoperability of both the underlying data and the API platforms through which access is granted. This is expected to result in far greater sustained participation among developers and therefore among third parties and data attribute providers.

7a. Standards

7a. 1 Outline

Standards are a key enabler to market-driven innovation. They provide uniform infrastructure to compete and innovate upon, and when distributed on an open basis help reduce market inertia and unlock network effect benefits from ubiquity. By improving access to APIs and data, a more diverse ecosystem of third parties will be cultivated whose participation will lead to greater product innovation and choice for customers.

This chapter outlines the underlying types of standards that should comprise the Open Banking Standard. It provides an overview of their specifications and guiding principles for design, development and delivery. Security Standards are addressed in Chapter 7c.

7a. 2 Key Recommendations

7a 2.1 Specifications for the Open Banking Standard

- The Open Banking Standard will include both API and data standards, thereby addressing both the underlying data and the mechanisms through which data is accessed. It will also include security standards, which are addressed in Chapter 7c.
- The API Standard should comprise the following specifications and/or meet the following criteria:
    - Use of REST as an architectural style and HTTP as the transport;
    - Use of JSON as the resource format;
    - Achievement of Level 2 from the Richardson Maturity Model;[11]
    - Adoption of a vendor and technology independent definition.
- The API Standard should comply with the following versioning requirements:
    - Support for major and minor releases;
    - Backwards compatibility for all minor – and as far as possible – major releases;
    - Prescription of minimum support time periods for major releases;
    - Embedded flexibility/response speed for security or functional errors.
- The API Standard should be designed with the following features:
    - A controlled core – hosting shared resources should be established and this should represent the slowest-changing part of the standard;

[11] http://restcookbook.com/Miscellaneous/richardsonmaturitymodel

  - Local extensions “at the edges” should be permitted, allowing for API provider innovations with subsequent potential incorporation back into the core;
  - Specific characteristics allowing API providers (data attribute providers) to address scalability challenges.

- The Data Standard should be defined to enable consistency and standardisation.

7a 2.2 Key principles for development and distribution

- The Open Banking Standard should endeavour to reuse and align with existing open standards, data sets, structures and semantics wherever possible.
- The Open Banking Standard should be provided on an open basis, available for access and use by anyone.

7a 2.3 Licensing recommendations

- The Open Banking Standard should be made available under a CC0[12] licence (effectively public domain) to promote its use, reuse and distribution. Failing this, CC-BY[13] (attribution) would be recommended.
- Open data in scope should be published under a CC0 licence (i.e. the same licence used by the Global LEI[14] system), thereby avoiding barriers to reuse and “licence chains”.
- System software should be made available under a MIT Licence, allowing the software to be as permissive as possible and thus avoiding difficulties when integrating with proprietary software.

7a. 3 Purpose, Principles and Policies

7a. 3.1 Principles

To deliver enhanced innovation and competition, the Open Banking Standard will be designed in accordance to the following principles.

- Openness – ensuring accessibility for all interested parties, across a wide range of participants, thereby incentivising adoption, distribution and participation.
- Usability – facilitating ease of implementation and a smooth user experience for participants.
- Interoperability – promoting and progressing towards an environment where data can be exchanged between parties in a frictionless manner across organisational and technological boundaries.
- Reuse – adopting and leveraging existing standards, taxonomies and data lists wherever possible and practicable to avoid duplicative efforts and maximise interoperability.

[12] https://creativecommons.org/about/cc0

[13] https://creativecommons.org/licenses/by/4.0

[14] https://www.gleif.org/en/lei-focus/what-is-an-lei

- Independence – promoting competition among and avoiding dependencies on vendor solutions and technologies; preserving optionality in delivery models and implementation technologies.

- Extensibility – establishing flexibility and encouraging adoptees to build upon the standard and innovate locally, while providing governance mechanisms to subsequently bring extensions “back to the core”.

- Stability – ensuring the provision of a stable environment for all participants where change is communicated, actioned and governed in a transparent and consistent manner.

- Transparency – providing visibility and clarity on issues pertaining to the standard and the environment it operates in (for instance its design, specifications, governance).

7a. 3.2 Policies and considerations

7a. 3.2.1 Openness and participation

Within the context of the Open Banking Standard, the definition[15] of an open standard is one developed and maintained collaboratively and transparently, and that can be accessed and used by anyone. However, it should be noted that there is no universally accepted definition of this term. The policy should also include the following.

> *All stakeholders should have the same possibility of contributing to the development of Open Banking Standard, which must include a public review as part of the decision-making process; the standards will be available for everybody to study; it is proposed that intellectual property (IP) rights of the [stakeholders] related to the specification would be worked around wherever possible, but any deemed essential are licensed on RAND [reasonable and non-discriminatory] terms or on a royalty-free basis to adopters of the standard, subject to an appropriate IPR governance framework being agreed.*

There is, however, no universally agreed definition of RAND and in practice some of the terms adopted may present difficulties for the open source software development model in relation to patents and royalty payments. The approach to RAND is discussed in more detail later in this chapter, as too is the approach to IP and patents.

7a. 3.2.2 Adoption of open standards

To best align with the principles specified in 7a. 3.2, the Open Banking Standard’s underlying solutions should represent open standards, thereby satisfying the following criteria. They should be:

- maintained through a collaborative and transparent decision-making process that is accessible to all parties and independent of any individual supplier;

- adopted by a specification or standardisation organisation, or a forum or consortium with a feedback and ratification process to ensure quality;

- published, thoroughly documented and made publicly available at zero or low cost;

- implementable and shareable under different development approaches, on different platforms.

7a. 3.2.3 Development of open standards and consideration of non-open standards

[15] Aligned to the European Interoperability Framework version 2.0.

Suitable open standards are not always available. Therefore, the Open Banking Framework must ensure engagement, as a key stakeholder, in the development of relevant open standards and take a pragmatic approach to the selection of appropriate standards that help to reduce cost, promote innovation and meet the needs and objectives of the Open Banking Standard.

Further work will be required to assess how standards that are not fully open can be made compatible within the context of the Open Banking Standard.

The following should be considered should compatibility of non-open standards be evaluated:

- Selection process – if and how utilisation of a non-standard can qualify and be justified for adoption.
- Implementation compatibility – at a minimum, standards should be licensed on a RAND or royalty-free and non-discriminatory basis, and terms and conditions must be compatible with the standard in both proprietary and open source software. Further considerations may be required.

7a. 4 API Standards

7a. 4.1 Approach, requirements and outcomes

As per the principles and policies, in defining the API Standard, the following approach should be taken.

- Existing open standards should be used wherever possible.
- Existing taxonomy and data lists (e.g. currency descriptions) should be used wherever possible and in instances where the standard itself cannot be used.
- Developer experience should play a significant role in informing design and a great developer experience should be seen as a key outcome.
- A working assumption has been made that the Open Banking API will initially be pull rather than push and that streaming protocols will not be considered in early phases.

In addition, the Open Banking API will specifically require:

- a tight API schema (URIs, request and response) on open repositories (e.g. GitHub);
- minimum publishable Key Performance Indicators (KPIs) due to potential business criticality and to manage expectations regarding performance;
- clear change control and versioning procedures to lessen the impact on API providers and consumers;
- once developed, the Open Banking API should align to the principles and specifically exhibit:
    - openness with no commercial barriers to entry;
    - technology and vendor independence;
    - minimal commercial or technology barriers to adoption, i.e. free from vendor costs, or licensing that prevents reuse, use of complex technologies, IP, etc;
    - freedom to innovate extensions to the standard (within a governance framework).

It should be noted that there are a number of emerging financial API sets in the market, but there is no existing standard that meets all requirements for an Open Banking API.

7a. 4.2 Architecture style

A number of architectural styles are used for Web APIs (i.e. APIs that use HTTPs as transport). Two of the more common are RPC and REST (REpresentational State Transfer).

7a. 4.2.1 Consideration of SOAP

SOAP (Simple Object Access Protocol) is a popular, mature, standardised RPC protocol. Microsoft originally developed SOAP as a replacement for older technologies that were not optimised for the internet. SOAP is based on XML, which works better over the internet than older RPC protocols using binary messaging. It is also extensible, with a wide range of existing standard extensions for security, addressing, messaging, etc. However, while SOAP is a mature technology, many developers find it heavyweight and difficult to use. The XML messages can be large and cumbersome, and the extensions can be complex to use.

7a. 4.2.2 Recommendation of REST

REST is a lighter-weight alternative to SOAP; it describes the architectural style of the Web. The Web's simplicity represents a key strength and RESTful APIs (i.e. APIs that follow the REST style) follow this simplicity by using URIs to address resources, HTTP methods and headers for actions, and representations for transferring state.

RESTful APIs are therefore easier for developers to use; the majority of modern Web APIs now use REST rather than SOAP.

However, REST is an architectural style, not a protocol or standard, and it allows for notable flexibility. As a result, the Open Banking API must define an unambiguous RESTful standard that specifies the exact interface to which all implementers must adhere. For example, it should specify the resources, HTTP methods, status codes, data formats, REST maturity model, URI naming, versioning, data formats, etc.

A common approach to evaluating the design of a RESTful API is to apply the Richardson Maturity Model, which has several "levels" reflecting the degree to which a given API conforms to the REST style. The Open Banking API should attain Level 2 on the Richardson Maturity Model at a minimum.

7a. 4.3 Resource formats

7a. 4.3.1 Recommendation of JSON

A number of data representations are available under REST (the recommended architectural style), including JSON and XML.

JSON (JavaScript Object Notation) is a popular, lightweight format that is easy for computers to parse and generate, and easy for humans to read and write. It is also programming language-independent and widely adopted for modern APIs.

However, unlike JSON, XML is currently in use in several existing financial formats. Consequently, there is a tension between the reuse of a financial standard (in XML) against developer preferences and their forward-facing expectations (supported by JSON's position as the default for modern APIs).

Given the trend in the industry strongly favours JSON over XML, the Open Banking API should adopt JSON to lower barriers for adoption and participation among its users.

7a. 4.4 API definition

To create the Open Banking API in the REST style, it is important to have a clear and unambiguous definition of the interface, i.e. URIs, requests, responses, HTTP methods and status codes.

There are several competing approaches for describing REST APIs, including RAML (RESTful API Modelling Language), HAL and SWAGGER (OAI).

A single descriptive language should be recommended; this will be addressed in future work.

7a 4.5 Versioning

Change control, i.e. semantic versioning,[16] needs to be managed effectively otherwise adoption of the Open Banking API could be negatively affected. Versioning should be explicit and a changed API should not be released without a new version.

The versioning process should:

- use release numbers for major and minor releases;
- provide/aspire to backwards compatibility for *all* API changes;
- provide backwards compatibility for all minor releases on a mandatory basis;
- support additive changes for minor releases;
- guarantee support for developers for major API versions, for a specified period;
- escalate security implementations when vulnerabilities come to light;
- apply to the data structures sent in the API requests and responses and, wherever possible, follow W3C Best Practices.[17]

7a. 5 The Open Banking API in Practice

7a. 5.1 Tight core but with extensibility at the edges

One of our guiding principles is to encourage innovation on the Open Banking API by extensibility (see 7a 3.2). This, however, needs to be balanced against stability, as API providers and consumers should be protected from adverse impacts from change. To strike a balance, a layered approach is proposed that allows different parts of the standard to change at different speeds. This will encourage "builds" on top of a stable "core".

7a. 5.1.1 Stability at the core

[16] http://semver.org/

[17] http://www.w3.org/TR/dwbp/#bestPractices

The core to the standard will specify resources that are common to all business areas, including shared resources such as identity, core account information, core product information etc. Changes in the core are expected to have an impact on every API and should therefore be managed carefully and occur relatively infrequently (e.g. once per half-year); the core should represent the slowest-changing part of the standard. Subsequent work will define the core in more detail.

7a. 5.1.2 Forking the standard

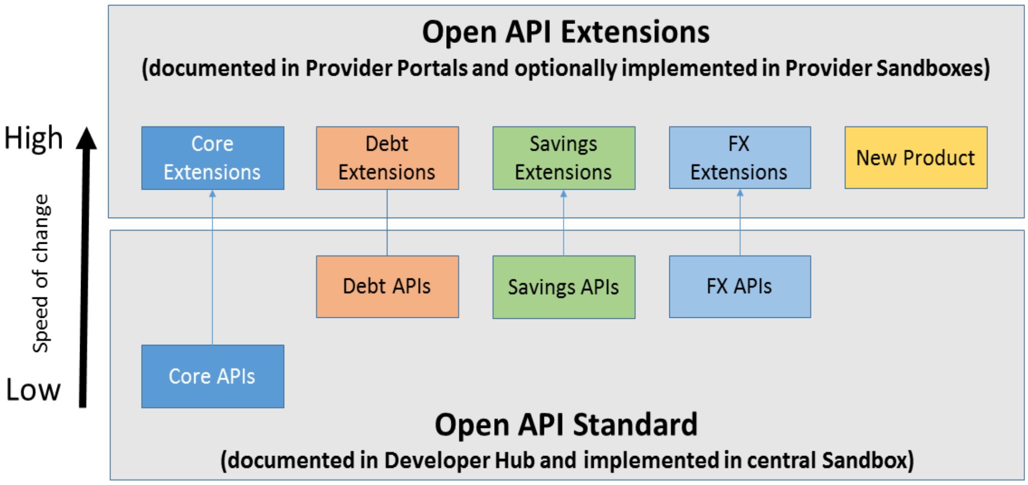
Domains included in the API are expected to be product-focused (e.g. cash account services, mortgage-related services, savings-related services). API providers are unlikely to implement every part of the API specification. It is likely that there will be domain-specific parts of the API that providers focus on. Therefore to enhance innovation and competition, developers should be able to "fork" the standard locally.

7a. 5.1.3 Extending at the edges

Extensions can be made to the core or to a product set. They can also be used to start a completely new product set of APIs. All extensions can be done without asking permission, to encourage innovation at the rate of the faster innovator.

Extensions to the standard should follow, where possible, the API Standard to ensure consistency across all APIs. These extensions may be subsequently incorporated into the core or a product domain, following approval within the governance model.

Figure 7a.1 Open API extensions



7a. 6 Change and Innovation (the GitHub Approach)

Change should be managed in a manner that encourages innovation and quick changes to the standard, while maintaining control of the core to minimise the impact of change. It’s important for all changes to be managed in an open manner, to be subject to critical review and to be documented with a full audit trail, including explanations.

A number of models exist to facilitate management of a layered API. GitHub represents a good, transparent implementation of a technical solution; it provides revision control and is well suited to editing a file in a distributed fashion.

The specification for the API Standard needs to have an open licence (potentially a maximum permissive licence, e.g. MIT) so users can fork and experiment. In GitHub there is still one canonical standard; the forks are duplicates (i.e. they are not “real” until they are merged in), so API providers can work on their own fork (see 7a. 5.1.2).

7a. 7 Control, Access and Security

7a. 7.1 Identity and identifier standards

The introduction of the Open Banking Standard may require a new approach to identifiers – particularly covering usage of standards and developer resources (see Chapter 7b for more on developer resources). These identifiers could enable the identification of parties, resources, devices, applications and products.

As a set of ongoing principles, identifiers should be:

- unique, so that they can unambiguously identify a given “object”; and
- non-proprietary, so that they can be freely used within the system without adding IP restrictions to data.

A good example of the trend towards unique, non-proprietary identifiers is the LEI, which identifies legal entities involved in financial transactions. Overseen by the world’s financial regulators and central banks, the LEI, and its associated reference data, is published under a CC0 licence allowing for free and unrestricted use.

More work will be required to determine if identifiers are needed, the instances in which they are needed and how a standard approach can be defined.

7a. 7.2 Permissions and entitlements

To preserve security and entitlement flexibility, these recommendations should be followed:

- Sensitive information should not be included in URIs as they are not considered secure (problems include attack vectors that leverage web server logging, caching, browser history, user agents, referrer header, etc.).
- Sensitive information should be replaced by a token, or with an indirect object reference (e.g. “account1” instead of an actual account number).
- Granted entitlements should be kept separate from resource descriptions, to enable flexible and sophisticated entitlements to be supported in the future.

More details on the security elements of the Open Banking Standard are available in Chapter 7c: Security.

7a. 7.3 Scalability and performance

Adoption of the Open Banking Standard could lead to increased load on legacy systems for API providers. In order to address this scalability challenge, implementers may leverage caching infrastructure to reduce the load on the core banking system.

A caching strategy will address read-based scalability challenges (i.e. the serving of data), which should represent the majority of API interactions. For API interactions that are write-based (e.g. instruction of payment) these should, where possible, be modelled asynchronously. Where appropriate for customer experience both parties will be able to perform other tasks while a response is being created and sent. Modelling these interactions asynchronously allows the core banking system to service the requests on a pull rather than push basis, eliminating the risk of overload.

The API specification should facilitate read-caching through the appropriate use of HTTP methods (i.e. GET/HEAD for read operations) and by permitting the use of HTTP caching mechanisms (e.g. expiry via cache control, conditional read via ETag/If-Match, etc.).

The API specification should facilitate write-asynchronicity by modelling as many write interactions as possible as asynchronous.[18] The API specification should define a generic protocol for asynchronous interaction that can be reused consistently across the entire API.

7a. 8 Data Standards

7a. 8.1 Requirement for standardised business data

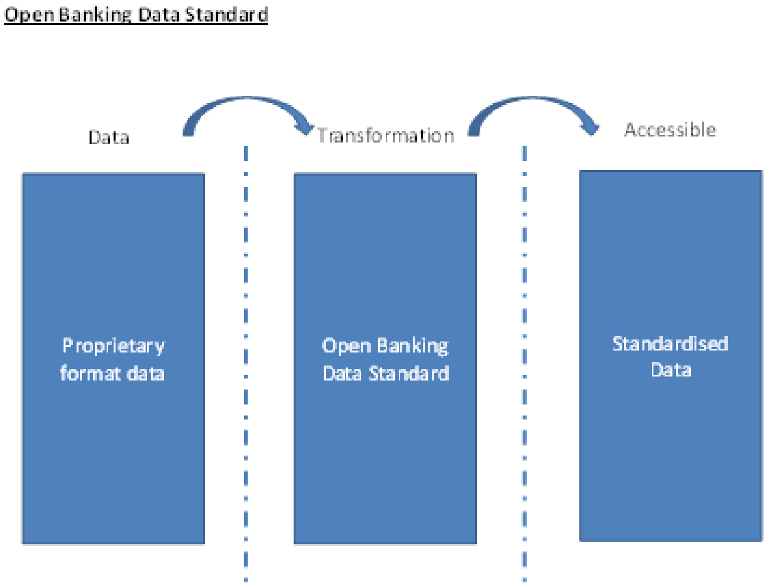
For the Open Banking Standard to reach its full potential, common business semantics (i.e. the meaning and understanding of data) and data consistency must be addressed.

A Data Standard (reference data model) is therefore needed to simplify and standardise data required for the Open Banking API. This is vital in ensuring that common data is made available in a uniform and consistent manner. Harmonisation will also allow non-standardised proprietary data to be made available in a common standardised way, enabling consistent usage.

For example, if the Open Banking API is used to source interest rates for personal current accounts and business accounts, each provider of that information (operating under the Open Banking Standard) would make that data available in a uniform and consistent structure, so that it can be called upon in an interoperable manner. It is recognised that harmonisation across all institutions represents a challenge.

[18] For an example of how this can be done, see https://www.tbray.org/ongoing/When/200x/2009/07/02/Slow-REST

Figure 7a.2 Open Banking Data Standard



7a. 8.2 Reference data model

The reference data model will describe data that is shared under the Open Banking Standard in a manner that is technology-neutral, consistent, reusable and well defined. It will form a library of structured and individual business components, data components and data structures (data types or patterns) described in a uniform notation. The model will be used by all those that adhere to the Open Banking Standard (a similar approach has been implemented by the World Customs Organisation).[19]

Data sets will be developed based on the scope of the data necessary to support the functionality of the core. Data elements and code lists will be aligned to the greatest extent possible with existing international data standards. Over time, as the scope of the data extends so too will the reference data model.

At this stage, it is still open to further investigation whether existing data models can be reused, such as the ISO 20022 Financial Repository,[20] or whether the Open Banking Standard will need to define and maintain a separate reference data model.

For further detail on existing data standards, please refer to Appendix 7: Existing data standards.

[19] See http://www.wcoomd.org/en/topics/facilitation/resources/~/media/70998C307D3C47C996DB047B664B92AE.ashx

[20] See https://www.iso20022.org/financial_repository.page

7a. 9 Open Data

Open data (as defined in Chapter 5) should be accessible via the Open Banking API and have its terminology harmonised through the reference data model (see section 7a 8.2). Open data should form part of the core Open Banking API and therefore needs to be consistently implemented across all organisations.

Open data should also adhere to the principles of open access and treatment of IP (such as codes, software, reference data, etc.). The licence rights to use open data need to be clear and potentially included as a field within the JSON.

7a. 10 Governance

7a. 10.1 Decision-making

In terms of deciding what will be adopted into the API and Data Standards, it is recognised that there are a variety of options (models such as Apache, W3C, OpenStack, etc.). It is recommended that any control should be light touch and appropriate. It is this report's view that some kind of standard moderator mechanism is required. What rights the body has and the precise mechanism defining how decisions about changes to the core Open API and Data Standards are made will need to be considered in the next stage of work. The decision-making process should be distributed in a way that is accessible, open to challenge and agile.

The developer hub (see Chapter 7b: Developer Resources) could be used as a means of ensuring process transparency. Those involved would not have preferential access for making changes, i.e. they should not have a separate process because they are part of the group.

There may exist the possibility to reuse governance structures of existing standards bodies for the Open Banking Standard, but this would need to be explored further.

7a. 11 Intellectual Property and Patents

7a. 11.1 Copyright and IP (relating to the Open Banking Standard)

To the extent possible, the copyright for all Open Banking Standards shall belong to the legal entity responsible for the Open Banking Standard (see Chapter 7d: Governance).

The treatment of IP (such as codes, software, reference data, etc.) should be according to the principles of open access and the nature of the Open Banking Standard as a public good. The objective of this shall be to ensure a regime that assures the availability in the public domain, without limit on use or redistribution (for the Open Banking Standard). Any IP rights should be held by, or licensed to the Open Banking Standard. Copyright should be used to the extent possible to promote the free flow or combination of information from disparate sources.

The Open Banking Standard should be designed to ensure that it is not locked in with a particular service provider for any key system functions or processes, and that the principles of competition are ensured on both global and local levels where appropriate. The governance of the standard should provide safeguards to ensure that competition principles and antitrust considerations are upheld.

The steady-state funding of the Open Banking Standard should be self-sustainable and reliable. The funding system should be based on an efficient, non-profit, cost-recovery model. The costs of implementing and sustaining the Open Banking Standard and developer resources (proposed in Chapter 7b) should be sufficiently modest not to act as a barrier to entry.

7a. 11.2 Approach on patents

Reference to patented items within the Open Banking Standard should be avoided. If, in exceptional situations, technical reasons justify such a step, there is no objection in principle to preparing standards that include the use of items covered by patent rights (as defined in the glossary) even if the terms of the standard are such that there are no alternative means of compliance.

If technical reasons justify the preparation of a document in terms that include the use of items covered by patent rights, the originator of the proposal shall draw the attention of the Open Banking Standard's Independent Authority to these patent rights. If the proposal is accepted, the originator shall ask any holder of such identified patent rights for a statement that the holder would be willing to negotiate licences in all of the countries where they have obtained patent protection under their rights with applicants throughout the world on RAND terms and conditions. A record of the right-holder's statement shall be recorded by the Open Banking Standard's Independent Authority. If the right-holder does not provide such a statement the proposal concerned shall not be included.

7a. 11.3 Licences

It is critical that licensing of the Open Banking system presents few legal and technical barriers to adoption, therefore using permissive licences to encourage reuse.

The following recommendations are made:

- Open Banking Standard (copyright): this should be made available under a CC0 licence (effectively public domain) that permits it to be freely used, reused and distributed, or failing that CC-BY (attribution).
- Open data falling under the Open Banking Standard: any licence here would be a barrier to reuse and potentially end up with long "licence chains". Therefore open data should be made available under a CC0 licence (the same licence used by the Global LEI system for its data).
- System software, e.g. core libraries or sandbox (see Chapter 7b: Developer Resources). Many banks will have difficulty in using software that is difficult to integrate with proprietary software; therefore we recommend licensing under a MIT licence.

7a. 12 Ubiquity – Achieving Network Benefits in a Collective Action Setting

7a. 12.1 Regulatory incentive – alignment with PSD2

As discussed elsewhere in this report, the revised Payment Services Directive (PSD2) requires some of the same outcomes as could be delivered via an Open Banking Standard in UK banking. As a result, there is a driver for some aspects of the implementation of an Open Banking Standard.

There is clearly an opportunity to leverage the regulatory drivers of PSD2 to ensure that at least the core elements of standardisation proposed in this report are adopted.

Of course, in terms of competition, the need for ubiquity should not result in standardisation activities that inadvertently lead to exclusion or discrimination against third parties or new technologies. As this work progresses, it will be important to take a collaborative approach which engages with the transposition of PSD2 so that respective policy processes are aligned.

7a. 13 Landscape

A number of existing projects might be looked to in terms of reusing or utilising elements for use in the Open Banking Standard. These are detailed in Appendix 8.

7b. Developer Resources

7b. 1 Chapter Outline

This chapter identifies the developer (third party) resources needed to deliver a compelling developer experience, thereby facilitating developer adoption. It outlines key requirements at each stage of a developer's journey and also provides recommendations to help preserve the developer experience in light of provider API constraints (e.g. limitations on use, costing etc.).

7b. 2 Key Recommendations

7b. 2.1 Developer resources requirements

7b. 2.1.1 Creation of a developer hub

A central developer hub containing reference documents for the API and a reference implementation of the core APIs should be established. It should contain an implementation register, listing API providers that have implemented the Open Banking Standard, specifying their products and versions.

The developer hub is seen as critical in aiding developers in discovery (i.e. understanding the data and services APIs expose) and engagement (i.e. identifying suitable API providers).

7b. 2.1.2 Development of a central sandbox

A central sandbox for the reference core Open Banking API (and product sets) in the developer hub should be provided. It should be implemented at all security levels, contain a set of executable tests that API consumers can use to validate compliance and be provided free of cost to developers.

The central sandbox is seen as a key enabler of developer "play", allowing experimentation with the API in a simulated environment. Its centralisation also accelerates developer adoption in an ecosystem where not all API providers will develop local sandboxes.

7b. 2.2 Methods to preserve the developer experience

KPIs, e.g. the number of calls per second allowed before throttling, maximum response time, etc., should be published by API providers to provide transparency on service/performance constraints.

7b. 3 Purpose

On the assumption that an Open Banking world is in operation, with many provider APIs operating under the Open Banking Standard, this chapter will outline the developer (third party) resources that is required to facilitate discovery, play and engagement from a diverse developer community. It will also outline further areas for consideration relating to developer adoption.

7b. 4 Developer Experience, Incentivising Adoption

7b. 4.1 Motivations

For the Open Banking Standard to be successful, an engaged developer community must be cultivated. Key to this is creating a compelling API developer experience (APX); barriers to participation should be as low as possible.

Developers will fall into distinct profiles that will require tailored APXs. Examples include:

- Hobbyist developers – individuals who are building their own app to run or to gain experience;
- FinTech developers – highly technical developers working in companies of 10-100 who want to experiment very quickly;
- Digital agencies or SI partners – technically adept developers who are building solutions for other companies;
- Corporate clients or large companies – from both financial services and adjacent industries who want to develop their own solutions.

7b. 4.2 Developer journey

In order to create high-quality APX, consideration should be given to the developer journey; understanding requirements across discovery, play and engagement.

7b. 4.2.1 Discovery

Developers need to know what data and services APIs expose. They need to develop an understanding of the data offered and how up to date it is, while forming a view of what the data and functionality provided via the API can be used for. In the instance material on use cases and worked examples are available, the developer will use these to inform of their participation and potential proposition development.

7b. 4.2.2 Play

Developers will want to experiment with the APIs – usually early in the lifecycle of a project. The developer may already have a business case, or may be in the process of determining potential value. Play can be undertaken in different ways, from using reference documentation (i.e. by typing in parameters and looking at sample responses), or experimenting in simulated environments.

7b. 4.2.3 Engagement

Before a developer can use an API in production with real data, they need to find an API provider that has implemented the APIs.

7b. 5 Developer Resources

7b. 5.1 Central developer hub

A central developer hub containing key reference documents and implementation registers should be created to support developers in gaining a practical understanding of the data and services offered from both the Open Banking Standard and specific API providers. This addresses key developer requirements in discovery and engagement (see 7b. 4.2).

Specifically, the developer hub will:

- contain reference documents for the API and a reference implementation of the core APIs;
- provide specifications as a set of executable tests;
- contain an implementation register, listing API providers that have implemented the Open Banking Standard, while also specifying which products and versions of the Open Banking API they have adopted;
- link to API providers that have implemented the Open Banking Standard (and potentially their extensions) and provide information on their implementations;
- hold all historic versions of the core Open Banking API, but implement the most recently approved.

The developer hub should be advertised on developer news and information platforms (e.g. Programmable Web) to increase awareness. It is also proposed that developers register with the hub, primarily so that notifications of change can be effectively disseminated.

7b. 5.2 Central sandbox

7b. 5.2.1 Recommendation to build a central sandbox

While the developer hub will support light aspects of play (through documentation), a more sophisticated and useful tool for developers would be a sandbox, which is a way to make programmatic calls to test the API.

Although API providers will be encouraged to develop local sandboxes, especially in instances where local extensions have been made, it is recognised that costs may present a barrier and further incentives may be required. Therefore we recommend firstly that a central sandbox be established and, secondly, that following work explores creative solutions to local sandbox development (e.g. outsourcing sandbox development to trusted parties).

It should be recognised that the cost to deploy and run the infrastructure to support a central sandbox will not be insignificant and will need to be considered as part of further phases of work.

7b. 5.2.2 Features of a central sandbox

A central sandbox for the reference core Open Banking API (and product sets) in the developer hub (see 7b. 5.1) should be provided. The sandbox should:

- implement all levels of security for APIs (note: Additional registration/identity management may be required to provide developers access to higher levels of security, e.g. two-factor authentication (2FA) (with test accounts/known responses) if required);
- contain a set of executable tests that API developers can use to validate compliance;
- be provided free of cost to developers so barriers to entry are avoided.

For clarity, it should be noted that use of the sandbox does not imply accreditation; (see Chapter 7d: Governance).

7b. 5.3 Examples

1. **Stripe:** an example of documentation pitched at developers is that available from Stripe. Its site allows developers to try the APIs out immediately and gives code examples in several programming languages.
2. **The Open Bank Project:** recently launched an API explorer that has received positive feedback. They let a developer access a dummy bank account making test calls with security to quickly discover value.

7b. 6 Other Considerations

7b. 6.1 Constraints

Developers will want to understand what constraints are imposed by APIs. These could include:

- limitations on use;
- costing, i.e. imposition of a charging model;
- (lack of) data freshness;
- limitations on support provided.

Constraints will vary depending on the API provider, so it is recommended that each provider gives clear information about all constraints.

This information should be provided in the form of Key Performance Indicators (KPIs), e.g. the number of calls per second allowed before throttling, maximum response time, etc. These KPIs should provide clarity on the above constraints. In addition, as a principle API response time should be at least as fast as the equivalent website (if this exists) so API access is not deterred.

Minimum service level agreements (SLAs) will not be imposed as this could present a barrier to entry. Different providers are likely to operate under different SLAs.

7c. Security

7c. 1 Outline

This chapter covers three broad areas.

1. Security aspects of the API specification, including authentication, authorisation, access levels and permission and encryption.
2. Security standards for data attribute providers and third-parties.
3. Security aspects of open data.

7c. 2 Key Recommendations

7c. 2.1 User consent

In the context of data-sharing with a third-party a principle of informed consent should be adopted. The user should clearly understand the authorisation they are being asked to provide, including:

- who they are providing authorisation to;
- what they are providing authorisation for (i.e. what the authorisation will permit the third party to do);
- how long the authorisation will last for.

7c. 2.2 Authentication

The process through which a customer authenticates itself to its data attribute provider (in order to further authorise a third party access) will be a tripartite process and should be designed to minimise digital friction. Specifically:

- data attribute providers and third parties should retain control over authentication method.
- OAuth 2.0 in conjunction with OpenID Connect are recommended as authentication protocols of choice – future work will be needed to specify the precise model.

7c. 2.3 Fraud detection and monitoring

- The API should provide support for out-of-band (OOB[21]) authentication.

[21] Out-of-band (OOB): Out-of-band is activity outside a defined telecommunications frequency band, or, metaphorically, outside some other kind of activity.

- Data Attribute Providers should be required to notify the user asynchronously/OOB when significant actions have occurred (e.g. a change to a payee).
- The API response should inform the third party that an OOB process is underway so that, where appropriate, they can inform the customer.
- The practicality of including fraud-relevant information (e.g. IP addresses) in the API return message from the third party should be assessed in future work.

7c. 2.4 Authorisation

Once a customer has authenticated with their data attribute provider tokens should be used to ensure the third party is acting within the bounds of the permissions granted. The third-party service should provide evidence that it is entitled to use the authorisation token (e.g. by way of providing a client ID and client secret) to the data attribute provider Each data attribute provider will be responsible for issuing its own tokens and ensuring third parties are in possession of legitimate tokens.

- Permissions: access granted to third-party providers should be defined in terms of specific permissions to data and/or functionality. To reflect the potential risks from malicious misuse of permissions and protect consumers' interests, the following are recommended:
    - Granting users and, in certain instances the data attribute provider revocation rights;
    - Requiring data attribute providers to establish a mechanism through which users can review and cancel their permissions;
    - Assigning risk levels to permissions;
    - Allowing for prohibitions on granting permissions;
    - Placing contextual limits on permissions where appropriate (e.g. payment limits);
    - Subjecting permissions to time/duration limits.
- Roles: a set of permissions and roles should be defined with a standardised nomenclature in future work.
- Encryption: API connections and data in transit should be encrypted using TLS v1.2 as a minimum.
- Certification: should be used to coordinate the management and issuing of digital certificates with a whitelist of approved companies.
- Security standards: it is suggested to use the Cheque Printers Accreditation Scheme (CPAS) as a model, i.e. a security accreditation model based on ISO27001 with a specific minimum threat profile, against which independent auditors can assess the security of data attribute providers and third parties (it may be appropriate to grant a waiver to certain data attribute providers, e.g. banks).

It is recommended that the task of defining a threat profile relevant to the open banking environment be carried out by a body that includes relevant professional individuals and wider representative stakeholders with experience of the financial sector and the threats the third parties and data attribute providers are likely to face. A control framework should be implemented to address the risk profile to set a reasonable industry standard security control. This should be done in such a way that allows flexibility for future threats and technical flexibility to allow innovation in implementation of the controls.

7c. 4 Risks

The growing threat from cyber-criminals means that the adoption of the Open Banking API brings with it significant security challenges. Banks have traditionally protected their clients' accounts and information within a clearly defined and tightly controlled environment. Allowing customers to grant third parties access to their data will expand the security perimeter beyond the data attribute providers' control, and introduce new risks. Responsibility for protecting clients' data will be shared by third parties.

The design of the Open Banking Standard must take account of this new security paradigm and address the risks it brings.

7c. 4.1 Open Banking API as a new attack vector

As a new technology and method of gaining access to customer data, it is likely that cyber-criminals will specifically focus on the open API as a new attack vector. The ability to amend or make payments will be a specific driver. Attacks are likely to include both exploiting any technical weaknesses that may exist in implementations of the open API, supporting applications and services, or through social engineering of customers who will be unfamiliar with the API process. Details obtained may be leveraged to effect an account takeover or commit fraud through other channels. The rollout of the Open Banking API may also provide opportunities for bad actors to exploit customers' naiveté or lack of familiarity with the processes surrounding the API to conduct phishing or social engineering attacks (e.g. criminals could attempt to create fake apps or services, or prompt customers to provide authority to a third party but not actually read the requests properly, just simply approve whatever has been requested in order to let the app or service work).

7c. 4.2 Aggregation of data at third parties

Third parties that collate and store data on behalf of customers are likely to become a primary target for criminals. A popular "main player" in this area could potentially hold a significant amount of customer data, across multiple data attribute providers. Compromising this single entity could be easier and more lucrative than attacking multiple data attribute providers.

7c. 4.3 Intermediary third parties

In the event that third parties are permitted to act as intermediaries for other third parties, there is the risk that data may be passed on to third parties that do not have appropriate security measures in place. Special consideration should be given to this scenario and clear policies should be put in place to govern and restrict how data obtained by the primary third party is passed to secondary third parties, and define what vetting requirements and security standards secondary third parties will be subject to.

7c. 4.4 Compromise of customer devices

Customer devices) such as personal computers, laptops, tablets and smartphones are commonly targeted by cyber-criminals, and have been shown to be highly susceptible to compromise. As a result, any data or credentials (e.g. access tokens) that are stored on customer devices are at risk of compromise.

Furthermore, when a customer device is used to access an API), the risk exists that a bad actor that compromises the customer device may be able to access the API by controlling the device remotely, effectively impersonating the user.

The opportunity to mitigate the risk of such attacks is limited. Therefore, the Open Banking API should include measures designed to minimise their impact if and when they do occur.

7c. 4.5 Emerging threats

Not all risks and threats can be anticipated. The security risk landscape will evolve and develop over time as existing security technologies become obsolete and bad actors develop new techniques. New threats may emerge that require rapid, decisive and coordinated action by third parties and data attribute providers.

The Open Banking Standard must be capable of recognising, reacting and adapting to emerging risks and threats. Requirements that third parties and data attribute providers share information on security incidents will facilitate recognition (see section 7c. 11.4: Information sharing and incident handling).

Policies and procedures should be established to support the implementation of changes to the Open Banking Standard at short notice.

7c. 5. Consumer Protection

7c. 5.1 Customer confidence

Customer confidence is built on a number of tangible and intangible elements and security clearly plays an important role Customer confidence in the API ecosystem is likely to be bolstered if it is clear that that third parties and data attribute providers are subject to appropriate security standards and that appropriate protections are in place from a fraud perspective.[22]

Ultimately, for customers, confidence may also link to the question of liability for losses that result from security breaches. This has security implications in that the security measures and standards employed should align with and support the liability model. Further consideration should be given to this topic at the next stage of the Open Banking Standard development.

7c. 5.2 Usability vs. security

It is important to ensure that security measures are put in place to mitigate risks associated with the Open Banking API. However, these should not be so restrictive and/or onerous that they unreasonably reduce the utility, usability and benefits derived from products and services reliant on APIs. The challenge is to balance customer protection with the potential benefits.

A possible benchmark to use for determining whether usability is unreasonably restricted is to compare the functionality offered by the open API with that offered by data attribute providers' existing websites and apps. For example, if, within the scope of the Open Banking API, a data attribute provider's own website and mobile app were to offer significantly more functionality than is available through the API, that would suggest that the API may be unduly restricted. Data attribute providers, and any other institutions, are free to provide additional services on top of the core Open Banking API;

[22] Recent research published by Ipsos MORI and Barclays shows that for customers using API-based products security is important and "consumer protection needs to form a key part of any developments in this area". See http://www.ipsos-mori.com/researchpublications/publications/1769/Open-API-Exploring-the-views-of-consumers-and-small-businesses.aspx

the point here is that restrictive practices (e.g. unnecessarily complex controls) for commonly defined services will be unacceptable.

Balancing usability and security inevitably requires a certain amount of risk acceptance. It is important that consumers are made aware of and understand the risks they may be incurring by making use of a third party's service or app.

7c. 5.3 Informed consent

7c. 5.3.1 Clarity

A core principle of this report is informed consent. This is discussed further in chapter 9, however, the principle of informed consent implies that the customer must be able to clearly understand the authorisation they are being ask to provide, including:

- who they are providing authorisation to;
- what they are providing authorisation for (i.e. what the authorisation will permit thethird party to do);
- how long the authorisation will last for.

If the third party intends to share the customer's information with another party, this must also be made clear and the customer must be given the opportunity to opt out of having their data shared.

Customers must have the ability to review this information before, during and after authorisation has been granted and to revoke any authorisation they have previously granted.

They must also have confidence that their data will not be retained by a third party unnecessarily after authorisation to access it has expired or been revoked. It is the responsibility of each third party and data attribute provider to ensure they are complying with relevant Data Protection Act (DPA).

7c. 5.3.2 Common terminology

The Open Banking Standard must define common terminology for describing the fine-grained permissions defined by the API, as well as any roles that may be granted. Definitions must be simple, concise and easily understood by customers. All parties should adhere to the standard terminology, with any variance highlighted and explained clearly.

Where a data attribute provider extends the functionality of their API beyond the core Open Banking API, care should be taken to ensure that users can distinguish between core and non-core functionality.

Information about the authorisations the customer is being asked to grant, or has granted, to third parties should be presented in clear and simple language (i.e. plain English). A standardised format and lexicon for third parties' terms and conditions governing customer data should form part of the standard.

7c. 6 Fraud Detection/Monitoring

It is anticipated that banks' existing fraud monitoring mechanisms will be utilised to detect fraudulent activity carried out through the APIs. Consideration should be given to mandating the supply of relevant information by third parties to data attribute providers to support risk-profiling activity (e.g. IP address, user agent, customer device characteristics). It is recommended that the Open Banking API allow third parties to supply such information within API messages.

Existing fraud information-sharing mechanisms are expected to be extended into this space (e.g. those provided by Financial Fraud Action UK).

Explicit API functionality to support out of band challenges should be put in place to allow data attribute providers to require an additional level of authentication before an action is authorised (e.g. a new payment). Third parties should also be able to request/trigger re-authentication by the data attribute provider (e.g. in the event that the third party detects suspicious activity that may not be apparent to the data attribute provider).

The API should support the use of one-time transaction authorisation codes that are supplied out of band to be submitted via the API, as well as transactions that must be authorised entirely outside the API. The latter implies that the API must also support the concept of "queued" or "pending" transactions that must be authorised by the customer before the data attribute provider will accept/action them.

We expect that data attribute providers will notify users asynchronously/ out of band (e.g. using SMS or push notifications) in a timely manner when significant actions are carried out via the API (e.g. the granting of permissions to a third party, the instruction of payments by third parties).

7c. 7 Alignment with Existing Standards

7c. 7.1 Existing security standards that can form part of the Open Banking API

As far as is practicable, existing, mature, open security protocols and standards should be leveraged for the Open Banking API. There are a number of obvious candidates for incorporation into the technical Open Banking API specification (e.g. TLS, OAuth and OpenID Connect).

There is also a range of security standards and schemes that should be taken into consideration, both in terms of application to data attribute providers and third parties, and also in terms of how these standards can be enforced. Examples include:

- ISO27000 family of security standards;
- PCI DSS;
- CPAS;
- tScheme.

It is suggested to adopt a security standards approach based on the ISO/IEC 27000 series of standards, with a tiered approach, i.e. the standard the third party is required to meet and the degree of scrutiny to which it is subject should be commensurate with the access the third party seeks to obtain. For lower levels of access (e.g. accessing open data), self-certification may be judged sufficient while high levels may require that the third party's compliance with the relevant standards be independently audited. This is the approach adopted by e.g. PCI DSS.

The servers and infrastructure operated by third parties and data attribute providers must be protected against cyber-attack. Security standards should mandate security controls that are commensurate with the nature of the data and functionality that is provided. At this stage, this report is not broaching details pertaining to appropriate security controls, but it is expected they will include the use of penetration testing, firewalls, intrusion detection systems, hardware security modules, OS patching policies, etc. It is recommended that a specific workstream is established to define the security standards in this area and then to review them at appropriate intervals to ensure that they are kept up to date with emerging threats and technologies.

Existing financial institutions (i.e. future data attribute providers) have built up considerable experience in this area; their input is expected to prove valuable.

The need and extent to include security testing of applications and servers on a timely basis is a topic that should be covered in further detail in future stages of work.

There are a number of other working groups and standards bodies undertaking work that has bearing on, or parallels with the Open Banking API, whose work could be leveraged as appropriate. Peer review is also an important step in the design of security standards. It is recommended that appropriate organisations and individuals be identified and invited to review and comment upon proposals and drafts produced in the process of creating the Open Banking API.

It is also recommended that work towards the Open Banking API be conducted as openly as is practicable and that the public is given the opportunity to review and comment on it informally (e.g. through mailing lists or social media).

7c. 8. Security and Authentication Aspects of the API Specification

7c. 8.1 Authentication

7c. 8.1.1 User experience, process and technical data flow

Within the context of an Open Banking API, there are four authentication scenarios:

- The customer authenticating themselves to an data attribute provider (in order to authorise a third party);
- The customer authenticating themselves to a third party;
- The third party authenticating themselves to an data attribute provider (in order to access a customer's data);
- The third party authenticating themselves to a customer.

Data attribute providers and third parties should own and control the method by which they authenticate their customers.[23] The methods by which a third party authenticates itself to a data attribute provider, and a user may identify a third party, should form part of the Open Banking API specification.

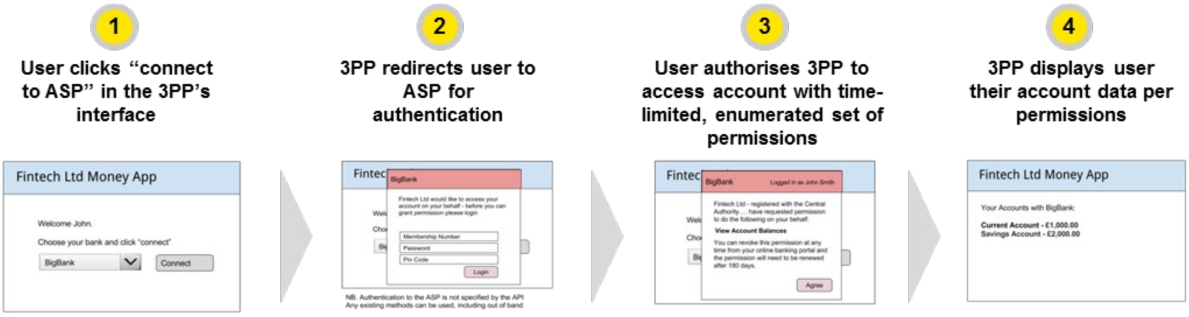
The process by which a customer authenticates themselves to a data attribute provider in order to authorise the granting of permissions to a third party will be a tripartite process, which should be designed in a way that minimises digital friction, to avoid discouraging or confusing customers. It will potentially involve a hand-off of customer interaction from the third party to the data attribute provider for the authentication to be carried out, followed by a redirect of the customer back to the third party from the data attribute provider after the authentication and authorisation interaction process has been completed.

This approach has the benefit of allowing the data attribute provider to continue to own and control the method for authenticating its customers (thereby minimising the risk that a third party could obtain permissions without explicit approval by the customer) and avoids mandating the use of specific authentication methods. Separately, customers will also need to authenticate themselves to third

[23] As previously noted, the EBA has already issued guidelines regarding authentication for internet payments (the Security of internet Payment Guidelines) and further elaboration on these rules in the context of third-party services is expected to support the implementation of PSD2.

parties in order to gain access to the services or functionality being provided. The method used by both data attribute providers and third parties to authenticate customers should be appropriate to adequately protect the data and functionality in question.

Figure 7c.1 Authentication and authorisation: customer experience example (account aggregation)



1 User clicks "connect to ASP" in the 3PP's interface

Fintech Ltd Money App

Welcome John.

Choose your bank and click "connect"

2 3PP redirects user to ASP for authentication

BigBank

Fintech Ltd would like to access your account on your behalf - before you can grant permission please login

NB. Authentication to the ASP is not specified by the API
Any existing methods can be used, including out of band

3 User authorises 3PP to access account with time-limited, enumerated set of permissions

BigBank Logged in as John Smith

Fintech Ltd - registered with the Central Authority.... have requested permission to do the following on your behalf:

View Account Balances

You can revoke this permission at any time from your online banking portal and the permission will need to be renewed after 180 days.

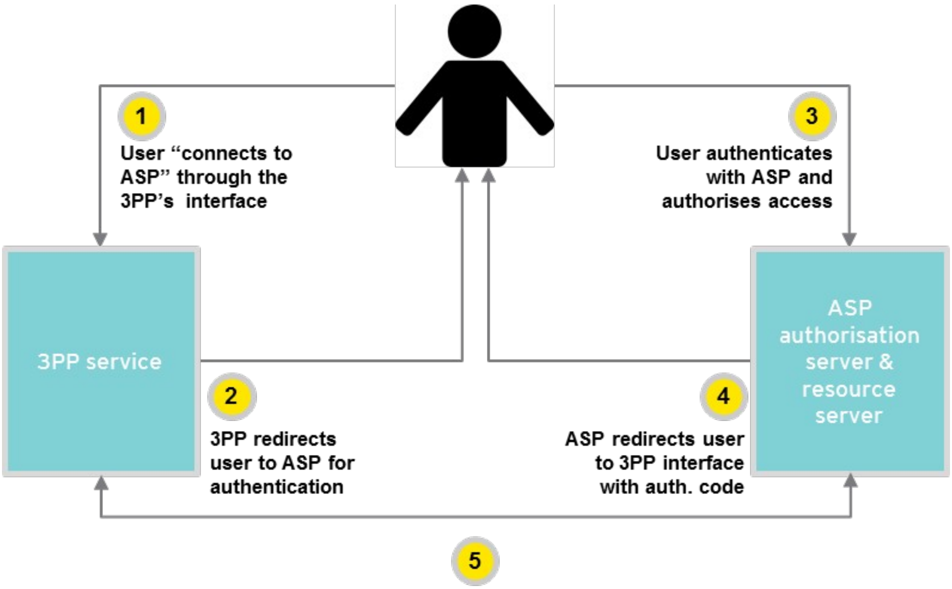
4 3PP displays user their account data per permissions

Fintech Ltd Money App

Your Accounts with BigBank:

Current Account - £1,000.00
Savings Account - £2,000.00

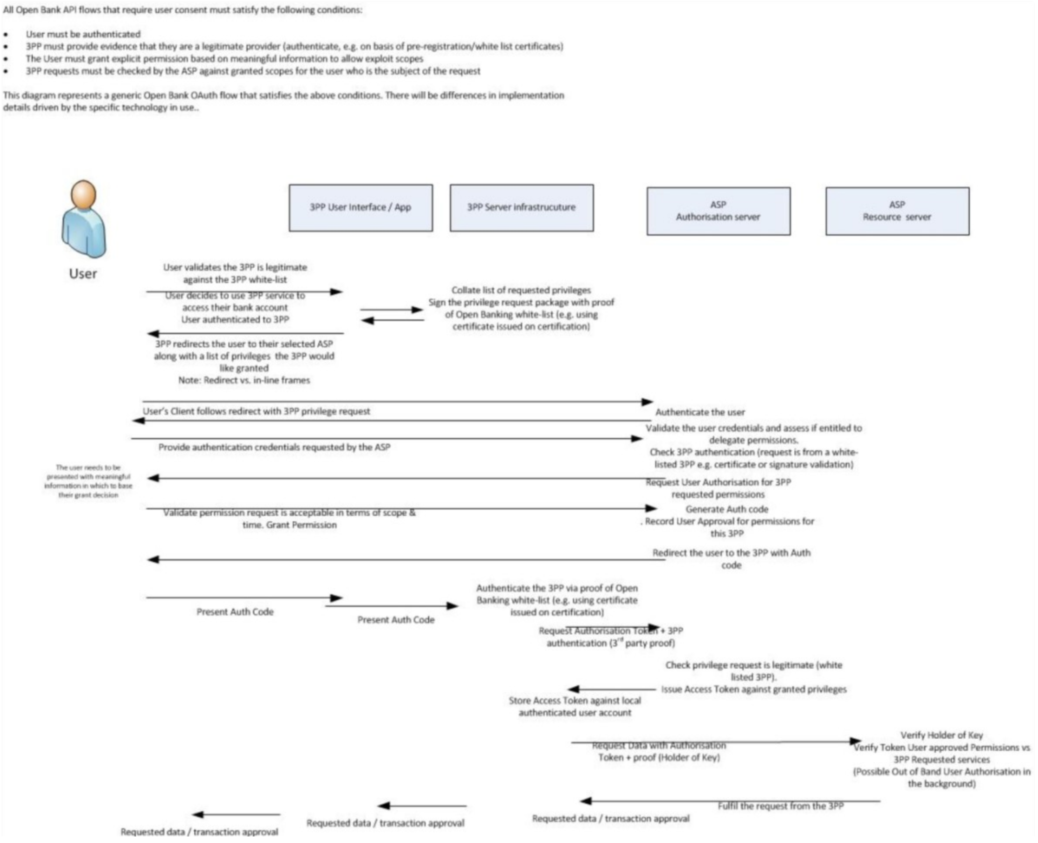
Figure 7c.2 Authentication and authorisation: high-level process flow



1
User "connects to ASP" through the 3PP's interface
3
User authenticates with ASP and authorises access
3PP service
ASP authorisation server & resource server
2
3PP redirects user to ASP for authentication
4
ASP redirects user to 3PP interface with auth. code
5

- 3PP service requests access token from ASP with auth. code
- ASP authenticates 3PP service & issues access token
- 3PP service requests user data with access token
- **ASP verified access token and sends user data**

Figure 7c.3 Authentication and authorisation: technical data flow



All Open Bank API flows that require user consent must satisfy the following conditions:

- User must be authenticated
- 3PP must provide evidence that they are a legitimate provider (authenticate, e.g. on basis of pre-registration/white list certificates)
- The User must grant explicit permission based on meaningful information to allow exploit scopes
- 3PP requests must be checked by the ASP against granted scopes for the user who is the subject of the request

This diagram represents a generic Open Bank OAuth flow that satisfies the above conditions. There will be differences in implementation details driven by the specific technology in use..

User
3PP User Interface / App
3PP Server infrastrucuture
ASP Authorisation server
ASP Resource server
User validates the 3PP is legitimate against the 3PP white-list
User decides to use 3PP service to access their bank account
User authenticated to 3PP
Collate list of requested privileges
Sign the privilege request package with proof of Open Banking white-list (e.g. using certificate issued on certification)
3PP redirects the user to their selected ASP along with a list of privileges the 3PP would like granted
Note: Redirect vs. in-line frames
User's Client follows redirect with 3PP privilege request
Authenticate the user
Provide authentication credentials requested by the ASP
Validate the user credentials and assess if entitled to delegate permissions.
Check 3PP authentication (request is from a white-listed 3PP e.g. certificate or signature validation)
The user needs to be presented with meaningful information in which to base their grant decision
Request User Authorisation for 3PP requested permissions
Validate permission request is acceptable in terms of scope & time. Grant Permission
Generate Auth code
. Record User Approval for permissions for this 3PP
Redirect the user to the 3PP with Auth code
Present Auth Code
Present Auth Code
Authenticate the 3PP via proof of Open Banking white-list (e.g. using certificate issued on certification)
Request Authorisation Token + 3PP authentication (3rd party proof)
Check privilege request is legitimate (white listed 3PP).
Issue Access Token against granted privileges
Store Access Token against local authenticated user account
Request Data with Authorisation Token + proof (Holder of Key)
Verify Holder of Key
Verify Token User approved Permissions vs 3PP Requested services
(Possible Out of Band User Authorisation in the background)
Fulfil the request from the 3PP
Requested data / transaction approval
Requested data / transaction approval
Requested data / transaction approval

7c. 8.1.2 Selection of OAuth 2.0 with future consideration of OpenID Connect

The Fingleton Report recommended the use of the OAuth 2.0 protocol, which supports the tripartite approach outlined in 7c. 8.1.1. This report endorses this recommendation, although further consideration must be given to the specific implementation.

The OAuth 2.0 protocol supports a variety of different interpretations and styles of interaction, with different security implications. The Open Banking API should prescribe how authentication and authorisation aspects of the standard are implemented, so the appropriate levels of consistency, interoperability and security are achieved. It is recommended that the OpenID Connect authentication protocol (which provides an identity layer on top of the OAuth 2.0 protocol) be considered as part of this process. Appendix 6 sets out some considerations pertaining OAuth 1.0 and 2.0 and OpenID Connect.

Having been granted permission to access a customer's account information and act on the customer's behalf, there must be a method whereby the third party can authenticate themselves to the data attribute provider during subsequent interactions. OAuth 2.0 solves this through the use of a token that is provided by the ASP to the third party at the point at which permission to access an account is granted. The third party then presents the token to the each time it wishes to access the account.

7c. 8.1.3 Further considerations

The Open Banking API should define a method by which users can identify any third party they are interacting with, particularly at the point at which they are granting authorisation, for example, using certificates. There must also be a method by which the data attribute provider may verify that a third party is authorised to receive the permissions it is requesting.

7c. 9 Authorisation

7c. 9.1 The authorisation process

The OAuth model as it would apply to the Open Banking API is as follows:

In the course of an interaction with the third party, the customer communicates intent to grant the third party access to account information held by a data attribute provider:

1. The third party requests access to the customer's account information from the data attribute provider;
2. The data attribute provider authenticates the customer;
3. The data attribute provider reviews whether the third party is authorised to receive the access it is requesting;
4. The data attribute provider displays to the customer the access being requested by the third party;
5. The customer reviews the access being requested by the third party and authorises the data attribute provider to grant the requested access to the account information and act on the customer's behalf;
6. The data attribute provider grants the third party the requested access.

Steps 5 and 6 must not involve the third party; doing so would provide opportunities for a bad actor to conceal the extent of the access being requested from the customer.

7c. 9.2 Responsibilities of the data attribute provider

The data attribute provider must allow the customer to review:

- pertinent information about the third party (e.g. the company name, location, what level of authorisation it has received);
- permissions being requested by the third party; and
- duration and validity for which the permissions will be granted.

After the fact, data attribute providers must provide an independent mechanism (i.e. without any third party provided software or service) for customers to review the permissions they have granted and revoke any.

Data attribute providers should also maintain the ability to limit, suspend or revoke a third party's access if they detect suspicious activity or become aware that it is in the customer's best interests to do so (e.g. if a third party has been removed from the whitelist for failure to maintain required security standards).

It is expected that each data attribute provider will issue its own authorisation tokens. Third parties are expected to securely manage tokens relevant to each data attribute provider. data attribute providers in turn, must ensure that the third party is in possession of legitimate authorisation tokens and that the requested data or service relates to the customer's legitimate account (i.e. the right customer is accessing the right account via the right third party at the right time). Data attribute providers must ensure that only valid tokens are accepted and that controls are in place to prevent common attack scenarios such as replay, enumeration, denial of service attacks, etc.

7c. 9.3 Requirements of the Open Banking API

Open Banking API specifications must clearly define the mechanism (e.g. authorisation tokens) by which:

- permissions are granted by the data attribute provider to the third party;
- evidence of authorisation is provided from the third party to the data attribute provider during subsequent API sessions without requiring re-authentication and re-authorisation from the customer (within the time limit of the permissions).

7c. 9.4 Permissions and roles

7c. 9.4.1 Permissions

Defining access by specific permissions

Permissions are the customer's informed consent for a third party to obtain data stored by the data attribute provider (e.g. an account balance or a list of transactions) or to instruct the data attribute provider to carry out some function (e.g. make a payment or suspend a standing order).

The access granted to third parties should be defined in terms of specific permissions to access data or functionality via the API. Permissions should be mapped to one or more API calls so that, given a specific permission (or set of permissions), it is clear to third parties which API calls may be accessed.

Assignment of risk levels

Permissions should be assigned risk levels that reflect the potential impact of malicious misuse of the permission. This applies both to the information being accessed (e.g. sensitive data that could be used for social engineering or identity theft) and the functions being accessed (e.g. setting up new beneficiaries, making high-value payments).

Prohibitions on granting permissions

The Open Banking API should allow for the possibility of prohibiting the granting of permissions unless (a) the third party is authorised to receive them, and (b) the channel through which the API is being accessed is approved for the exercise of the permissions in question. The Open Banking API should define rules governing which permissions may be exercised over which channels. An example of such a rule might be that payments cannot be instructed by software running on a user device that does not make use of a trusted execution environment. Such rules must be enforced by data attribute providers.

Limitations on permissions

Where appropriate, it should be possible to apply contextual limits. For example, it should be possible to limit a permission to a specific number of uses (e.g. make no more than three payments, set up one standing order), or limit any permission that can be used to make or instruct payments from an account to a maximum amount and/or maximum amount/period combinations (e.g. £100 limit per day; £1,000 limit during any 30-day period).

Duration of permissions

Consideration should be given to permissions being subject to a time/duration limit (with a maximum duration of e.g. one year). Each request by a third party for a permission should adhere to the principle of least privilege and be appropriate to the nature of the data or functionality sought (e.g. a transient interaction versus persistent access over a long period). It may be expedient to draft some guidelines that define what is appropriate. The customer must be able to override the duration (if any) requested by the third party, both at the time permission is granted and at any point subsequently.

Permissions and authorisation

The data attribute provider must ensure that no permissions are granted to a third party without first being displayed to and authorised by the customer. The customer must have the opportunity to opt not to grant the third party any or all of the permissions being requested, or to apply relevant limits to any permission (the data attribute provider may opt to apply default limits but these should not be overly restrictive).

Permissions and data protection

In accordance with the data protection principles, third parties should not retain data they have obtained by dint of a permission that has expired (or been withdrawn) for longer than is appropriate.

7c. 9.4.2 Roles

The Open Banking Framework should define a number of common role profiles, under which collections of permissions may be requested by third parties. Common profiles should cover core use cases for specific user types (e.g. accountant, financial adviser, power of attorney). Data attribute providers should provide support for the roles that are appropriate to the type of account the customer holds. This will enhance the usability of the API, by simplifying the mechanism for requesting and granting permissions.

Any divergence from industry norms for the common role permissions must be highlighted explicitly prior to permissions being granted.

7c. 9.4.3 Future consideration of centralised permissions management

The case for creating a central repository of permissions that users have granted to third parties (e.g. an aggregated view of “permissions dashboards”) is unclear at this stage. There are benefits as well as risks.

- Benefit: giving customers a single view of their permissions “dashboard” (the permissions they have granted across multiple organisation).

- Risks: concentrating information for accounts that have profiles attractive to fraudsters in a single repository makes them a high-value target; there may be possible privacy issues; the cost of implementation may be high.

Future phases of work may want to undertake a more detailed evaluation on creating a central permissions repository.

7c. 9.5 Encryption

The Fingleton Report recommended the use of HTTP Strict Transport Security (to ensure that API connections should only be made using HTTPS, thus ensuring that all data in transit is encrypted), and Perfect Forward Secrecy (to minimise the impact if session keys are compromised). This report supports this recommendation and further suggests that the specification mandates the use of TLS v1.2 as a minimum, with a defined set of strong cipher suites.

The case for message-level encryption is less straightforward. Existing bank apps and websites do not use message-level encryption, so mandating its use would go beyond current industry norms. It may also require significant changes to existing technology architecture deployed by many banks. Unless stakeholders (data attribute providers in particular) indicate a strong preference for its inclusion, it is suggested that message-level encryption should not form part of the Open Banking API at this time. However, its inclusion should be considered in the future if the security threat environment changes significantly and/or its use becomes more widespread.

Similarly, the case for including provision for (or mandating the use of) message authentication codes in the Open Banking API should be assessed during the next phase, in consultation with data attribute providers and third parties.

7c. 10. Whitelisting

7c. 10.1 Whitelisting and its limitations

Where access to the' data attribute providers' API occurs from a server end-point controlled by the third party), whitelisting may be enforced through the use of cryptographic certificates, with a high degree of confidence provided by the fact that the secret key is protected by the security surrounding the server (and, optionally, by a hardware security module).

For client-side app use cases, the application software is likely to be running on the customer's hardware, which must be assumed to be insecure. As a result, a cryptographic certificate is not practicable, as the secret key is subject to compromise. To support innovation, further exploration should be made into whether the API specification should allow data attribute providers the option to grant API access to a customer (as opposed to a third party) to use software or a service they have developed themselves.

7c. 10.2 Authentication certification

The use of digital certificates is recommended for third party authentication, and to certify that the third party has been to access customer data via the API.

7c. 10.3 Secure coding

Both third parties and data attribute providers should be required to adopt measures to minimise the risk of security deficiencies in any software they deploy to provide or consume API data. Measures may include adoption of a secure software development lifecycle methodology (e.g. OpenSAMM, Security Development Lifecycle), penetration testing, fuzzing, or source code review. The stringency of the measures required should be commensurate with the nature of the data/functionality being served or consumed.

The case for requiring that testing or review be carried out by independent specialists should be explored further in the next stage of work.

7c. 10.4 Information sharing and incident handling

It should be the responsibility of all participants in the API ecosystem to share any information on fraud security threats. Information-sharing mechanisms may already exist but will need to be expanded to incorporate the wider ecosystem. It is noted that Financial Fraud Action UK (FFA UK) has made proposals to provide a mechanism for firms to share information on security breaches, etc.[24]

[24] In an effort to prevent and/or mitigate payment fraud, FFA UK works very closely with UK banking institutions to facilitate and coordinate eCrime intelligence-sharing among them. In order to avoid any future gaps in the UK's eCrime intelligence picture, FFA UK proposes to incorporate 3PPs into its existing intelligence-sharing mechanism and threat-management process. This would enable 3PPs and banks to share fraud threat and risk intelligence to prevent and/or reduce cases of fraud. These proposals still need ratification.

Data attribute providers should provide a channel for third parties to report any defects or bugs with security implications, adopt formal procedures for acknowledging and investigating such reports, addressing any security vulnerabilities discovered. In addition to existing statutory requirements, it is recommended that third parties and data attribute providers be required to report any security breaches that affect API data or functionality, to both the Independent Authority, and to any customers affected. In the case of a third party suffering a security breach that affects API data obtained from a data attribute provider, the data attribute provider should also be notified.

Protocols should be put in place to facilitate the exchange of information between third parties and data attribute providers in support of investigation of potential fraud or security breaches.

7c. 10.5 Auditing

It is expected that detailed audit logs will need to be maintained by data attribute providers and third parties to facilitate investigations. Further work to define the parameters of these logs will be required in the next phase.

7c. 11. Approach to Open Data

By definition, there is no reason to restrict access to truly open data. Therefore, there is no need to prevent unauthorised access to open data (although there may be a need to restrict access for other reasons, such as preventing denial of service (DOS) attacks). If open data is to be accessed via the same API that provides access to customers' accounts, provision must be made for a level of access that does not require authentication (permission level zero, as opposed to no authentication).

There may be a need to protect the integrity of open data and prevent alteration of open data by bad actors. Therefore, the infrastructure used to provide access to open data should be secured to prevent unauthorised alteration. Authentication of the source of the data may also be required.

Finally, if personal data is anonymised in order to facilitate its publication as open data, care must be taken to ensure that the steps taken to anonymise it preclude de-anonymisation (including through the combination of multiple open data sets). There is more discussion in chapter 9.

7d. Governance

7d. 1 Outline

This chapter further details the scope of governance required to operationalise the Open Banking Standard. It outlines key governance entities required, their roles, responsibilities and activities. It also provides an overview of how these governance entities engage with participants to ensure their obligations are met and how issues that materialise between participants are resolved.

7d. 2 Key Recommendations

7d. 2.1 Creation of an Independent Authority

- An effective governance model will require an Independent Authority with a clear mandate to carry out its duties and sufficient funding to perform those duties effectively.
- The primary role of the Independent Authority would be to ensure standards and obligations between participants are upheld using a risk-based approach. These obligations cover issues such as how customer complaints are handled, how data is secured once shared and the security, reliability and scalability of the APIs provided, as set out elsewhere in this report.
- It would work alongside an industry-led Standards Governing Body, whose primary role would be to set and evolve all standards necessary to the success of the Open Banking Standard.
- No direct contracts would exist between participants; rather, failure to meet the standard and their obligations could result in the Independent Authority sanctioning participants. For third parties this could mean withdrawal of. Further work is needed to determine appropriate sanctions for data attribute providers.

7d. 2.2 Vetting and accreditation

- The Independent Authority should vet third parties and accredit solutions. Obligations will apply to third parties at both an organisational and application level. The approach taken will be proportionate to the risk involved.
- The Independent Authority may choose in the future to authorise other organisations to perform vetting and/or accreditation, including platforms, trade associations or incubators. This would reduce the authority's workload and open up access to the Open Banking API.

7d. 2.3 Insurance

- Third parties would be expected to hold insurance. Consideration should be given to establishing a scheme by which new entrants could pool their risk to remove a potential barrier to entry. The Financial Conduct Authority (FCA) could potentially play a role by bringing forward guidance as to the appropriate levels of insurance required, commensurate with the risk.

7d. 2.4 Issue resolution

- Where customers are affected they should be able to contact either their third party or data attribute provider to initiate this process. Where issues are not resolved within a specific time period, participants can escalate them to the Independent Authority, which will rule on whether standards have been breached. The role of the Financial Ombudsman Service needs to be explored further.

7d. 2.5 Implementation

- The governance entities should be introduced in phases, looking at specific use cases.
- The governance model should cover but not be limited to the provisions of PSD2.
- Further work is required to evaluate costs and funding options.

7d. 3 The Role of the Governance model

7d. 3.1 Why do we need governance?

The introduction and ultimate success of an Open Banking Standard in the UK banking sector will require an effective governance model to be defined and implemented. This will ensure the needs of all participants are adequately and equitably addressed and that trust and confidence in the ecosystem is established and maintained.

Where personal data is involved it is particularly important that all parties understand their rights and obligations in the context of that data. This applies not just at the point of transfer or receipt, but subsequently when that data is retained, reused or even redistributed.

In an ecosystem system based on open APIs – where direct contracts between the supplying and receiving parties do not exist – an effective governance model is required. It is important that this reflects the needs of all participants in an equitable and transparent manner to ensure its ultimate success. Equally important is that the model leverages existing or emerging processes and does not seek to provide for issues that are already dealt with in existing laws and regulations.

7d. 3.2 What would an effective UK governance model cover?

As covered in previous Chapters, in the end-to-end ecosystem there are three key roles.

1. Data providers
2. Third parties
3. Customers

There will be a number of additional participants including e.g. regulators, government, consumer advocacy groups and standards and other expert bodies. Any governance model must be future-proofed to account for the roles of different participants evolving over time.

The governance model will define and oversee the performance of all participants through all phases of engagement. These phases are:

1. Discovery
2. Initial engagement
3. Active engagement
4. Issue resolution

It would also ensure that the physical elements of the ecosystem are effectively established and maintained.

7d 3.3 What would an effective governance model look like?

An effective governance model will require an Independent Authority with a clear mandate to carry out its duties and sufficient funding to perform those duties effectively. The overall role of the Independent Authority would be to ensure the effective set-up and subsequent operation of the ecosystem. It would operate according to the following principles:

- Be independent of third parties and data attribute providers to ensure their and customers' confidence in the ecosystem;
- Act transparently;
- Enable innovation and participation from participants of all sizes;
- Promote the interests of customers in all of its activities;
- Facilitate evolution of the ecosystem in line with new technologies and customer needs;
- Adopt a risk-based approach.

The Independent Authority should:

- Oversee but not define the data, technical and security standards that apply to the ecosystem;
- Oversee but not define the standardisation of open data in the UK banking sector;
- Create a clear process for issue resolution between participants and an escalation and appeal process;
- Establish a process through which interested parties can participate in an advisory capacity to ensure the effective evolution of the ecosystem.

The ecosystem would thus include the following bodies alongside which the independent authority would work:

- A Standards Governing Body, whose primary role would be to set and evolve the data, technical and security standards that would apply to the ecosystem;
- An Appeals Board, where the Authority's decisions could be challenged; and
- A Strategy Forum where a broad range of stakeholders would input into the evolution of the ecosystem as a whole.

The role, responsibilities and composition of all bodies will require further work. It is recognised that there are existing and emerging models, expertise and capabilities across industry, as well as internationally and from other sectors, which could provide useful reference.

There has been some debate about an approach that establishes the independent authority within an existing regulator such as the FCA. Research conducted by Ipsos MORI, mentioned previously in this report, suggests a consumer expectation that regulators would play a key role.

Reporting lines and accountability for the Independent Authority will require clarification.

7d. 5 Membership

Objective criteria to determine membership of each body should be established to ensure there are no challenges of discrimination in terms of who can be a member. A right of appeal against membership decisions should exist. A transparent approach should be taken to publishing all membership decisions, including any complaints about third parties being excluded.

7d. 6 Scope

The work of the Independent Authority and related bodies as set out in this chapter will encompass all activities pertaining to the open banking ecosystem by all participants, as set out above and throughout this document.

7d. 6.1 Legal and regulatory scope

While no direct contracts will exist between participants, non-performance of the obligations defined below will result in the Independent Authority's withdrawal of accreditation and vetting and hence the third parties' ability to use the Open Banking Standard.

The Independent Authority will not seek to address areas where legal provision or regulation already exist but, as detailed below, action may be taken in light of relevant rulings by regulators. However, it is essential that the definition, implementation and oversight of the standards and the operation of the ecosystem must take into account key legal issues.

Should systemic risk be identified, in any form, in the Open Banking Standard or the overall ecosystem, the Independent Authority must have both the mandate and the means by which to take immediate and swift action to minimise that risk.

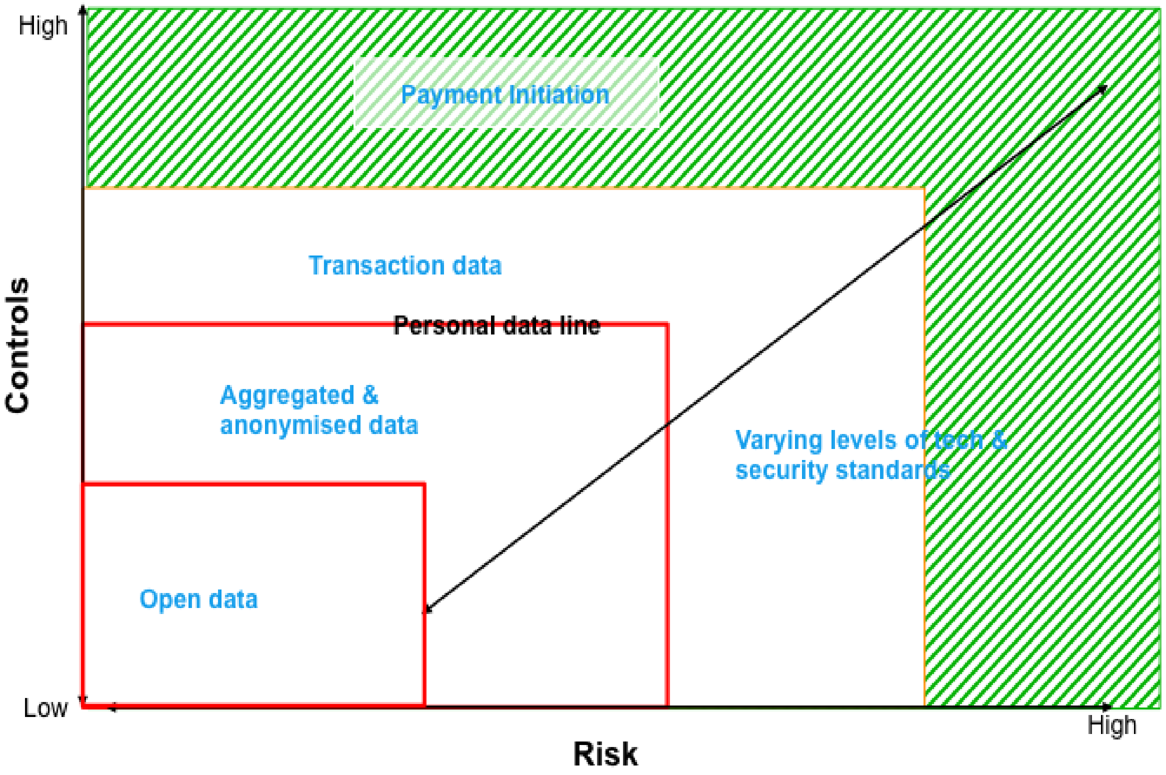
In the context of competition law it is essential that no party discloses or shares its commercially sensitive information with any other. A separate competition law policy will be drawn up. The policy should ensure that:

- access to and participation in standard-setting, including any planning and consultation process, is unrestricted;
- the procedure for adopting the standard is transparent;
- there is no obligation imposed to comply with the standard; and
- the Open Banking Standard will be accessible by all parties on fair RAND terms.

7d. 6.2 Ensuring participants meet their obligations

The Independent Authority should take a risk-based approach to ensuring obligations are being met.

Figure 7d.1 Levels of control



7d. 7 Vetting and Accreditation

In the proposed model, organisations would be vetted and solutions accredited. Underlying standards would apply to each.

As Figure 7d.1 illustrates, the level of controls required increase depending on the level of data access required and hence the risk involved. For example, for certain levels of access, a third party will need to demonstrate how they as an organisation, as well as their solution, protect personal data. They should also be expected to provide certain commitments, e.g. not to "de-aggregate" any anonymised data they receive. The approach the authority takes to ensuring these obligations are being met will vary according to the risk each presents to the customer and will range from requiring self-assessment to regular audits.

Successful vetting and accreditation would result in both a digital certificate against which data providers could validate themselves and a physical certificate (e.g. a kitemark) that could be displayed to customers.

7d. 8 The Role of Platform Providers

Platform providers that aggregate data from multiple sources already play a role in lowering the barriers of entry for third parties that cannot afford to build out connections to data attribute providers independently. They can also embed and enforce standards across the community of third parties assessing their platform. In principle, therefore, platforms could remove significant workload from the Independent Authority because the latter would not have to vet the third parties using its service directly.

The risks associated with platform providers accessing the Open Banking API are greater, however, and therefore the Independent Authority would take a more stringent approach to assessing and monitoring standards in their case. For example, where a platform offered third parties one-time access to a single customer's recent transaction data, that platform would face greater scrutiny than if a third party connected directly.

7d. 9 The Role of Access Organisations

The independent authority could potentially choose to appoint access organisations to take on the role of accrediting third parties against the standards set by the Standards Governing Body according to a process set out by the Independent Authority.

Access organisations could be purely commercial entities, charging third parties for accreditation, or existing operators such as trade associations or incubators that would deliver this service as part of their overall offering. They could also choose to focus on a particular use case for the Open Banking API and only offer accreditation for the level of access that this use case requires. Under this model, potential third parties would in the first instance go to the developer hub for information on the data available and technical specifications of the Open Banking API. If it were required, they would then seek accreditation against the necessary standards from an access organisation. Outsourcing accreditation to access organisations would have a number of benefits:

- It would establish a self-funding model for accreditation.
- It would lead to competition between different accreditation paths, speeding up time to market for data recipients.
- It would allow the independent authority to focus its resources towards areas of greatest risk to the end-customer.

It may take time for appropriate organisations to emerge that could operate as access organisations and therefore it is envisaged that the Independent Authority would retain a role in vetting third parties and accrediting their solutions for the short to medium term.

7d. 10 Obligations Between Participants

Participants must comply with a defined set of obligations through each of the four phases of engagement.

7d 10.1 Discovery

This is the first stage for participants that wish to find out information about the Open Bank Standard and how it might affect them. The Independent Authority will play a central role in ensuring that up to date, relevant and accurate information is provided and that the language used for key terms is consistent and that the information is accessible. Failure by data attribute providers or third parties to provide access to up to date and accurate details to customers could lead to sanctions.

7d 10.2 Initial engagement

This is the stage during which participants wish to find out more detail. For data attribute providers and third parties the additional information and support might include, for example:

- details about the role of the Independent Authority and the role of the other related bodies;
- the technical details of the standards;
- details of the SLAs/obligations between participating data attribute providers and third parties;
- details of the rights of participants;
- details about the costs of participation;
- details of any sanctions that may apply;
- a comprehensive set of FAQs;
- a helpline number, contact details email address and phone numbers for further questions.

For customers, additional information might include, for example, access to:

- how they can identify vetted third parties and accredited solutions (kitemark details);
- details of the type of solution and services that are available and from whom.

The Independent Authority will play a key role in providing access to relevant information and support for all participants. This includes but is not limited to:

- accreditation and vetting submissions from third parties, ensuring that these are handled quickly and effectively;
- queries arising from any participant.

7d 10.3 Active engagement

During this stage participants are actively engaged in the ecosystem. Obligations for data attribute providers include but are not limited to:

- providing third parties with timely and effective responses to legitimate API calls;
- providing third parties with support contact details should queries arise;
- providing customers with the ability to transfer their data to a third party;
- providing customers with support contact details should queries arise.

For third parties, this includes but is not limited to:

- the presentation of clear, fair and transparent terms and conditions to the customer;
- providing customers with support contact details should queries arise.

For customers this includes but is not limited to:

- reading and accepting the terms and conditions presented by the third party for the service/solutions being provided;
- where relevant, and where they wish to, providing their consent to the transfer of their data from the data attribute provider to the third party.

7d 10.4 Issue resolution

The behaviour of data attribute providers and third parties is already regulated by various regimes depending upon the nature of their business. Regardless, the process for customers to receive redress in the context of their engagement with the ecosystem should be as simple and efficient as possible.

The role of the authority should be to:

- provide clear guidance to customers regarding their legal rights;
- mandate that data providers and third parties establish mechanisms to engage each other should issues arise; and
- act as an escalation point if the customer does not feel they have received adequate redress.

Customers should be able to contact their data attribute provider or third parties if they have a complaint. Data attribute providers and third parties should be incentivised to resolve the customer's issue fairly and efficiently. If they fail to do so customers should be able to escalate the issue to the authority, which can take appropriate action.

Third parties or data attribute providers that are found to have failed to meet the required standards, or harmed the customer in some other way, may face action by the Independent Authority. This could include a requirement to alter business practices within a specific time period, providing compensation to customers who have been affected, enhanced vetting or a referral to a competent authority (e.g. the ICO or FCA). In some cases, third parties and data attribute providers may find themselves barred from accessing the ecosystem temporarily or permanently.

Third parties would be expected to hold insurance. As it is envisaged the standard could be implemented ahead of PSD2 coming into full force, the FCA could bring forward guidance on the insurance third parties should be expected to carry. This should be commensurate with the risk different third parties pose to the customer and not present an undue barrier to new entrants.

7d. 12 Funding of the Independent Authority

7d. 12.1 Sources and methods of funding

There will need to be an initial source of funding to cover the start-up costs. Further thought will need to be given as to how to raise these funds. However, it is probably important that no one future scheme member (or group of members) is seen to provide significant funding because of potential concerns around undue influence over certification and disputes relative to other members.

Options could include government funding, grant funding, philanthropic donations or industry fees.

It should be an ambition that the Independent Authority and ecosystem are ultimately self-funded. This would normally be achieved through revenue-generating activities such as:

- Certification and/or membership fees;
- Dispute resolution fees;

Further thought will need to be given as to the exact nature and quantum of such costs and how to finance them. Funding governance should not become a barrier to new entrants – either third parties or data attribute providers.

One way of minimising costs, including those related to vetting and accreditation, would be to embed the governance processes into an established body such as those listed below. However, there may be some unique aspects to this ecosystem that dedicated groups or bodies would be required to consider.

There are various accredited bodies that undertake certifications against defined standards. Some of the more significant in the UK include:

- The "Big 4" auditing professional services firms (PWC, Deloitte, EY, KPMG) and other professional services and consulting firms that provide many independent audit, certification and accreditation services.
- UKAS (UK Accreditation Services) – the national accreditation body for the UK, appointed by the government, to assess organisations that provide certification, testing, inspection and calibration services. While primarily focused on providing accreditation to certification providers, it does also perform some certification services itself.
- CESG CTAS (CESG Tailored Assurance Service).

The scope and reach of the final governance and certification requirements will have a substantial impact on the level of costs that will be incurred in setting up and running the ecosystem, as will the number of participants. However, both set-up and ongoing operational costs could be expected to extend into several million pounds.

8. Regulatory and Legal Considerations

8.1 Overview

The Open Banking Standard is affected by a number of existing legal and regulatory requirements, including the Data Protection Act (DPA), competition law, IP and the Payment Services Directive (PSD). These requirements are also evolving with PSD2 and GDPR, which will need to be implemented in the UK over the next two to three years.

Given the intentionally very wide scope of data and services potentially within scope, this chapter identifies a range of issues, not addressed elsewhere in this report, that should be considered and, where practicable, proposes potential solutions that will help ensure that the Open Banking Standard is implemented in a legally compliant way, enhancing trust by customers, third parties and data attribute providers.

8.2 Key Recommendations

- The Open Banking Standard should be designed taking into account GDPR and PSD2 principles and reviewed once the respective rules are finalised.
- The sponsor of the Open Banking Framework should work with government and regulatory bodies to ensure that the implementation of domestic legislation considers the effective implementation of this initiative (and vice versa).
- Further consideration is required by government as to whether the Open Banking Standard proposed provides adequate customer protection to determine whether regulation of participants beyond existing requirements is necessary.
- Further consideration should be given as to whether the Open Banking Standard requires third parties to disclose to the customer whether they are regulated and the complaint procedure (including any alternative dispute resolution service or lack thereof).
- The Open Banking Standard will need to cater for, and reflect, the respective IP rights of participating parties, including:
    - in developing the standard;
    - in relation to the licensing arrangements between data attribute providers and third parties, and terms of use in relation to the API; and
    - determining appropriate sanctions if a party does not comply with the conditions of the licence or terms of use.
- Parties continue to have a responsibility to ensure they comply with third-party IP rights.

- The Open Banking Standard develops minimum clear standards for what consent to sharing of data might look like.
- Consideration will also need to be given as to how the process will cater for fair processing notices as part of the consent process.
- Further work is required to consider how the Open Banking Standards caters for:
  - more than one signatory on an account, e.g. joint accounts or corporate accounts;
  - different access permissions on the underlying account, which can be common for corporate accounts where there may be limits on the types of amounts of payments that can be made by particular signatories.
- The API should provide sufficiently granular control in terms of the data third parties are able to obtain to mitigate the silent party risks, as it will be practically difficult to obtain consent from parties whose personal data is included in the customer's transactional information.
- Beyond this, as part of the implementation of the Open Banking Standard, a focused working group should develop a standardised approach to the measures outlined above:
  - providing adequate assurance to all parties that privacy risks will be sufficiently addressed;
  - minimising impact on potential use cases; and
  - accommodating relevant requirements under emerging final PSD2 and GDPR texts.
- Third parties should be directed to relevant ICO guidance to assist with compliance.
- Each time anonymised data sets are added to the scope of the Open Banking Standard, a standardised approach to anonymisation should be imposed to minimise risks of de-anonymisation. The risk of data misuse can be mitigated by putting in place appropriate sanctions such as temporary or permanent bans from API access for third parties that fail to comply with their DPA or other legal obligations. This provides an added incentive to treat data appropriately.
- Data requests from third parties to data attribute providers should make clear from which country the request is coming.
- Further work is required to confirm how the Open Banking Framework will apply to third parties based outside of the European Economic Area (EEA) (or transferring data outside of the EEA) given DPA requirements, in particular in relation to European Commission adequacy decisions or the requirement for model contracts. The utility of standardised controller-processor agreements should be investigated. This could involve the use of standard contractual clauses approved by the European Commission.
- There is an opportunity to work with the EBA to maximise consistency between the regulatory technical standards and the Open Banking Standards – such discussion may be best led by HM Treasury.

8.3 Forthcoming Regulatory Changes

8.3.1 The draft European General Data Protection Regulation (GDPR)

The GDPR will make wide-ranging changes to the data protection legal landscape in the UK and across the EU. The GDPR has been the subject of intense debate and controversy since the original draft was published in 2012. The GDPR was finalised in 2015, with an implementation period likely to be two years. There is more information on the key changes relevant to the development of the Open Banking Framework in Appendix 3; however, this is neither exhaustive nor certain, as at the time of writing the text was not yet finalised.

8.3.2 Revised Payment Services Directive

PSD2 will need to be implemented in member states from January 2018. The timeframe for implementation is staggered, as the EBA will have responsibility for producing further standards and guidance in respect of some of the requirements.

PSD2 will for the first time regulate payment initiation services and account information services. It will also set out requirements for parties involved in a payment to securely authenticate and communicate with each other. As such, this report takes into account known principles when developing recommendations. An overview and the detailed requirements relevant to the Open Banking Framework can be found in Appendix 1. However, there is still much detail to be finalised during implementation.

Third parties providing services under PSD2 will need to be registered payment service providers and therefore supervised by the FCA. PSD2 also sets out the respective requirements and obligations of the data attribute provider, third party and the customer, including the ability for customers to make a complaint to an alternative dispute resolution service (the Financial Ombudsman Service).

The Open Banking Standard, however, could be used for products outside the scope of PSD2 or other use cases that may not be subject to this regime. A policy decision is necessary as to whether any potential customer confusion or detriment means third parties using the Open Banking Standard should be regulated in a similar way.

8.4 Design of the Framework

8.4.1 Designing for competition

While the Fingleton Report recommendations were largely intended to increase competition and innovation in the banking sector, complying with competition law is also relevant to the design of the Open Banking Framework.

The Competition Act 1998, which corresponds with EU law principles, prohibits:

1. Agreements between undertakings, decisions by associations of undertakings or concerted practices that may affect trade within the UK and have as their object or effect the prevention, restriction or distortion of competition within the UK. This prohibition covers the exchange of commercially sensitive information between competitors.

2. The abuse of a dominant market position that has or is capable of having an effect on trade within the UK.

Any new Open Banking Standard must ensure that no commercially sensitive information is shared between competitors and not create unnecessary barriers to entry.

Competition law will need to be taken into consideration when setting the Open Banking Standard and ensure that:

- participation in standard-setting is unrestricted;

- the procedure for adopting the standard in question is transparent;

- there is no obligation to use the standard, although if a party chooses to do so, they also agree to comply with it; and
- provide access to the standard on fair, RAND terms.

These principles have been applied in the recommendations throughout this report and will need to be borne in mind as the framework develops.

8.4.2 Protecting IP rights

IP rights may arise in relation to existing data sets provided by data attribute providers or new datasets created as a result of the Open Banking API. These fall into three broad categories:

1. Database rights and copyright in the databases themselves;
2. Patented processes or trade secrets used to create/process/analyse the data;
3. Trademarks related to data attribute providers' or third parties' branding.

Chapter 7a: Standards proposes a mechanism for ensuring that IP rights are considered in the development of the standards and are licensed appropriately. The IP issues in relation to the development of the API and the standards, as well as the licensing of the data, are complex and will need to be considered in more detail.

For the proposed API to operate effectively, wide use of the data must be permitted. This is likely to be subject to a set of conditions contained in a licence and underpinned by terms of use for the API. The terms of the licence will need to be developed with the standards.

The design of the Open Banking Standard will also need to cater for the IP and other rights that are held by different parties and that will arise in relation to the programme and the various use cases. This is to ensure that those rights are not inappropriately devalued or breached, which may give rise to liability or reduce the incentive for parties to innovate.

Similarly, any party contributing to or accessing the Open Banking API will need to ensure that they are acting in accordance with any third-party rights and that an appropriate licence or contractual arrangement in place, where relevant. For example, if data is to be consumed/aggregated/analysed by third parties, then any presentation of that data must not make a claim to ownership of that data, or suggest that it cannot be obtained for free.

It is likely that a third party would seek to exclude liability for the factual accuracy of any input data. The extent to which a third party might be liable would depend on whether new data was created from it, but it will be in both the data attribute provider and third parties' interests to ensure that the data is presented correct "as at" a certain date. Liability in relation to content or accuracy of data is more likely to become an issue where data is no longer correct as a result of being out of date.

8.4.3 Catering for customer information

The Open Banking Standard is intended to apply to both open data and customer data. There are further significant legal considerations where customer data, and in particular personal data, is involved. For example:

- The DPA requires the processing of personal data, i.e. data relating to an identifiable individual, must be fair and lawful, that it must be transferred with adequate protection and information must be kept secure. Personal data collected must not be excessive given the purposes of the processing, must remain accurate and up to date, and be processed in line with the rights of the individual.

- Banks may have a common law duty of confidentiality to their customers. This will apply to consumers and corporate customers.

- Obligations arise under the Financial Services Regulatory Regime, including the Financial Services and Markets Act 2000 and FCA/PRA Handbook(s) such as SYSC 3.2.6(R) – Information Security Requirements, the Electronic Money Regulations 2011 (EMR) and the Payments Services Regulations 2009 (PSRs).

- The UK ICO published guidance (non-binding, except to the extent that legal requirements are described).

Below are some of the key issues that will need to be considered further as the Open Banking Standard develops.

8.4.3.1 Should the framework differentiate between individuals and businesses that are in scope?

This report's recommendations do not differentiate between individuals and businesses. Although the DPA does not apply to legal entities, in England banks have a common law duty of confidentiality to their customers, including corporate customers. While it has not been established in case law that this duty applies to other payment service providers (e.g. electronic money institutions and payment institutions), nor that it applies in Scotland, it is common practice to apply this principle to protect customers' financial information.

In addition, the PSRs apply the same security obligations to both consumers and SMEs. These will be extended further by PSD2 in respect of information services and initiation services. This report recommends applying the same standards to both individual and business customers.

8.4.3.2 When can customer information be disclosed?

The customer's explicit consent to the transfer of information between a data attribute provider and a third party is a core principle underpinning the Open Banking Standard. This is for a number of reasons:

- DPA obligations;

- proposed PSD2 requirements; and

- ensuring the data attribute provider has authority to share the information under its mandate.

DPA obligations

There are two key actors under the DPA: a data controller, who is the person that determines the purposes for which and the manner in which any personal data are or will be processed, and who is responsible for compliance with the DPA; and a data processor, who is a person who processes data on behalf of a data controller. The analysis in this report assumes that both the data attribute provider and the third party, once it receives customer personal data, will be considered data controllers under the DPA. However, this will require further consideration as the Open Banking Standard develops.

Under the DPA, a data controller must rely on the following grounds to process personal data:

- consent – which is specific, informed and freely given;

- compliance with a legal obligation, e.g. which may be relevant to services within scope for PSD2 and potentially data portability requirements under the GDPR;

- necessary to pursue legitimate interests, provided that the processing is not unwarranted due to a prejudicial effect on the rights, freedoms, or legitimate interest of the individual.

Where sensitive personal data (broadly, data relating to race, ethnicity, criminal offences, health, political opinions, or religious beliefs) is to be processed, the data controller must have the explicit consent of the customer, such as ticking a clearly labelled box on an online form. Explicit consent cannot be inferred from data subject actions. The pursuit of legitimate interests is not available as a basis for this processing under the DPA.

Given the wide range of personal data that may be transferred using the API, the framework currently caters for explicit consent. The DPA also requires in most cases that the data subject be given a "fair processing notice" or "privacy notice" that broadly sets out who the data controller is, how the data will be processed and for what purpose.

For third parties, this requires consideration but should be relatively straightforward. In contrast, for the data attribute provider there are some challenges as they do not control what the third party will do with the data, making the provision of an accurate fair processing notice difficult. A pragmatic solution (see Chapter 7c: Security) could be for the third party to include in its data request an explanation of:

- the data sought;
- the purpose of the data processing;
- the identity of the third party;
- confirmation that the data subject has consented to this processing.

The data attribute provider could then provide a fair processing notice and request customer consent on the above basis. This information is also likely to be required under PSD2 for in-scope accounts.

PSD2

Under PSD2, it will be necessary for third parties to obtain explicit consent from customers to provide initiation or information services. This will need to be communicated to the data attribute provider, who will also need to ensure that the third parties' customer is authorised to give instructions on the account.

Mandate

The data attribute provider will need to ensure that the customer is authorised to give the data attribute provider instructions in relation to the account for which information has been requested.

Liability

An appropriate consent process functions less as a model to transfer liability, but to clarify the rights and responsibilities. This places some of the responsibility on the customer to ensure they knew what services they were using, and also places responsibilities on the third parties to process data correctly.

Where customers grant consent for the use of their data, provided that consent is in a format easily understood and verifiable by the all parties, there should be no ambiguity under law as to what data was supplied and what it was to be used for.

8.4.3.3 Transfer of 'silent party information

When X receives a payment from Y, a record of that payment, which may include a name, account details and a reference, is recorded in X's financial transaction data by the relevant financial institution. This is not unexpected and is the status quo for transactions that are happening all of the time. However, this information is the personal data of Y, who will not have consented to processing by third parties (the "silent party").

Where a silent party's data is included in the financial transaction data, the third party subsequently processing it needs an appropriate legal basis for that processing. As outlined above, lack of consent does not prevent processing per se; other legal grounds for processing exist, in particular:

- Where sharing the data is necessary to comply with a legal obligation, this can be grounds for the processing. For transfers required under PSD2, this could be an available legal basis.
- Where the transfer is not required by PSD2, the "legitimate interests" basis for processing can be used, provided the processing does not have a prejudicial effect on the rights and freedoms, or legitimate interests, of the individual (i.e. of the silent party data subject).

Beyond having a legal basis for processing this third-party data, controllers must also meet the other requirements of the DPA, notably around fairness. As with consent, providing a fair processing notice to silent party data subjects would probably not be practicable, as neither the third party nor the data attribute provider would have a ready means to make contact. The DPA provides an exemption for situations where providing the fair processing notice would involve disproportionate effort, but controllers should still take steps to ensure that this data is not used in inappropriate ways that the third party might not reasonably expect.

When considering whether the third party has met the legitimate interests condition, the ICO would consider:

1. Whether the third party has requested only information it needs. Following discussion with the ICO, it is recommended that the API should be built in such a way which allows for the transfer of only those categories of data required (akin to permissions found on mobile operating systems – a flashlight app shouldn't need access to geolocation services, for example).
2. What has been done with the data and whether it was being used in ways that could adversely affect the unconnected third party, for example if data about the unconnected third party was being used for marketing or determining differential pricing.

There are likely to be additional challenges where the silent party's personal data amounts to "sensitive personal data", e.g. a payment from the data subject to a silent party individual includes a reference that suggests a medical condition or membership of a political party. Similarly, where the customer is (for example) a trade union or medical centre, its transaction history would be likely to contain sensitive data of members/customers.

Midata

This issue was considered as part of the PCA midata initiative and resolved by redacting or partly redacting the descriptor field in some transactions to minimise the risk for silent party data appearing.

The PCA midata initiative had the specific objective of enabling consumer comparison of PCA options and the redactions agreed were designed to have minimal impact on this use case. Replicating this approach would be the surest way to address the silent party risk but the Open Banking initiative has a wider objective than midata, and some of the use cases outlined in this report might require unredacted descriptor fields in order to function. For example, small business accounting packages may use the silent party data in descriptor fields to reconcile transactions in order into their books.

Another relevant difference between midata and the Open Banking initiative is that midata allowed users to download their transaction history and then send it to anyone. In contrast, under the Open Banking Standard, data would be shared by more secure channels directly between the data attribute provider and athird party vetted by the Independent Authority. This reduces risks of third party misuse of personal data and of inadequatethird party data security.

At a minimum, a balance is needed between privacy concerns and ensuring data-sharing is sufficient to enable the provision of useful services.

Alternative solutions

Both third parties and data providers need to be able to comply with their obligations and manage their risks. Following discussion with the ICO, the report believes that forthird parties this is likely to involve:

- Careful selection of data to ensure only that necessary for the service is requested from data attribute providers.

- Not processing the personal data of silent party individuals in ways that could be seen as unfair, or outside of the reasonable expectations of these silent parties (for example, a third party accounting system provider using these silent party individual data to reconcile customers' financial records would probably be reasonable, but using it to prepare a direct marketing list or to profile the silent party individuals would probably not be).

Data attribute providers also need to manage their risk. Where a data attribute provider shares a silent party individual's data with a third party, and that third party uses it inappropriately, there is a risk that this third-party individual could take action against the data provider for having shared the data without acquiring consent. Given that data providers cannot control the processing done by third parties, this legal risk carried by data providers must be managed by other means.

Insofar as PSD2 requires the data provider to transfer the data to the third party, this could provide an alternative legitimate basis for the transfer and should protect the data provider to an extent. However, not all services provided, or all accounts accessed using the Open Banking API may be in scope for PSD2. Where the transfer is not required under PSD2 (or other legal requirements) other options must be used. Several options are available.

- Ensure the API allows for requests of precise data points so as to minimise the sharing of data not required for the third party's service.

- Targeted redactions should be considered where data fields are likely to involve silent party individuals' data, especially sensitive data. However, not all IT systems will be able to redact data at a granular level, so this kind of mitigation would need to be implementable in practice.

- Terms and conditions – account providers may need to consider updating their T&Cs to reflect data processing under the Open Banking Standard.

- Guidance on appropriate usage of silent party individuals' data could be developed to assist third parties to ensure they treat this data appropriately. Existing ICO guidance could be used and further ICO input sought.

- Governance and enforcement – where the ICO takes action against a third party for inappropriately processing the data of silent parties, this should result in appropriate action by the Independent Authority, for example, consideration could be given to a temporary or even permanent ban. This would help reassure data attribute providers that data they share will not be used inappropriately and reinforce customer confidence in the framework.

There are a number of outstanding uncertainties that make it difficult to fully resolve this issue at this time, for example the impact of GDPR and PSD2 is still to be understood. The above potential measures will therefore need to be developed further during the implementation of the Open Banking Framework.

Anonymised data

Anonymisation is where personal data is rendered anonymous in such a way that the data subject is no longer identifiable. The ICO draws a distinction between anonymisation techniques used to produce aggregated information, for example, and those – such as pseudonymisation – that produce anonymised data but on an individual-level basis. The latter can present a greater privacy risk, but not necessarily an insurmountable one.

The DPA should not apply where data is genuinely anonymised. However, it is possible in some cases to convert this type of data into personal data by combining it with other data in order to “reverse engineer” the identity of the data subject(s), also known as de-anonymisation.

The general view from the ICO is that a data controller that links various anonymised/aggregated data sets together in order to identify individuals (and thus create personal data) will not be complying with data protection obligations, except in exceptional circumstances. This is because the data is received on the basis that it is anonymous and the data subjects will not have received an appropriate privacy notice. Certainly, it is difficult for them to consent to processing.

Third parties seeking to acquire multiple sets of anonymised data will need to ensure they have measures in place, such as silos and company policies, to ensure that such de-anonymisation does not occur. The ICO’s code of practice on anonymisation will prove a useful resource.

8.5 Arrangements Between Participants

The aim of the Open Banking Framework is to create an open standard without requiring bilateral arrangements between a third party and each data attribute provider. This is also consistent with the principles of PSD2. However, as the framework develops further consideration will need to be given to the areas below.

8.5.1 Services outside PSD2’s scope

The Open Banking Standard should not prevent bilateral contracts, which may still be appropriate depending on the services being provided by the third party. The scope of the Open Banking API assumes that it covers only transfer of the data from the provider to the third party. PSD2 prohibits making relevant data provision conditional on the existence of a contract for initiation and information services relating to in-scope accounts, but the third party may still need or wish to enter into contractual arrangements for related services. For example, where an aggregator site refers customers to a financial institution, a contract for the referral part of the service may be appropriate and indeed required under other legal requirements, for example, where an application for credit may be involved.

8.5.2 Transfers of personal data outside of the EEA

Principle 8 of the DPA states:

> *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

A number of mechanisms are available to ensure that an adequate level of protection is provided. The most commonly relied upon include the use of model contract clauses set by the European Commission, or where the European Commission has declared a jurisdiction has adequate standards of data protection, permitting transfers to that country.

This requirement poses challenges where the third party is outside of the EEA; the data attribute provider cannot legally comply with the data request unless such model contract clauses or a European Commission adequacy decision are in place. Note that the regime for transfers out of the EEA is likely to change materially under the GDPR, although the details are not yet certain.

8.5.3 Agreements facilitating data transfers

Under Principle 7 of the DPA, a contract is needed between any controller and data processor acting on this controller's behalf. This contract must state that the processor will only process in accordance with the controller's instructions, and must meet certain other minimum standards. Where there are any intermediaries in between the data attribute provider and the third party (e.g. network providers), some type of processor agreement will be needed.

8.6 Security

8.6.1 Designing a secure system

Payment Services Providers have a duty under the DPA (Principle 7) and the Financial Services Regulatory Regime (SYSC 3 – banks, Reg. 6(5) EMR - electronic money institutions, and Reg. 6(5) PSR – payment institutions) to ensure data is kept secure and protected from fraud and misuse of personal data.

PSD2 will also introduce obligations between data attribute providers and third parties to authenticate themselves and communicate securely. At the date of this report, the EBA has issued a discussion paper on strong customer authentication and secure communication, in relation to its mandate to develop regulatory technical standards. The security requirements of the Open Banking Standard will need to be further developed as the requirements under PSD2 are finalised.

8.6.1.1 What happens if the third party misuses data or uses it beyond the permission granted?

Under the DPA and pursuant to any duties of confidentiality owed, the information must be used in accordance with the permission granted by the customer. In addition, PSD2 will also place restrictions on the use of data beyond the purposes explicitly agreed to by the customer. This means that if the fair processing notice provided only allows for specific uses, the third party cannot use the data for non-approved purposes without first seeking further consent from the customer.

Once the third party receives the information from the data attribute provider, it is assumed that it will be doing so (where personal data is in scope) as a data controller and therefore will be responsible for ensuring compliance with the DPA. This means the liability for misuse of data sits firmly with the third party.

However, despite this legal reality, the perception of the customer might not consider this subtlety and, indeed, the customer may assume that as the data attribute provider has allowed for data to be sent to the third party, they are still in control of the information and therefore liable should anything go wrong. (And indeed, if the data attribute provider does not have a valid legal basis for the data transfer, it will at law be liable.)

Such misuse or further incompatible uses might comprise profiling of individuals, direct marketing (without consent), selling of customer information to third parties (without consent) and other uses for which the customer will not have provided consent, nor been provided notice. Furthermore, the information gathered by third parties may lead to insights and profiling possibilities that cannot yet be foreseen, giving rise to wider data privacy concerns and the potential to significantly undermine customer trust in the Open Banking Standard.

8.6.1.2 Systemic data breaches

Much of the discussion around open data and an open API naturally focuses on the data within scope. With a proper system of governance and clearly defined roles and responsibilities, it would be possible to achieve a degree of clarity as to how liability flows from the actions of those involved in the chain. If the data is already open, then logically interception presents no legal issues. For anonymised, aggregated, non-personal data; much will depend on the extent to which that data is currently freely available (and is therefore a subset of open data). However, where that data is only provided under an API either to specific individuals or under a contract, then there would be scope for those parties to agree at that time who would be liable in the event of a breach.

Transaction data, whether under PSD2 or otherwise, presents more of a problem; while banks have obligations to refund customers for unauthorised transactions (see below), an API standard introduces a further element of risk and data attribute providers would need to be comfortable in the robustness of the standard in order minimise their credit risk. One option would be to mitigate their risk with insurance. As noted in Chapter 7c: Security, it is likely that cyber-criminals will specifically focus on the open API as a new attack vector. It is impossible to predict how attacks may be carried out, but malware-type attacks constantly present difficulties for banks, in that customers must take some degree of responsibility for the security of their own devices and security details.

DPA breaches might also be problematic. Loss of data resulting from a breach caused by malware might be covered by appropriate customer communications/disclaimers. A systematic non-customer-driven breach (perhaps via a distributed DOS attack) might need to be covered by insurance.

In the event of a data breach (such as hacking), the relevant data controller will be liable and responsible for any reporting. Reporting will also be required under PSD2 if the service is in scope. Each party therefore needs to be clear throughout the process as to its obligations, particularly where it is a data controller. The data controller might not necessarily be clear to the data subject, which could lead to confusion.

8.7 Liability Principles

The sharing of any data naturally gives rise to questions of liability both in relation to the safeguarding of the data and the ultimate use of (and reliance on) that data by all parties involved.

A key element of the establishment (and success) of an Open Banking Standard will be to give any parties touching the data (broadly speaking, data attribute providers, third parties and customers) comfort as to the extent of their liability for controlling, supplying, accessing, processing and ultimately relying on the data. Liability flows from the respective legal rights and obligations of those parties (whether contractual, statutory or under common law), and different data sets may give rise to different rights and obligations.

It follows that at this stage, there is no clear or simple answer to the question “who is liable”, as this will depend on what data is transferred and what use might be made of it. This report has considered these issues at a macro level when looking at data sets and governance, but much will depend on the data sets ultimately within scope and significant further work will be required. However, some broad principles for liability are likely to flow from the purpose and proposed structure of an API framework.

1. Data attribute providers are under broad duties to ensure that information supplied is correct. It is unlikely they would be prepared to accept any specific *contractual* liability, provided that the data they are supplying is factually correct, clear, fair and not misleading, defamatory, or discriminatory, and not infringing on the IP rights of others. Ultimately, data would be provided “as is”.

2. The vetting/accreditation procedure would not seek to alter or transfer liability between the data attribute provider and third parties, but function purely as a way of providing access to the API.

3. Anyone supplying or accessing data already has obligations under existing legal and regulatory frameworks, such as the Data Protection regime. An API Standard would not seek to alter that.

4. Where customers grant consent for the use of their data, provided that consent is in a format easily understood and verifiable by the all parties, there should be no ambiguity under law as to what data was supplied and what it was to be used for. The role of any authority would be to set minimum clear standards for what that consent might look like.
5. This incentivises all parties to ensure that customers understand what their data is to be used for and how it will be accessed, and each organisation must therefore take steps to mitigate any losses they may suffer for their own mishandling of the data (for example, using data outside the scope of their consent, or breaching the provisions of the data protection regime).
6. Where something goes wrong, the customer is unlikely to be concerned with who is to blame. The way access to the API is governed will not change that, but the governance structure could make it clear that the customer could contact either the data attribute provider or third party in the first instance, and it would be up to those parties to resolve the issue themselves. Ultimately, as noted above, liability would flow from existing legal rights and obligations.
7. Insofar as the API is used to provide commercial services, between any or all of the data attribute providers, third parties and customers, it will be the contractual arrangements between the parties that make it clear where liability resides.

The vetting/accreditation procedure would not seek to alter or transfer liability between the data attribute provider and third parties, but function purely as a way of providing access to the API. This would help further the aim of the framework to promote competition and innovation.

However, data attribute providers may feel nervous about exposing large quantities of data to third parties, some of which may not be subject to any existing regulatory framework; while under PSD2, account aggregation and information services would be regulated, there may be many others that are not. Therefore, it is logical for data attribute providers risks to be mitigated and for third parties' risks to be covered by the governance framework making it clear what those accessing the API need to achieve by way of baseline standards, such as data storage and access, and possibly insurance or capitalisation requirements.

8.7.2 Immediate refunds under PSD and PSD2

Under PSD2, in the case of unauthorised transactions the payer is entitled to address a refund claim to the account provider, even where a third party is involved and without prejudice to the allocation of liability between the PSPs. There is a formal obligation on the third party to *"immediately compensate"* the account provider where the latter is liable for an unauthorised payment transaction or a non-executed or defective payment. In both cases the burden of proof is on the initiator.

The proposed governance structure is unable to shift these obligations, but for any services provided that do not fall outside those where a PSD2 refund is obligated, account providers may choose not to provide an immediate refund. This creates a lack of clarity for some customers, where, potentially, services may be a combination of those envisaged under PSD2 and those either not envisaged or expressly excluded. Data attribute providers could choose to extend the immediate refund right at their discretion, but it is difficult to see how it could be mandated without regulatory or legal intervention.

9. Implementation Plan

9.1 Outline

This chapter proposes recommendations on how the Open Banking Standard can be operationalised. The aspiration is to cover the full extent of its scope by Q1 2019 in time for PSD2 (as detailed in Chapter 5: Scope of Data).

Proposals take into account both near-term and medium-term considerations; the former address points for imminent action (i.e. within a six-month horizon) and the latter provides an indicative roadmap to a live and fully operational Open Banking API. Steps should be taken to ensure that the momentum, interest and progress that has been made to date are maintained as future phases of work are initiated.

9.2 Key Recommendations

Near-term deliverables (Q1/Q2 2016)

- Establishment of an “Open Banking Implementation Entity” (OBIE) mandated with planning, designing and delivering future phases of the Open Banking Standard.
- Completion of an industry consultation to source feedback on this report’s recommendations and also views on the design of future phases of work.
- Engaging in dialogue with industry bodies and participating in ongoing consultations pertaining to related industry initiatives (including CMA Retail Banking Market Investigation and PSD2).

Indicative medium-term milestones (H2 2016-2019)

- Launch of a minimum viable product (MVP) – based on open “available” data by Q4 2016.
- Migration of midata onto the Open Banking API by Q1 2017.
- Inclusion of customer transaction data on a read-only basis by Q1 2018.
- Progression towards the Open Banking Standard’s full scope (as per Chapter 5: Scope of Data) by Q1 2019.

9.3 Overview

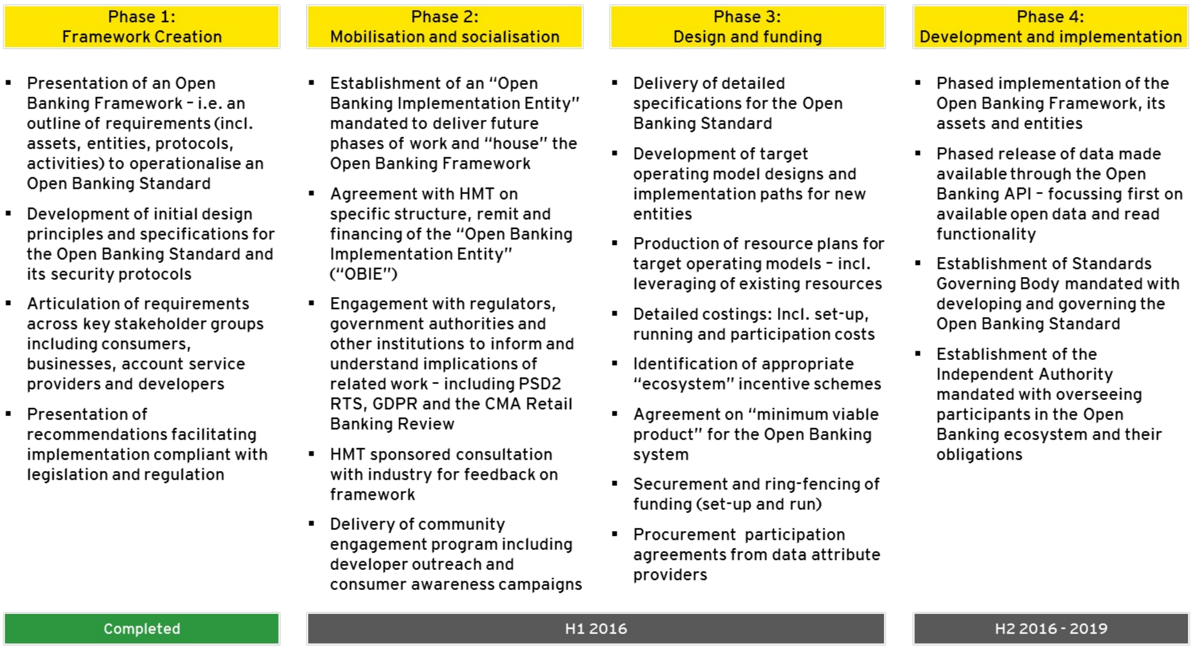
Production of this report completes the first phase of work: delivering a framework from which an Open Banking Standard can be developed, governed and adopted. It outlines key assets, entities, activities and protocols that are needed to facilitate data-sharing across financial services. Assuming

Phase 1 has been completed, it is proposed that subsequent work will be completed across three key phases.

- Phase 2 (Q1 2016) – Mobilisation and socialisation: Establishing an OBIE to take forward the proposals presented in this report and engage in formal consultations and broader community engagement activities.
- Phase 3 (Q2 2016) – Design and funding: Completing a detailed specification for the Open Banking Standard and designing target operating models for new entities. This phase should culminate in the securement of funding and commitments of participation from first-adopter data attribute providers.
- Phase 4 (Q2 2016–2019) – Development and implementation: This is expected to be an iterative process that evolves over time, in terms of both participation and underlying functionality provided by the Open Banking API. A phased approach will be taken to both infrastructure development and data release, with the Open Banking Standard aspiring to reach its full scope by 2019, in time for PSD2.

Figure 9.1 provides details on the phasing.

Figure 9.1 High-level implementation plan



Phase 1: Framework Creation	Phase 2: Mobilisation and socialisation	Phase 3: Design and funding	Phase 4: Development and implementation
▪ Presentation of an Open Banking Framework - i.e. an outline of requirements (incl. assets, entities, protocols, activities) to operationalise an Open Banking Standard ▪ Development of initial design principles and specifications for the Open Banking Standard and its security protocols ▪ Articulation of requirements across key stakeholder groups including consumers, businesses, account service providers and developers ▪ Presentation of recommendations facilitating implementation compliant with legislation and regulation	▪ Establishment of an "Open Banking Implementation Entity" mandated to deliver future phases of work and "house" the Open Banking Framework ▪ Agreement with HMT on specific structure, remit and financing of the "Open Banking Implementation Entity" ("OBIE") ▪ Engagement with regulators, government authorities and other institutions to inform and understand implications of related work - including PSD2 RTS, GDPR and the CMA Retail Banking Review ▪ HMT sponsored consultation with industry for feedback on framework ▪ Delivery of community engagement program including developer outreach and consumer awareness campaigns	▪ Delivery of detailed specifications for the Open Banking Standard ▪ Development of target operating model designs and implementation paths for new entities ▪ Production of resource plans for target operating models - incl. leveraging of existing resources ▪ Detailed costings: Incl. set-up, running and participation costs ▪ Identification of appropriate "ecosystem" incentive schemes ▪ Agreement on "minimum viable product" for the Open Banking system ▪ Securement and ring-fencing of funding (set-up and run) ▪ Procurement participation agreements from data attribute providers	▪ Phased implementation of the Open Banking Framework, its assets and entities ▪ Phased release of data made available through the Open Banking API - focussing first on available open data and read functionality ▪ Establishment of Standards Governing Body mandated with developing and governing the Open Banking Standard ▪ Establishment of the Independent Authority mandated with overseeing participants in the Open Banking ecosystem and their obligations
Completed	H1 2016		H2 2016 - 2019

9.4 Key Actions for Q1 2016

9.4.1 Establishment of an OBIE

An entity should be established and mandated with the primary purpose of planning, designing and delivering future phases of the open banking initiative. This chapter will refer to this body as the Open Banking Implementation Entity (OBIE).

Prior to the creation and operationalisation of the Independent Authority (see Chapter 7d: Governance) the OBIE will "house" the Open Banking Standard and any IP associated with it. The

OBIE will further develop both the framework and its underlying components, with the subsequent piloting and launch of the Open Banking Standard, its associated governance entities and developer resources (under a phased, iterative approach).

The OBIE should seek membership and/or representation from key industry and regulatory bodies, including those from the banking, data and technology sectors. Requirements from future phases of work should contribute to the identification of members and participants needed. This should include adequate participation from regulatory bodies, given the need to comply with ongoing and incoming regulation and the need to launch governance entities to oversee the rights and obligations of those participating. Due consideration should also be given to adjacent industry participation, particularly in light of potential learnings from security practices, and future cross-industry collaboration potential.

Given the significance of its mandate, the OBIE should be appropriately funded and resourced. Initial funding should cover at minimum phases 2 and 3 and ideally with a longer-term time horizon in mind (e.g. two years).

9.4.2 Consultation with industry

Pending feedback from the government and HM Treasury, a formal consultation with the banking industry should commence soon after publication (expected Q1 2016). The consultation will provide a feedback mechanism through which thoughts on this report's recommendations can be logged. It will also give an opportunity to source opinions on how best to take the Open Banking Standard forward. Output from this consultation should be used by the OBIE in planning subsequent phases of work.

9.4.3 Dialogue with industry bodies

Further to industry consultation, steps should be taken by the OBIE – or the co-chairs of the Open Banking Working Group in the interim – to engage with parallel industry, regulatory and governmental studies and initiatives. This includes the CMA's Retail Banking Market Investigation and the PSD2 initiative. Feedback should more broadly be sought from institutions such as the Bank of England, Prudential Regulation Authority, FCA, ICO, EBA and Payment Systems Regulator.

9.4.4 Community engagement

A programme of stakeholder engagement should be established to inform, educate and, in certain cases, mobilise key audiences. These audiences include:

- political stakeholders;
- industry bodies;
- the banking sector;
- the FinTech community;
- consumers and businesses.

A range of engagement mechanisms will be used depending on the audience. These will include events, roundtables, forums and ongoing communication through both the press and other channels. Trade associations are expected to play a key role, either directly supporting in events and programmes and/or assisting in ongoing communications through leveraging their own channels. It would also be beneficial for government to assume a role in future communications, thereby raising awareness of both the Open Banking Standard and the profile of the OBIE once established.

9.5 Indicative Medium-term Timelines

9.5.1 Adopting a phased, iterative approach

A phased approach to implementation is suggested, building out the scope of data and the Open Banking API’s range of functionality over time. Initial phases will deliver a MVP with a more restricted scope and functionality, primarily focusing on available open data (on a read-only basis).

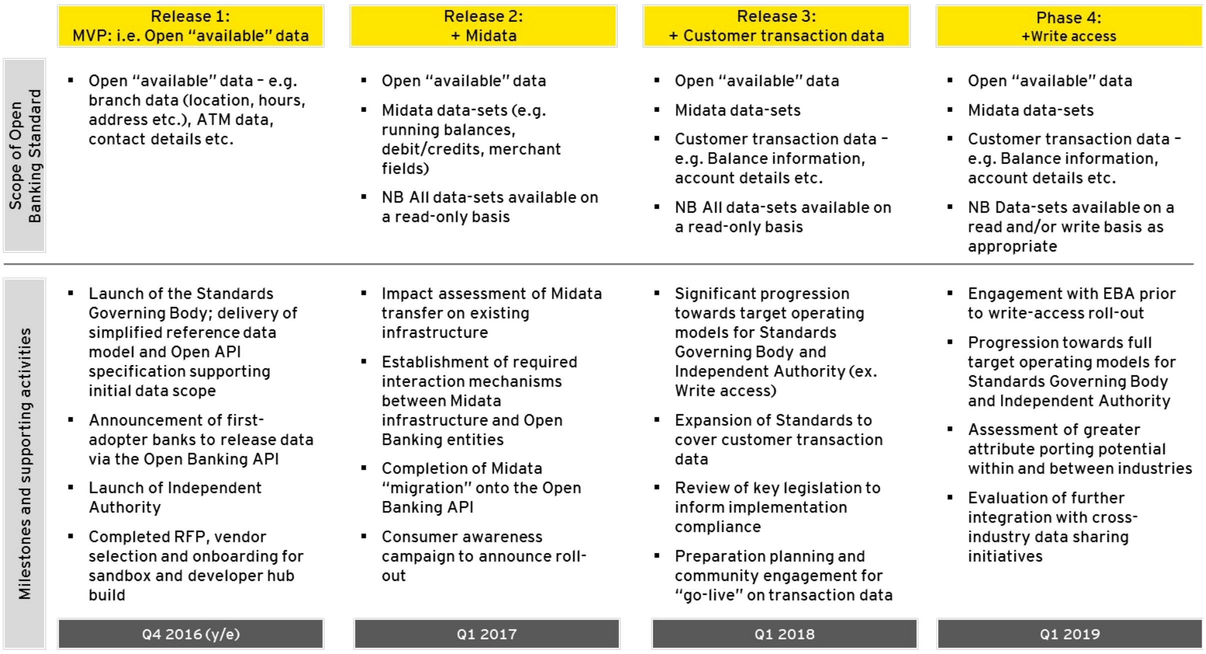
Iterative builds will progressively add functionality and data onto the Open Banking API, factoring in learnings from prior releases. At these junctures, feedback and requests from key participants and user reference groups will be assessed, informing the subsequent phase.

In defining these phases, the following have been taken into account:

- strength of use case(s) associated with the data set;
- current availability of the data;
- implementation ease in making the data available.

Further detail is presented in the indicative release schedule outlined in Figure 9.2.

Figure 9.2 Indicative release schedule (Phase 4: Development and implementation deep-dive)



	Release 1: MVP: i.e. Open “available” data	Release 2: + Midata	Release 3: + Customer transaction data	Phase 4: +Write access
Scope of Open Banking Standard	▪ Open “available” data – e.g. branch data (location, hours, address etc.), ATM data, contact details etc.	▪ Open “available” data ▪ Midata data-sets (e.g. running balances, debit/credits, merchant fields) ▪ NB All data-sets available on a read-only basis	▪ Open “available” data ▪ Midata data-sets ▪ Customer transaction data – e.g. Balance information, account details etc. ▪ NB All data-sets available on a read-only basis	▪ Open “available” data ▪ Midata data-sets ▪ Customer transaction data – e.g. Balance information, account details etc. ▪ NB Data-sets available on a read and/or write basis as appropriate
Milestones and supporting activities	▪ Launch of the Standards Governing Body; delivery of simplified reference data model and Open API specification supporting initial data scope ▪ Announcement of first-adopter banks to release data via the Open Banking API ▪ Launch of Independent Authority ▪ Completed RFP, vendor selection and onboarding for sandbox and developer hub build	▪ Impact assessment of Midata transfer on existing infrastructure ▪ Establishment of required interaction mechanisms between Midata infrastructure and Open Banking entities ▪ Completion of Midata “migration” onto the Open Banking API ▪ Consumer awareness campaign to announce roll-out	▪ Significant progression towards target operating models for Standards Governing Body and Independent Authority (ex. Write access) ▪ Expansion of Standards to cover customer transaction data ▪ Review of key legislation to inform implementation compliance ▪ Preparation planning and community engagement for “go-live” on transaction data	▪ Engagement with EBA prior to write-access roll-out ▪ Progression towards full target operating models for Standards Governing Body and Independent Authority ▪ Assessment of greater attribute porting potential within and between industries ▪ Evaluation of further integration with cross-industry data sharing initiatives
	Q4 2016 (y/e)	Q1 2017	Q1 2018	Q1 2019

9.5.2 Creating a federated ecosystem linked by standards

Progression towards the Open Banking Standard’s full scope will be guided by both the high-level implementation plan presented in this report as well as more detailed plans produced in future phases.

Operationalisation of the standard is expected to proceed on an agile, iterative, adept basis, refining and updating approaches at each phase. This is expected to take into account an expanding range of views and opinions from those participating and those seeking to participate. Ultimately, this approach is viewed as cultivating a federated ecosystem with a multitude of players whose participation will help drive increased interoperability and portability of data.

A rich ecosystem with a range of developers will help to better identify consumer preferences and needs. Therefore innovations and use cases not yet considered or featured in this report (see Chapter 6: Benefits) are likely to surface through the implementation process. These will require refinements to the Open Banking Standard; the implementation approach should retain flexibility to respond to these changes going forward.

Appendices

Appendix 1. PSD2 Overview

1. Background

The first PSD was published in 2007 and transposed into UK law as the Payment Services Regulations in 2009. PSD1 was an important text; it regulated payment services and PSPs throughout the EU and EEA. The directive's purpose was to increase pan-European competition and participation in the payments industry, including the involvement of non-banks, and to provide for a level playing field by harmonising consumer protection and the rights and obligations for PSPs and users.

In line with the review clause in PSD1, the European Commission issued a proposal for a revised Payment Services Directive (PSD2) in July 2013. Publication of the final text in the Official Journal of the EU was due in December 2015, with entry into force 20 days later (i.e. January 2016). Member states are required to transpose PSD2 into national law by, and apply the majority of the provisions from, two years after entry into force of the directive.

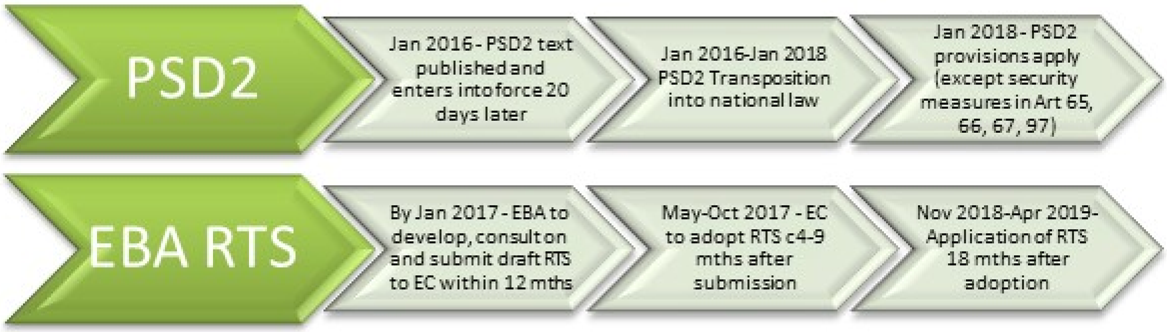
2. Current status and perspectives

2.1 Key facts/changes expected from PSD2

- It is intended to promote the emergence of new players (e.g. FinTechs) and the development of innovative mobile and internet payments in Europe to encourage EU competitiveness worldwide.
- Payers have the right to make use of a payment initiation service provider (PISP) and account information service provider (AISP) where the payment account is accessible online. PISPs and AISPs cannot be required to enter into contractual relationships with account-servicing PSPs (AS PSPs).
- Requirements for strong customer (and also dynamic transaction) authentication.
- Regulatory technical standards on authentication and communication will be defined by the EBA.
- Extension of scope to include one-leg payments and all currencies.
- Access to payment accounts, to address PSPs' ability to open and maintain payment accounts with credit institutions with such access to be on an objective, non-discriminatory and proportionate basis.
- Requirements regarding the management of operational and security risks and incident reporting to be consistent with the approach being adopted under the Network and Information Security Directive, which is still going through the EU legislative process.
- Requirements for AS PSPs to provide a yes or no confirmation of availability of sufficient funds to card-based payment instrument issuers (PIIs).

PSD2 is expected to confer a number of mandates on the EBA, consisting of six technical standards, five guidelines and the development of a register. One of these mandates requires the EBA to develop RTS on strong customer authentication and secure communication channels between account-servicing PSPs and PISPS, AISPs and card-based PIIs, application of which is subject to a separate implementation timeframe from the other PSD2 provisions. The EBA will need to submit the draft RTS to the European Commission within 12 months from entry into force of PSD2. Dependent upon how long it takes the Commission to adopt the RTS (thought to be anywhere between four to nine months, although this is not fixed), the RTS are to be applied 18 months after their adoption and entry into force (current assumption: sometime between November 2018 and April 2019).

Figure A1.1 PSD2 timeframes



PSD2

Jan 2016 - PSD2 text published and enters into force 20 days later

Jan 2016-Jan 2018 PSD2 Transposition into national law

Jan 2018 - PSD2 provisions apply (except security measures in Art 65, 66, 67, 97)

EBA RTS

By Jan 2017 - EBA to develop, consult on and submit draft RTS to EC within 12 mths

May-Oct 2017 - EC to adopt RTS c4-9 mths after submission

Nov 2018-Apr 2019- Application of RTS 18 mths after adoption

3. Political and regulatory path forward

The payments industry in the UK is working closely with the regulators as they prepare for transposition of PSD2. As this report understands it:

- HM Treasury (HMT), which is responsible for transposing PSD2 in the UK, is proposing to engage with a range of stakeholders. This is expected to take place in early 2016.

- In 2016 HMT will continue to work closely with stakeholders, the FCA and the Payment Systems Regulator (PSR) to draft the implementing legislation. At present it is understood that HMT plans to consult on the draft legislation around the end of Q1 2016 with an aim to publish its legislation a year prior to the transposition deadline (i.e. by the end of 2016).

4. Implications for the proposition around an Open API in UK banking

The Fingleton Report did cite PSD2 and recognised that it would lead to market changes. It suggested that taking forward proposals to implement an open API in UK banking would provide:

> "...*an opportunity to get ahead of PSD2... PSD2 may impose similar requirements on banks as some of the recommendations on APIs considered here… As it currently reads, banks would have to allow third parties, via an interface (an API), to initiate payments from bank accounts. That access must be given on the same basis as if to the account owner, i.e., if the owner can initiate a payment at zero cost, then so must a third party, obviously with appropriate consents. Telecom companies, among others, are keen to develop this ability. This has potentially profound consequences for banks, as it may reduce their ability to use current account relationships as gateway products for the sale of other products and services. This could encourage UK banks to consider strategies for addressing these changes at an early stage. It may challenge the behaviour whereby bank account customers often, by default, buy and use other financial services such as loans, mortgages, savings, foreign exchange and even online access from their core account providers. It could facilitate easier access for customers to*

> *competitors who might have keener price points and more innovative or user-friendly functionality. It may also incentivise existing banks to develop and match these innovative features.*"

This report recognises the overlaps between the PSD2 requirements and the proposals as set forth in the Fingleton Report; each of the subgroups has consciously acknowledged any prescriptions already laid down in the near-final text. However, the two proposals do not overlap fully.

- The timelines of the PSD2 proposals and the API proposals do not entirely align. As noted above, PSD2 is running to a regulatory timetable that does not align fully with the timelines as proposed by HMT in its March statement.
- The scope of the two sets of requirements overlaps in some areas but there are also some significant differences. PSD2 was conceived primarily with payment initiation services in mind (write access); the Fingleton proposals are based on the concept of more openness of customer data, albeit with an acknowledgement of write access. These different requirements necessarily result in quite different governance and technical approaches.

As a result of the PSD2 requirements, the EBA will be tasked with developing RTS. These RTS will be legally binding on all PSPs across the EU. They will therefore "trump" anything done at a national level. The EBA's remit will cover aspects including (but not limited to):

1. guidelines on implementing/monitoring of security measures;
2. RTS on strong customer authentication and common and secure communication covering online access to payment account, initiation of electronic payment transaction and exemptions;
3. improving incident reporting throughout the EU (guidelines on classification, content, format and criteria for reporting). Sections (1) and (2) above certainly overlap with areas where this report has made recommendations as regards the framework for an open API in UK banking.

The clear benefit for the open API proposals resulting from their overlap with PSD2 requirements is the opportunity to utilise the regulatory drive created by PSD2 to help to achieve ubiquity and market adoption of, at least the core, elements of the Open Banking proposals. A level of ubiquity is certainly required in order to achieve harmonisation, market momentum, and customer acceptance.

A more detailed analysis of PSD2 as it relates to the key areas that this report has focused on can be found in Chapter 8: Regulatory and Legal Considerations.

5. Considerations for a way forward

As noted earlier, the Open Banking Working Group has worked to ensure that as far as possible an understanding of the PSD2 requirements (which have in part yet to be further defined by the EBA) has been factored into the recommendations on the framework for an Open Banking Standard and open data API in UK banking. For example, the accreditation mechanism proposed in Chapter 7c: Security acknowledges that third parties authorised under PSD2 with the FCA will be able to conduct business regardless of whether they are accredited.

At the time of writing, it is thought that the EBA will consult widely on its RTS, beginning in late 2015 or early 2016. While these consultations will be public and therefore open to all organisations to submit views, there would clearly be a benefit in being able to take forward a "UK position" that has the broad support of a majority of the market. It is hoped that through this report and the next steps associated with it, the market can achieve some consensus around how aspects of PSD2 could be delivered, and that these views can be strongly and confidently transmitted to the EBA. Accordingly, the Open Banking Working Group has already been in contact with the EBA, which is apprised of the work taking place. Further liaison between HMT and the EBA is scheduled for 2016.

It is also expected that the output from the Open Banking Working Group will help HMT and the FCA in shaping the transposition and implementing legislation of PSD2. Again, further liaison on this point is scheduled for early 2016.

6. Detailed requirements of PSD2's impact on the Open Banking Standard and Open Banking Framework

This section sets out in more detail the requirements of PSD2 relevant to the design of an API framework for the sharing of payment account information and initiation of payments. These requirements are accommodated in the proposals of the other chapters of this report.

Table A1.1 Scope of PSD2

	Scope
New regulated services – PIS and AIS	Payment initiation services (PIS): *"a service to initiate a payment order at the request of the payment service user (PSU) with respect to a payment account held at another payment service provider"* (PSP) Account information services (AIS): *"an online service to provide consolidated information on one or more payment accounts held by the payment service user [PSU] with another PSP or within more than one PSP"*. Payers/PSUs have the right to use PIS or AIS but the right only applies where the payment account is accessible online. Providers of such services are termed payment initiation service providers (PISPs) and account information service providers (AISPs)

Confirmation on availability of funds	PSD2 also includes a new provision (Article 65) that will require account-servicing PSPs to provide a confirmation (yes/no answer) on the availability of funds, i.e. whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer upon request of a card-based payment instrument issuer, subject to certain conditions being met. The AS PSP to provide the confirmation immediately provided that: ● The payment account of the payer is accessible online. ● The payer has given explicit consent, prior to the first request being made, to the AS PSP to respond to requests from a specific PSP to provide the confirmation. The PSP can request the confirmation if: ● The payer has given explicit consent to the PSP to request the confirmation. ● The payer has initiated the card-based payment transaction using a card-based instrument issued by the PSP. The PSP authenticates itself towards the AS PSP before each confirmation request, and securely communicates with the AS PSP in accordance with the common and secure open standards of communication to be determined in the EBA draft RTS (which will also apply to PIS and AIS). It is understood the card-issuing PSP will need to have appropriate authorisation (e.g. a licence to issue payment instruments as well as offer direct debits, credit transfers with credit line services as per PSD2 Annex 1 services points 4 and 5). As the PSP would receive the consumer funds, authorisation for PIS would not be enough. Card-based PIIs could have either a relationship with the PSU, or with the merchant, or both.
Account type	Payment account: *“an account held in the name of one or more PSUs which is used for the execution of payment transactions”*. Whether an account is deemed to be a payment account depends on its underlying purpose. The FCA Perimeter Guidance (PERG) Ch. 15.3 sets out the factors to consider and indicates that such accounts can include *“current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account mortgages”*. Conversely, the PERG does not view fixed-term deposit accounts (where there are restrictions on the ability to make withdrawals), child trust fund deposit accounts and cash Individual Savings Accounts (ISAs) as payment accounts. PSD2 introduces the term Account-Servicing PSP (AS PSP), i.e. a PSP providing and maintaining a payment account for a payer.

Geography and currency	PSD2 applies on a pan-European basis and, unlike PSD1, will extend many of the provisions to one-leg transactions and all currencies, not just the euro and other member state currencies. Solutions will need to work seamlessly within a national community and on a cross-border basis.
Reach and access channel	All AS PSPs need to be able to interact with any or all PISPs or AISPs on a pan-European basis if the payment account is accessible online. "Accessible online", while not explicitly defined, is understood to mean the use of all common types of devices (e.g. computers, tablets and mobile phones). A number of AS PSPs' online banking propositions may have an entirely domestic (or eurozone only) focus (reflecting their existing client base and business model) and do not enable PSUs to initiate cross-border payments in another currency. This report's view is that AS PSPs can only be required to execute those payment types that are currently offered by their existing model. In other words, an AS PSP should not be forced to offer e.g. SEPA DD just because of PIS and PSD2.
	Governance
Payment service providers and authorisation	PSD2 distinguishes between six categories of PSP: (1) credit institutions; (2) electronic money institutions; (3) post office giro institutions; (4) payment institutions; (5) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities; and (6) member states or their regional or local authorities when not acting in their capacity as public authorities. Undertakings - other than those referred to above as (1), (2), (3), (5) and (6) or benefiting from a waiver under Article 32 or 33 - that intend to provide payment services are required first to obtain authorisation as payment institutions. A firm wishing to offer PIS that was not already an authorised PSP would need to seek authorisation as a payment institution. Authorisation shall only be granted to a legal person established in a member state. Article 33 defines the supervisory regime for AISPs that are treated as payment institutions, but only subject to some of the PSD2 provisions. If a firm wished to start offering AIS and was not already authorised as a PSP, it would need to seek authorisation to do so. Recital 48 indicates that AISPs *"should be allowed to provide services on a cross-border basis, benefiting from the 'passporting' rules"*. If an AISP that was not already an authorised PSP also wished to provide add-on PIS, it would need to seek authorisation as a payment institution. PSD2 lays down the authorisation regime for payment institutions. Article 5 deals with the subject of applications for authorisation.

	Such applications must include, for example, a security policy document describing measures taken to protect PSUs from fraud, illegal use of sensitive and personal data. The capital held by payment institutions providing PIS *“shall at no time be less than EUR 50,000”*.
Transition	According to Article 115 of PSD2, member states should allow those who have provided PIS or AIS before PSD2 enters into force to continue to do so during the transitional period pending transposition of PSD2 into national law and pending application of the security measures to be defined by the EBA RTS.
PISP and AISP	PISPs and AISPs can be PSPs (e.g. credit institutions such as banks) that provide other regulated payment services and niche players who are specifically authorised to carry out PIS or AIS. AS PSPs can offer PIS and AIS if they wish.
Registration in the home member state	Member states are required to establish a public register of authorised payment institutions, AISPs and their agents. Branches of payment institutions are to be entered in the register of the home member state if those branches provide services in a member state other than their home member state. The public register will identify the payment services for which the payment institution is authorised or for which the AISP is registered. The register is to be *“publicly available for consultation, accessible online, and updated without delay”*. Competent authorities are required to enter in the public register any withdrawals of authorisation or withdrawal of a waiver and

	notify the EBA.
EBA Register	The EBA is obliged to *“develop, operate and maintain an electronic central register”* containing the information from the public registers, as notified by the competent authorities. The EBA will be responsible for the accurate presentation of that information. Competent authorities are responsible for the accuracy of the information and for keeping the information up to date. The register will be made publicly available on the EBA’s website and *“shall allow for easy access to and easy search for the information listed, free of charge”*. EBA is to develop draft RTS *“setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein. The technical requirements shall ensure that modification of the information is only possible by the competent authority and the EBA*”. EBA is to submit the draft RTS to the Commission [date not yet specified in the PSD2 text] for adoption. EBA is required to develop *“draft implementing technical standards on the details and structure of the information to be notified” by the competent authorities “including the common format and model in which this information is to be provided”*. The draft implementing standards are to be submitted to the Commission [date not yet specified in the text] for adoption. This report sees the EBA Register and information contained therein as the key mechanism to enable the AS PSP to obtain assurance on a regular (although not necessarily transactional) basis of both the identity and authorisation status of the PISP and AISP in order to protect the PSU against fraud and impersonation (e.g. criminal organisations pretending to be authorised PISPs and AISPs. The EBA Register would need to be highly automated, dynamic and updated in near real time (24x7 “hot-hot”) in order to be an effective source of information. The AS PSP may need to cross-check the authorisation status on a real-time basis. We believe it would be impractical to create a separate register for each country, which all AS PSPs would then have to access.

AS PSP and PISP/AISP relationship	The AS PSP must *"treat payment orders transmitted through a PISP without any discrimination for other than objective reasons… in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer"*. The AS PSP can't refuse to execute an authorised payment order irrespective of whether the payment order is initiated by a payer via a PISP, unless prohibited by other relevant EU or national law. Provision of PIS or AIS *"shall not be made dependent on the existence of a contractual relationship"* between the PISP, AISP and AS PSP for that purpose.
Consent	PIS - Article 66(2) states that the payer gives explicit consent for a payment to be executed in accordance with Article 64, which allows for consent to be given in a form agreed between the payer and the PSP and also allows for consent to be given via the PISP. Article 80(2) states that the payer *"shall not revoke the payment order after giving consent to the PISP to initiate the payment transaction"*. Article 80(5): *"After the time limits specified in paras 1 to 4, the payment order may be revoked only if and in so far as agreed between the PSU and the relevant PSPs"*. AIS - Article 67(2) indicates the AISP should provide services only where based on the PSU's explicit consent and access only the information from designated accounts and associated payment transactions. Article 94(2) states that PSPs shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the PSU. This report believes the AS PSP needs to be assured on a transactional basis of the genuineness of the PSU's consent. Clarity is required regarding what information can be accessed in terms of the data to be exchanged. The implication of Article 94(2) is that the extent of the information accessible to third parties is at the PSU's discretion. Various "mandate management" issues need consideration. How can the AS PSP be assured genuine consent is given by the PSU to initiate a payment transaction if the first communication is received through the PISP? It also needs to be made clear to the AS PSP what the PSU is consenting to. For example, with the use of an AISP, what information has the PSU consented to be shared and what happens if consent is subsequently withdrawn or altered? How is the AS PSP informed if the PSU withdraws consent? Clarity will also be needed on this from a liability context.

Liability/recourse	In the case of unauthorised transactions the payer is entitled to address a refund claim to the AS PSP, even where a PISP is involved and without prejudice to the allocation of liability between the PSPs. There is a formal obligation on the PISP to *“immediately compensate”* the AS PSP where the latter is liable for an unauthorised payment transaction or a non-executed or defective payment. In both cases the burden of proof is on the PISP. For example, according to Article 73 (see also Article 90), the AS PSP is required to refund the payer *“immediately, and in any event no later than by the end of the following business day”. If the PISP is liable, it is required to immediately compensate the AS PSP at its request for the losses incurred or sums paid as a result of the refund…”* The burden of proof is on the PISP *“to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge”*. At present, it remains unclear how the AS PSP will be able to obtain recourse from the PISP in the absence of any agreed resolution mechanism. This report considers it will be necessary for the EBA RTS to provide a communication channel for this purpose as part of the flows of information to be exchanged between the AS PSP and PISP.
Professional indemnity insurance	Undertakings applying for authorisation to provide PIS are required *“to hold professional indemnity insurance, covering the territories in which they offer services, or some other comparable guarantee against liability to ensure that they can cover their liabilities”* (Article 5). Similar provisions apply in the context of AIS to cover their liability vis-à-vis the AS PSP or the PSU *“resulting from non-authorised or fraudulent access to or non-authorised or fraudulent use of payment account information”*. The EBA will be mandated to issue guidelines *“on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or comparable guarantee”*. In doing so it is to take account of: ● The risk profile of the undertaking; ● Whether the undertaking provides other payment services or is engaged in other business; ● The size of the activity (for PIS this means the value of the transactions involved and for AIS the number of clients that make use of the AIS); ● The specific characteristics of comparable guarantees and the criteria for their implementation. The EBA is expected to review the guidelines on a regular basis.

	Use cases
PIS	PIS can take place in (but is not limited to) the context of an e-commerce scenario where the PISP's relationship is with the merchant and interactions with the PSU may be on a one-off or ad-hoc basis. Recital 27 describes such payment services as *"establishing a software bridge between the website of the merchant and the online banking platform of the payer's AS PSP in order to initiate internet payments on the basis of a credit transfer"*. It is understood PIS may also be offered as an add-on service alongside AIS (where the provider has the necessary authorisation) e.g. to move funds from one payment account to another.
AIS	PSD2 (Recital 28) describes AIS as providing the PSU *"with aggregated online information on one or more payment accounts held with one or more other PSPs and accessed via online interfaces of the AS PSP. The PSU is able to have an overall view of its financial situation immediately at any given moment"*. Article 67 simply refers to *"enabling access to payment account information"*, where the account is accessible online. In the context of AIS there would be a direct relationship between the AISP and the PSU.
Type of PSU	While much of the context given in the PSD2 Recitals appears to be written from a consumer's perspective, it is understood there is nothing in the provisions relating to PIS and AIS that would prevent such services being offered to all types of PSU, businesses as well as consumers.
	Data
Definition	Sensitive payment data Article 4(32) – data, including personalised security credentials that can be used to carry out fraud. For the activities of PISPs and AISPs, the name of the account owner and the account number do not constitute sensitive payment data.

PIS	The PISP shall: ● ensure that any other information about the PSU, obtained when providing PIS, is only provided to the payee and only with the PSU’s explicit consent; ● not store the PSU’s sensitive payment data; ● not request from the PSU any data other than those necessary to provide the PIS; ● not use, access or store any data for the purposes other than for the provision of PIS as explicitly requested by the payer; ● not modify the amount, the payee or other feature of the transaction. Article 47 requires the PISP to make available to the payer’s AS PSP the reference of the payment transaction. The AS PSP shall: ● immediately after receipt of the payment order from a PISP, provide or make available all information on the initiation of the payment transaction and all information accessible to the AS PSP regarding the execution of the payment transaction to the PISP.
AIS	The AISP shall: ● provide services only where based on the PSU’s explicit consent. ● access only the information from designated payment accounts and associated payment transactions. ● not request sensitive payment data linked to the payment accounts. ● not use, access or store any data for purposes other than for performing the AIS explicitly requested by the PSU, in accordance with data protection rules. The AS PSP shall: ● treat data requests transmitted through the services of an AISP without any discrimination for other than objective reasons.
Data protection	Article 94 of PSD2 addresses data protection. It permits the *“processing of personal data by payment systems and PSPs when necessary to safeguard the prevention, investigation and detection of payment fraud”*. It indicates that *“provision of information to individuals about the processing of personal data and the processing of such personal data” i*s to be carried out in accordance with European and national data protection legislation. It states that PSPs *“shall only access,*

	process and retain personal data necessary for the provision of their payment services, with the explicit consent of the PSU".
	Security and authentication
Definitions	Authentication Article 4(29) – a procedure that allows the PSP to verify the identity of a PSU or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials. Strong customer authentication Article 4(30) – an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. Personalised security credentials Article 4(31) – personalised features provided by the PSP to a PSU for the purposes of authentication. Sensitive payment data Article 4(32) – data, including personalised security credentials that can be used to carry out fraud. For the activities of PISPs and AISPs, the name of the account owner and the account number do not constitute sensitive payment data.

Personalised security credentials	There are ambiguities and seeming contradictions in the PSD2 text as to whether the PSU's personalised security credentials can be shared directly with the PISP or AISP or not. Article 97(3) - in reference to situations where the payer accesses his account online, initiates an electronic payment transaction or carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuse - refers to PSPs having in place *"adequate security requirements to protect the confidentiality and integrity of the PSU's personalised security credentials"* while Article 66(3b) and Article 67(2b) oblige the PISP and AISP *"to ensure that the personalised security credentials of the PSU are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties…"*. While Article 69 requires the PSU to *"take all reasonable steps to keep its personalised security credentials safe"*, Recital 69 states that terms and conditions or other obligations imposed by PSPs on PSUs in relation to keeping personalised security credentials safe should not be drafted in a way that prevents PSUs from taking advantage of services offered by other PSPs, including PIS and AIS. Clarity is needed from the Commission during transposition as to whether the intention is to provide access to information and communication to initiate a payment rather than access to the payment account itself. It is unclear if the intention is that AS PSPs will be required to develop and issue new sets of personalised security credentials to all PSUs – which will come at a significant cost – that can, somehow, be made invisible when used with PISPs and AISPs.

Authentication	PSD2 Article 97 addresses authentication. Article 97(1) distinguishes between three scenarios when PSPs should apply strong customer authentication i.e. when the payer: *“(a) accesses his payment account online;* *(b) initiates an electronic payment transaction;* *(c) carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses”*. In all these cases, according to Article 97(3), PSPs must *“adopt specific security requirements, to protect the confidentiality and the integrity of the PSUs’ personalised security credentials”*. When the payer initiates an electronic remote payment transaction, Article 97(2) requires PSPs to *“apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee”*. These provisions also apply when payments are initiated through a PISP or information is requested through an AISP (see Article 97(4)). AS PSPs must allow PISPs and AISPs *“to rely on the authentication procedures provided by the AS PSP to the PSU”* (Article 97(5)). As a general principle, we believe AS PSPs cannot be prevented from carrying out their normal AML/security/sanction checks and processes etc. just because payment initiation or account information have been requested via a PISP or AISP. Nor should AS PSPs be prevented from implementing new/enhanced security measures to address evolving market threats.
EBA RTS	Article 98 addresses RTS on authentication and communication – see Standards section below for more information. The PISP and AISP are required to identify themselves to the AS PSP *“every time a payment is initiated” (*PIS) or *“for each communication session”* (AIS) and communicate with the AS PSP, payer, payee, PSU in a secure way in accordance with the common and secure open standards of communication (Article 98(1d)) to be developed as part of the EBA RTS on authentication and communication. In the context of the provision regarding confirmation on availability of funds, the card-based payment instrument issuer must authenticate itself *“before each communication request”* and securely communicate with the AS PSP in line with the EBA RTS. The AS PSP is also required to securely communicate with PISPs and AISPs in line with the EBA RTS.
	Standards

EBA Register	See Governance section for further information. EBA is to develop draft RTS *“setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein. The technical requirements shall ensure that modification of the information is only possible by the competent authority and the EBA*”. EBA is to submit the draft RTS to the Commission [date not yet specified in the PSD2 text] for adoption. EBA is required to develop *“draft implementing technical standards on the details and structure of the information to be notified” by the competent authorities “including the common format and model in which this information is to be provided”*. The draft implementing standards are to be submitted to the Commission [date not yet specified] for adoption.

EBA RTS	See Security and Authentication section for further information. Article 98 requires EBA to develop RTS on authentication and communication in close cooperation with the ECB and in consultation with relevant stakeholders – within 12 months of entry into force of PSD2 – to be addressed to PSPs. The RTS have to be submitted to the European Commission for adoption, a process we estimate could take anywhere from 4 to 9 months. The RTS will apply 18 months after they have been adopted and enter into force. Until then PISPs and AISPs are allowed *“to continue to perform the same activities …in accordance with the currently applicable regulatory framework”* (Article 115(5)). In the meantime, (Article 115(6)) until individual AS PSPs comply with the RTS…they must *“not abuse their non-compliance to block or obstruct the use of payment initiation and account information services for the accounts that they are servicing”.* RTS to be reviewed/updated if appropriate, on a regular basis by the EBA (Article 98(5)). The EBA RTS are intended to specify: ● requirements of the strong customer authentication procedure referred to in Articles 97(1) & (2); ● requirements *“with which the security measures have to comply … in order to protect the confidentiality and the integrity of the PSUs’ personalised security credentials”* (in line with Article 97(3)); ● requirements *“for common and secure open standards of communication for the purpose of identification, authentication, notification and information as well as for the implementation of security measures, between AS PSPs, PISPs and AISPs, payers and payees”*; ● exemptions to application of Articles 97(1), (2) & (3), which are to be based on the following criteria: ○ the level of risk involved in the service provided; ○ the amount and recurrence of the transaction, or both; ○ the payment channel used for the execution of the transaction. The EBA RTS should (Article 98(2)): ● Ensure an appropriate level of security for PSUs and PSPs through the adoption of effective and risk-based requirements; ● Ensure the safety of PSU’s funds and personal data; ● Secure and maintain fair competition among all PSPs;

	● Ensure technology and business-model neutrality; ● Allow for the development of user-friendly, accessible and innovative means of payment. Recital 93 indicates that the requirements of common and open standards of communication should: ● *“allow for the provision of online payment services” and should “ensure the interoperability of different technological communication solutions”*. ● *“ensure that the AS PSP “is aware that he is being contacted by a PISP or AISP and not by the client itself”*. ● *“ensure that PISPs and AISPs communicate with the AS PSP and with customers involved in a secure manner”*. In developing those requirements, EBA should *“pay particular attention to the fact that the standards to be applied are to allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services”.* It should also *“take into account the privacy dimension, in order to identify the risks associated with each of the technical options available and the remedies that could be put in place to minimise threats to data protection”.*

EBA RTS consultation	It is understood that the EBA will issue a discussion paper once the final PSD2 text is published in the Official Journal of the EU (January 2016?) to check whether it has identified all of the key issues. A formal public consultation on the draft RTS will subsequently be undertaken, probably a few months later. Feedback will be used to finalise the draft RTS before submission to the European Commission for adoption by January 2017(?). EBA has indicated it will be considering the current guidelines on the security of internet payments when developing the RTS and the extent to which they are aligned with PSD2, need to change or be adapted to reflect evolving market conditions.
EBA guidelines versus RTS	The EBA has explained the difference between guidelines and RTS, which this report understands to be as follows: EBA can only issue RTS if given an explicit mandate. Once RTS are adopted by the EC (and published in the Official Journal) they become EU law and must be complied with. Member states and national authorities do not need to issue secondary legislation. EBA does not need a mandate to issue guidelines, which should be reviewed after two years; guidelines are not directly applicable in EU law. National authorities are expected to integrate into their national supervisory regimes and take action. In cases of non-compliance this should be reported to the EBA. However, national authorities also have the option not to comply, e.g. the guidelines on the security of internet payments where the UK, Estonia and Slovakia have not complied as the national authorities lacked the legal power to do so. Guidelines are addressed to firms. However, if a national authority decided not (or was unable) to implement the guidelines it is unlikely that the EBA would pursue a specific firm for breach of EU law (although it has the power to do so). However, there is an obligation on firms to make their best efforts to comply. If a third party launched a legal challenge against a firm for non-compliance, legal interpretation of the extent of compliance would be for the court or ombudsman to determine. Firms need to be able to explain the reasoning behind why the guidelines have been followed or why they have not.

Appendix 2. Digital identity review

1. Background

Digital identity and digital identity assurance are topics that have been growing on the government, regulatory and industry agenda in the UK for some time. As the world becomes increasingly digitised, the need has grown for a reliable and efficient way of proving people are who they say they are when they want to access a digital product or service. In the UK, the use of digital ID by consumers is not yet widespread.[25] In Europe, adoption of some form of digital ID is more common: "2*1 European member states are now issuing national eID documents. 20 of them are proposing secure electronic identification, authentication and digital signatures to hundreds of thousands of online services using the internet, tablets and mobile devices*... *Market penetration in some countries such as Belgium is close to 100%.*"[26]

In part, the growth in the use of digital IDs is the result of the Regulation on Electronic Identification and Trust Services For Electronic Transactions (eIDAS), published in 2014. The regulation established requirements for mutual recognition of notified electronic ID schemes across EU member states for accessing public services. Growth in use may also be the result of private sector initiatives, for example, the mobile network operator-led GSMA Mobile Connect solution and the web-based Fast Identification Online (FIDO) alliance.

Despite this growth, there is as yet still no consistent view about the best way to deliver digital ID solutions, to what standards and to what levels of security, which inevitably limits the interoperability. Digital ID schemes in Europe in many cases require the citizen to hold a centrally issued physical ID card that is used as one of the factors of authentication. In the UK, this is seen as politically unpalatable. Indeed the approach taken for GOV.UK Verify is intentionally decentralised/federated.

2. Developments in the UK

There are a wide variety of activities underway in the market, both in the UK and internationally. It is not possible to provide an exhaustive list here. However, these are some of the more relevant ones in the UK when considering the OBWG API Framework.

2.1 The UK government's GOV.UK Verify programme

[25] Within the banking infrastructure, electronic/digital ID for business use, e.g. authentication and digitally signing transactions, is more common. Many UK and US banks participate in the IdenTrust Framework, which "*provides a global common identity standard that provides non-repudiable, legally enforceable, contractually bound digital signatures that are interoperable across geographies, companies and applications*".

[26] Eurosmart: The Future Digital Identity Landscape. A country with good penetration of digital identity is Estonia, which offers "e-Residency – a transnational digital identity available to anyone in the world interested in administering a location-independent business online. e-Residency additionally enables secure and convenient digital services that facilitate credibility and trust online". Note, however, that the Estonian system also relies on use of a smartcard and, for example, to establish an Estonian bank account currently requires an in-person meeting at the bank.

The UK Identity Assurance Programme (IDAP), part of the Cabinet Office's Government Digital Service (GDS), has been developing a requirements-based, federated identity assurance service called GOV.UK Verify.[27] It allows citizens to prove they are who they say they are (to a level of confidence) when they sign in to government services that require an online identity authentication. Users of the online government services (i.e. UK citizens) need to register themselves via an identity provider (IDP),[28] which is a private sector organisation certified against government standards (as defined in the Good Practice Guides). The IDP will perform checks to confirm the user’s identity, issue a credential and then assert that identity to the government department via GOV.UK Verify. The service has been running in beta alongside government department services since October 2014 and aims to become the default way for people to access government digital services by April 2016.

GDS has been engaging widely with industry about the development of GOV.UK Verify. It is clear that for the government and its citizens there would be benefit in wider use of the services offered by IDPs. At present this remains a decision for individual firms and the programme would need to align with their own market strategy and risk appetite. GDS is also exploring whether the trust framework created through the Good Practice Guides could be extended into the private sector (an early adopter may be the TISA Digital ID project: see below). This work is ongoing but it would clearly be valuable to monitor it in the next phase of this work.

2.2 The Tax Incentivised Savings Association (TISA) digital ID for consumers of UK financial services

In February 2015, TISA launched The Savings and Investments Policy Project (TSIP), a coalition of more than 50 companies and trade bodies, which published a report for the government entitled Saving our Financial Future. The report sought to promote greater levels of saving among UK consumers and made a number of recommendations, including one on the creation of a digital ID. It identified that one of the barriers to customers switching or changing financial services providers was the difficulty associated with onboarding because of a lack of an ability to assert a digital identity. Consequently, TISA established a digital ID project to take forward the work. The TISA project proposes the potential reuse of some of the GOV.UK Verify framework.

If both projects above proceed as planned, it is likely that within the next few years citizens and financial services customers will have become more accustomed to obtaining and using digital identities.

3. The use of digital ID in UK financial services

The use of digital identity within financial services is a complex topic. At present, the adoption of digital identity mechanisms is ultimately a commercial decision for each individual organisation, which will make decisions based on its understanding of its customers and its own liability and risk appetite.

In the Nordic countries, an approach has been taken whereby a form of trust framework[29] between banks and government enables customers to use a single electronic ID (known as BankID) to access

[27] See https://identityassurance.blog.gov.uk/

[28] Current IDPs include the Post Office, Experian, Digidentity and Verizon, Barclays, GB Group, Morpho, PayPal and Royal Mail.

[29] A trust framework is a certification program that enables a party that accepts a digital ID credential (called the relying party) to trust the identity, security and privacy policies of the party that issues the credential (called the identity service provider) and vice versa.

a variety of services (e.g. a payment service for online shopping, login and payment via internet banking, change of address with the postal service, placing a bid when buying property, login on municipal websites, purchasing units in equities funds). Such an approach clearly has benefits for customers, such as ease of access to services, in that they are issued just one electronic ID to access a range of services. However, there are downsides as well, such as the risks inherent if the user's credentials are breached.

This report recommends that organisations (e.g. ASPs and 3PPs) should own and control the method by which they authenticate their own users. This means (at least for the short to medium term) that it should remain a commercial decision whether an organisation chooses to take advantage of a digital identity mechanism to authenticate its users. However, the market is likely to be driven by customer demand, and if demand for using ubiquitous digital identities is present then this may lead to changes to current authentication processes, e.g. if customers show preference for using a single set of "credentials" across numerous providers.

At this stage the OBWG API Framework has not been designed to rely on digital identities. However, if the use of a digital ID model(s) were to grow then the authentication processes as described in this report should be able to accommodate this.

4. Digital ID services as a use case of open APIs

Digital ID services are likely to form a prominent use case of the open API in and of themselves. The increased access to consented customer data is likely to provide improvements to some current digital identity assurance services (including GOV.UK Verify[30]) and lead to new ones coming into existence.

[30] See the paper published by OIX: The use of bank data for identity verification, http://www.oixuk.org/wp-content/uploads/2015/08/THE-USE-OF-BANK-DATA-FOR-IDENTITY-VERIFICATION-OIX-White-Paper-FINAL-August-2015.pdf

Appendix 3. General Data Protection Regulation

The General Data Protection Regulation (GDPR) will make wide-ranging changes to the data protection legal landscape in the UK and across the EU. Table A3.1 below aims to summarise key changes that are relevant to the development of the Open Banking API framework. It is not exhaustive and not certain; the final text has not been agreed so these impacts could change. This analysis distinguishes, where appropriate, between the two rival draft texts: that of the European Parliament (EP) of 12 March 2014, and the General Approach of the Council of Ministers agreed on 15 June 2015. At the time of writing, the EP and the Council were negotiating a final text, which is likely to contain elements of both draft texts.

Table A3.1 Key changes of GDPR

Key topic	Impact/comment
Data minimisation (Article 5)	CHANGE: If the EP text prevails, rather than requiring data collected not to be excessive (current DPA requirement), the requirement would instead be to ensure that only the “minimum necessary” for the intended purposes is processed. IMPACT: Data attribute providers and 3PPs will need to have refined and clear data-processing purposes in order to ensure that only the minimum is shared, and the API framework will need to allow for a minimum of unnecessary data-sharing in each instance.
Profiling and information to be provided to the data subject (Article 20)	CHANGE: Profiling activities are portrayed in the EP draft of the regulation as being quite negative and could in some instances be prohibited. IMPACT: The range of use cases that could be provided through the open data initiative could be curtailed.
Consent (Articles 7 and 4(8))	CHANGE: 1) The EP text would require consent to always be “explicit”. This is more complex and requires more explanation than does ordinary consent. 2) Data subjects must be able to withdraw consent freely at any time under both texts. IMPACT: 1) Services designed to rely on consent would need to instead use explicit consent. 2) All controllers must ensure that they have processes in place to allow the withdrawal of consent. Data attribute providers must be able to determine on an ongoing basis whether consent for the ongoing

	sharing of data is valid or has been withdrawn.
Right to data portability (Article 18 of Council text, Article 15(2a) of EP text)	CHANGE: Although the details vary between the two texts, broadly the data subject has the right to receive their personal data (where they have provided it to the controller) and transfer it to another controller. There is an exemption to protect IP rights under the Council text. IMPACT: The API framework could form an efficient means of meeting this obligation, both for data attribute providers and 3PPs.
Right to object (Article 19)	CHANGE: Data subjects will have a right to object to processing that is based on the "legitimate interests" of the data controller. Under the EP text this right will be unrestrained, while under the Council text controllers will be able to refuse to halt processing, if deemed appropriate following a "balancing of interests" test. IMPACT: Data attribute providers and 3PPs will need to have systems enabling them to comply with this requirement. Although processing will more likely be based on consent in the first instance, where a data subject cannot consent (e.g. where the data of a third party is mixed with the data of the end-customer) then legitimate interests might be used, with the third-party data subject then able to object. In practice this is probably unlikely, but controllers will need to have systems in place to enable compliance.
Data protection by design and by default (Article 23)	CHANGE: All data controllers will need to proactively implement systems and policies to ensure that data processing is compliant with the GDPR. Demonstrating compliance can be assisted by following an approved Code – see Article 38. IMPACT: More planning, systems and documentation will be needed by data controllers.
Joint data controllers (Article 24)	CHANGE: Under both texts, where two or more controllers jointly determine the purposes and means of the processing of personal data, they are "joint controllers". They must in this case determine their respective responsibilities for compliance with their obligations, including the provision of a privacy notice. IMPACT: Depending on the nature of the arrangement between the data attribute provider and the 3PP, this requirement to cooperate and assign responsibilities could apply. This could arise where a service is provided under a contractual basis by a 3PP to a data attribute

	provider, for example, insofar as this is consistent with PSD2 rules.
Data breach notification and impact assessment (Articles 31 and 32)	CHANGE: Controllers will need to notify the ICO and data subjects in the event of a data breach. The minimum severity threshold for these two types of notification, and the timeframes for compliance, are yet to be finalised. Under Article 26, processors must assist controllers to comply with this requirement. IMPACT: For processors, they must ensure that they have systems in place to notify the controller of data breaches. For controllers, in the event of a data breach at a 3PP that crosses the severity threshold, the 3PP will need to notify the affected data subject(s). This does appear to overlap with requirements proposed under PSD2 and further work will be required to understand how the two regimes will work together.
Codes of conduct (Article 38)	CHANGE: The ICO will be empowered to approve industry codes of conduct to assist data controllers wishing to process personal data in a compliant manner. Given the complex nature of the GDPR, this could be helpful for smaller businesses and startups in particular. This will also help reassure data attribute providers that the personal data they share with 3PPs will be processed in a fair and compliant manner.
Registration with the ICO (no article)	CHANGE: Contrary to the DPA, the GDPR does not require data controllers to register with the ICO.

Appendix 4. The current account midata initiative and its relevance

1. Background

The PCA midata initiative was focused on enabling consumers to shop around more effectively for an appropriate current account. To this end, participating banks allow their customers to download a specially formatted midata file, which can then be uploaded to a third-party price comparison website, which will analyse the file and recommend current account options/providers on the basis of the customer's specific transaction history.

In July 2014 CEOs from a number of UK retail banks made a commitment to deliver current account midata downloads on the basis of an agreed midata standard.

2. Midata file content

According to the agreed July 2014 midata standard:

- *Banks that have committed to deliver midata downloads will provide personal current account customers, registered for online banking, with their own current account transaction data, on demand, in electronic format, by 31 March 2015.*
- *This data will be available for customers to access and download, anonymised as appropriate and provided in a format that is consistent with this agreed industry standard.*

Downloads include 12 months of transaction history, transaction type, descriptor field and amounts.

Midata files could theoretically be used for many purposes but the focus of the initiative was on PCA comparison. The content and design were agreed with this purpose in mind through a working group of participating banks, PCWs and government observers.

3. Risks and legal challenges

Over the course of the project, a range of challenges presented themselves.

Fraud

Customers' banking data includes a lot of information about that person. Depending on the nature of that data, this could be used to impersonate the customer (for example, questions about recent transactions are often used by banks to help verify a customer's identity e.g. when the customer has lost their password). Also, some banks' transaction description fields include the account number of either the payer or payee. Fraudulent websites could seek to take advantage of this, as could hackers gaining access to poorly secured (but legitimate) websites that store customer data.

Data protection issues

The DPA sets rules to protect the privacy and data of individuals. These rules were highly relevant to the midata initiative, as midata files could contain personal data, including potentially sensitive personal data. Transaction histories in midata files can often include the personal data of third parties. This is particularly the case for standing orders and other transfers to friends and family, which will frequently have that person's name in the descriptor line and may also include account numbers.

A more detailed explanation of data protection issues is contained in the Chapter 8: Regulatory and Legal Considerations.

Trust

It is important that consumers have faith in the process. This requires effective protection of their data, transparency and also reasonable standards of accuracy in comparison calculations.

Technical

Transactional data is not structured the same way in each bank. This has an impact on third parties' ability to analyse files, which will look different for each bank, despite the standardised content and format. For example, transaction codes vary between banks as do the entries in the descriptor field, even for identical transactions. These differences in the information in descriptor lines for transactions also mean that data protection and fraud risks are potentially different for different banks.

There are also technical limitations to banks' ability to redact data. Redacting numbers in certain fields is feasible, as is redacting certain fields entirely. But more complex approaches, such as distinguishing between the names of individuals versus companies, is not technically possible.

Oversight

Although midata files were designed with current account comparisons as the primary purpose, consumers could theoretically upload a file to any site that requests it. There is no control over what customers do with their files and offering midata services is not a regulated activity, so there is no licensing framework (although FCA licensing would be needed for websites providing a credit-broking service).

The DPA and other laws still apply, but the absence of supervision or licensing does increase risks to consumers.

4. Mitigations

The midata working group sought the advice of the ICO and a privacy impact assessment was conducted. There were extensive discussions of the data necessary for comparisons to occur, the fraud and data protection compliance risks, and the technical limitations faced by banks seeking to redact unnecessary or sensitive data.

Ultimately, a range of measures were agreed to address the issues above:

- (Imperfect) anonymity – midata files do not directly include the consumer's name or account number, although it was recognised that a PCW could easily request the consumer's name at the time of upload.

- Redactions – the consumer’s name or account number (or those of silent third parties) would sometimes appear in certain transactions’ descriptor fields. Therefore, redactions were agreed to minimise the chance of this occurring:
    - Transaction types identified as being less relevant to account comparison and more likely to contain third parties’ data were subject to standardised redactions, in line with the DPA requirement for data processing not to be excessive.
    - The transaction types of most relevance to account comparison were identified as ATM transactions, debit card/point of sale transactions, direct debits (because of their relevance to account provider rewards), and fees, charges and interest. These transaction types are subject to little or no redaction.
    - This was done on the basis of transaction codes, although these vary between banks, creating a possibility of slightly different application in practice.
    - The most recent month’s data is excluded from the file, as this is more commonly used in banks’ identification and verification (ID&V) processes.
    - The detail of these redactions is set out in the midata standard.
- Transparency – disclosures by the bank and the websites, describing the process, risks, the data in the files and how this would be used.
- Customer consent was made a condition of the download.
- Code of conduct – a voluntary industry code of conduct was prepared by participating banks, certain participating PCWs, and in consultation with the government in order to clarify best practice.

5. Relevance to the Open Banking initiative

The above experiences provide useful insights into issues of relevance to the Open Banking initiative and how data protection and other risks can be managed in data-sharing arrangements. However, there are also relevant differences.

- Purpose – although midata files could in theory be uploaded anywhere, they were designed particularly for analysis of account usage and the recommendation of account options. The Open Banking API initiative is much broader of purpose, as indicated in the range of use cases in this report.
- Scope of data – midata files’ content is standardised to include specific data points. Therefore, third parties receiving uploads see all of this data, irrespective of the service (or purported service) to be provided to the customer. Under the Open Banking initiative, a wide range of data points would be within scope, but different third-party service providers would be able to tailor the data requested to fit the service they provide.
- Data delivery method – midata provides the customer with a standard file, which the customer can then do with as desired. This creates a risk that the customer would supply it to third parties that are not transparent about how they would use the data (e.g. mining it for insights into the consumer’s behaviour in order to target marketing material, or selling it on without disclosing this properly to the consumer), or even to fraudulent sites seeking to acquire customer data to impersonate that customer and gain access to their bank account. Under the Open Banking initiative there is greater scope for control of who receives the customer’s data via a vetting of 3PPs.

For a more detailed explanation of the midata initiative, the code of conduct and the content of midata files, see http://www.pcamidata.co.uk.

Appendix 5: Detailed indicative data release

Table A5.1 Data scope

Req. ref	Data class	Schema	Attribute L1	Attribute L2	Attribute L3
R001	Open data	Provider name			
R002	Open data	Branch(s)			
R003	Open data		Location		
R004	Open data		Address		
R005	Open data		Hours		
R006	Open data		Facilities		
R007	Open data		Services		
R008	Open data	Contact(s)			
R009	Open data		Type		
R010	Open data		Contact		
R011	Open data		Purpose		
R012	Open data		Note		
R013	Open data	ATM(s)			
R014	Open data		Location		
R015	Open data		Address		
R016	Open data		Services		
R017	Open data		Status		

R018	Open data	Digital service(s)			
R019	Open data		Type		
R020	Open data		URL		
R021	Open data		Requirements		
R022	Open data		Note		
R023	Open data	Product(s)			
R024	Open data		Type		
R025	Open data		Description		
R026	Open data		Benefits		
R027	Open data		Charges		
R028	Open data		Demographic		
R029	Open data		Accept rate		
R030	Open data		Legacy		
R031	Open data		Eligibility		
R032	Non-public customer facing data	Account holder			
R033	Non-public customer facing data	Account holder DOB			
R034	Non-public customer facing data	Account holder address			
R035	Non-public customer facing data	Account holder contact(s)			
R036	Non-public customer facing data		Type		
R037	Non-public customer facing data		Contact		

R038	Non-public customer facing data	Account(s)			
R039	Non-public customer facing data		Account name		
R040	Non-public customer facing data		Account type		
R041	Non-public customer facing data		Activity available from		
R042	Non-public customer facing data		Account number		
R043	Non-public customer facing data		Sort code		
R044	Non-public customer facing data		IBAN		
R045	Non-public customer facing data		Balance		
R046	Non-public customer facing data		Statement from		
R047	Non-public customer facing data		Statement to		
R048	Non-public customer facing data		Opening balance		
R049	Non-public customer facing data		Closing balance		
R050	Non-public customer facing data		Debit system		
R051	Non-public customer facing data		Card type		
R052	Non-public customer facing data		ATM limit		
R053	Non-public customer facing data		Manage via		

R054	Non-public customer facing data			Branch	
R055	Non-public customer facing data			Online	
R056	Non-public customer facing data			Post	
R057	Non-public customer facing data			Post office	
R058	Non-public customer facing data			Telephone	
R059	Non-public customer facing data			Text alerts	
R060	Non-public customer facing data			Smartphone	
R061	Proprietary data		Interest payment frequency		
R062	Proprietary data		Interest payment method		
R063	Proprietary data		Interest rate type		
R064	Proprietary data		Representative example		
R065	Proprietary data		Benefit(s)		
R066	Proprietary data			Type	
R067	Proprietary data			Note	
R068	Proprietary data		Eligibility		
R069	Proprietary data			Age min	
R070	Proprietary data			Local area only	
R071	Proprietary data			Business only	
R072	Proprietary data			Visa holders allowed	

R073	Proprietary data			Northern Ireland only	
R074	Proprietary data			Islamic law	
R075	Proprietary data			Students only	
R076	Proprietary data			Upgrading customers only	
R077	Proprietary data			Fundings	
R078	Proprietary data			Financial income	
R079	Proprietary data			Residency	
R080	Proprietary data		Fee(s)		
R081	Proprietary data			Type	
R082	Proprietary data			Frequency	
R083	Proprietary data			Amount	
R084	Proprietary data			Tier lower	
R085	Proprietary data			Tier higher	
R086	Proprietary data		Fee cap(s)		
R087	Proprietary data			Fee count max	
R088	Proprietary data			Fee count max frequency	
R089	Proprietary data			Fee amount max frequency	
R090	Proprietary data			Fee type(s)	
R091	Proprietary data			Applies to	
R092	Proprietary data		Rate(s)		
R093	Proprietary data			Annual interest AER	
R094	Proprietary data			Annual interest EAR	
R095	Proprietary data			Annual interest percentage type	

R096	Proprietary data			Annual interest yearly	
R097	Proprietary data			Applies to	
R098	Proprietary data			Frequency	
R099	Proprietary data			Period lower	
R100	Proprietary data			Period upper	
R101	Proprietary data			Tier lower	
R102	Proprietary data			Tier upper	
R103	Proprietary data			Transferred accounts only	
R104	Proprietary data			Type	
R105	Non-public customer facing data		Overdraft Buffer(s)		
R106	Non-public customer facing data			Type	
R107	Non-public customer facing data			Applies to	
R108	Non-public customer facing data			Amount	
R109	Non-public customer facing data			Note	
R110	Non-public customer facing data		Repayment		
R111	Non-public customer facing data			Minimum payment required	
R112	Non-public customer facing data			Minimum payment due	
R113	Non-public customer facing data			Charge(s)	
R114	Non-public customer facing			Statement of arrears?	

	data				
R115	Non-public customer facing data		Transaction(s)		
R116	Non-public customer facing data			Transaction ID	
R117	Non-public customer facing data			Posted date	
R118	Non-public customer facing data			Transaction date	
R119	Non-public customer facing data			Amount	
R120	Non-public customer facing data			Description	
R121	Non-public customer facing data			Credit/debit	
R122	Non-public customer facing data			Currency	
R123	Non-public customer facing data			Type	
R124	Non-public customer facing data			Is recurring	
R125	Non-public customer facing data			Recurring frequency	
R126	Non-public customer facing data			Merchant	
R127	Non-public customer facing data				Merchant ID
R128	Non-public customer facing data				Merchant category code
R129	Non-public customer facing data				Merchant category code name

R130	Non-public customer facing data				Merchant name
R131	Non-public customer facing data				Merchant location
R132	Non-public customer facing data				Market segment code
R133	Non-public customer facing data				Transaction auth date
R134	Non-public customer facing data				Transaction auth time
R135	Non-public customer facing data				Authorisation time of transaction
R136	Non-public customer facing data				Approval/denial reason code
R137	Non-public customer facing data				Approval denial reason type
R138	Non-public customer facing data				Cash back flag
R139	Non-public customer facing data				System transaction code
R140	Non-public customer facing data				Cardholder ID method
R141	Non-public customer facing data				POS entry mode
R142	Non-public customer related data	Maintainer			
R143	Non-public customer related data	Created date			
R143	Non-public customer related data	Last updated			

Appendix 6. Open banking: risks and mitigants

Please refer to Chapter 7c: Security for context.

Table A6.1 Risks and mitigations

Risk	Impact	Mitigation examples
MALWARE		
Infection of EUDs with malware designed to facilitate man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks	Compromise of customer data and fraud Reduced customer confidence, limiting take-up	User education and awareness regarding malware infection prevention Adopt measures to detect infection and deny API access to infected devices Develop a visible kitemark scheme to give users confidence that apps and software are accredited (can be spoofed) Provide a lookup service so users can independently check approved 3PPs Use of mutual authentication techniques to show the user they are interacting with legitimate software (e.g. show personalised attributes such as a picture provided by the user) OOB authentication/authorisation challenges for high-risk actions (e.g. making payments) Behavioural monitoring

Malware on 3PSP server	Enables MITM attacks, resulting in wholesale compromise of customer data and fraud	Security standards to protect servers from unauthorised access Regular scanning of servers for static malware signatures; network monitoring for malware traffic patterns Behavioural monitoring OOB authentication/authorisation challenges for high-risk actions (e.g. making payments)
Malware on ASP server	Compromise of customer data and fraud	Security standards to protect servers from unauthorised access Regular scanning of servers for static malware signatures; network monitoring for malware traffic patterns
Use of tailored malware (targeted at API interactions and/or designed to detect api data) that is unrecognised by antivirus software	Compromise of customer data and fraud	Behavioural monitoring

Risk	**Impact**	**Mitigation examples**
3PP RISKS		
Users fail to properly read and/or understand the permissions they are granting to 3PPs (e.g. while users will be prompted to provide authority to 3PPs, they may not read the request properly)	Users inadvertently grant greater permissions to 3PPs than they intended Lack of clarity regarding responsibility/liability if fraud occurs and the user suggests they didn't understand what they were approving Reputational damage through poor customer communications and lack of clear and explicit permissioning	User education Clear standards (and restrictions) for 3PPs on content and format of terms and conditions Prompting of users to review permissions by ASPs when appropriate, such as if the user changes their core credentials with the ASP (potentially indicating some concern of the user about those credentials) or when the ASP detects a suspected fraud attempt against the user's account

Account data obtained via the API (legitimately) is subsequently compromised (e.g. after being downloaded and stored on a 3PP platform or user device)	Compromise of customer data Leveraging of such data data to effect a social engineering attack (on the bank) to effect fraud or an account takeover Reputational damage to the ASP	Clear security requirements for participants throughout the delivery chain Adoption by ASPs of customer authentication protocols that do not rely on knowledge of information that can be obtained via the API
Overly onerous or expensive security vetting requirements	Prospective 3PPs are discouraged from undergoing security vetting reducing customer choice	Ensure that vetting requirements do not place an undue/unreasonable burden on 3PPs Adopt standardised vetting processes and certification that allow financial institutions to remain aligned with FCA recommendations Adopt a tiered approach to security vetting that aligns the level of vetting with the risk associated with the permissions the 3PP wishes to be able to obtain
Lack of clarity regarding rules governing 3PPs' ability to act as intermediaries or platforms for making API data available to other service providers or software	3PPs use their vetted status to provide access to APIs to parties that have not been vetted Lack of clarity regarding responsibility/liability if customer data is compromised or fraud occurs Greater risk of compromise of customer data stored by parties who are not subject to security standards	Clear security requirements for participants throughout the delivery chain, including clearly defined rules governing how 3PPs may relay API data to other parties Use of data protection regulations to prohibit processing of data obtained via APIs by persons or organisations who have not been vetted/authorised
Bad actors imitate legitimate 3PSPs through email phishing and fake websites	Compromise of customer data and fraud Reduced customer confidence, limiting take-up	User education and awareness Coordination of efforts by 3PPs and ASPs to identify phishing sites and have them taken offline or blocked All ASPs and 3PPs should consider measures (e.g DMARC) to prevent phishing
Bad actors imitate legitimate 3PAPs by developing fake apps and software	Compromise of customer data and fraud Reduced customer confidence, limiting take-up	Require OOB verification of high-risk actions (e.g. addition of payees, initiation of payments) carried out via apps and software

Increased risk of vishing Little to no capability from the customers to authenticate a caller purporting to be calling from an ASP or 3PP	Grooming of customers for fraud Reputational damage to 3PPs and ASPs Reduced customer confidence, limiting take-up	Customer education by both 3PPs and ASPs Adoption by ASPs and 3PPs of consistent processes for identifying themselves to customers in a manner that provides assurance of the source
Theft or loss of EUDs	It is not possible to protect data at rest where the attacker has access to the storage media and sufficient time to attack the system (e.g. data stored on smartphones). Bad actors could also exploit poor authentication controls to make use of apps, software or service that had previously been authorised by the legitimate user. Compromise of customer data and fraud Reduced customer confidence, limiting take-up	Avoid storing data on EUDs where possible, or limit it to non-sensitive data Use of appropriate authentication controls by 3PPs to prevent impersonation of users by bad actors who have obtained the user's device Use of labels to minimise the distribution of sensitive data (e.g. account nicknames instead of account numbers) to prevent their use in social engineering attacks
Impersonation by bad actors of account holders when registering with 3PSPs (e.g. through the use of PII obtained from other sources)	Bad actors gain indirect access to accounts via 3PSPs. Compromise of customer data and fraud Reduced customer confidence, limiting take-up	Require that users must be authenticated using their ASP's authentication solution before 3PPs are authorised to access any sensitive data
Compromise of 3PSP servers resulting in the wholesale theft of access tokens	Wholesale compromise of customer data and fraud Could lead to large-scale data breaches in a similar way to credit card data breaches today. The access token acts as a magic value that provides access to data and services	Security standards to protect servers from unauthorised access Use of Holder of Key (HoK) controls in conjunction with measures to protect keys (e.g. hardware security modules) Granting of short-lived tokens for high-risk functions Technical measures to prevent the use of stolen access (e.g. IP whitelisting, mutual SSL)
Risk	**Impact**	**Mitigation examples**
ASP RISKS		

Bad actors exploit the API as an attack channel to gain full (i.e. write) access to ASPs' core systems	Unauthorised manipulation of ASP systems Wholesale compromise of customer data and fraud Reputational damage to the ASP	Security standards to protect API infrastructure from unauthorised access and ensure robust application security
Reduction in ASPs' ability to detect fraud due to the presence of 3PPs as an intermediary between ASPs and their customers	Some ASPs use information such as the user's IP address or user agent to inform their fraud prevention measures. Compromise of customer data and fraud	Allow 3PPs to pass data on the end-point transaction environment back to ASPs Allow ASPs to require re-authentication (i.e. authentication challenge) if they have grounds to believe that an API request may be the result of fraudulent activity
Targeting of 3PPs with social engineering attacks	3PPs will become part of the social engineering attack surface. Bad actors may seek to gain indirect access to users' accounts by carrying out social engineering attacks against 3PPs (e.g. requesting password reset) Compromise of customer data and fraud	Education of 3PP customer service staff regarding social engineering Security standards requiring robust user authentication by 3PPs during customer service interactions to prevent social engineering Include in the API Standard a mechanism that allows 3PPs to trigger re-authentication of users by ASPs, and require that 3PPs do so in the aftermath of events such as password resets
Risk	**Impact**	**Mitigation examples**
ECOSYSTEM RISKS		
Lack of public confidence in the security measures surrounding the API	Lack of understanding on the part of the public could cause them to over-estimate the risks associated with using API-based services, apps or software Reduced customer confidence, limiting take-up	Public education regarding the risks and benefits of the API Standard Adoption of policies similar to the Direct Debit Guarantee to foster public confidence in the API Standard
Varying levels of security across ASPs and 3PPs	When users' data is stored in multiple locations by multiple parties, the security that protects such data is only as strong as the weakest link Compromise of customer data and fraud	Define common security standards that are enforced across all parties

Difficulty in identifying the source or site of a security breach	When users' data is stored in multiple locations by multiple parties, identifying the source or site of a security breach may not be straightforward Inability to react effectively to security breaches Lack of clarity regarding responsibility/liability for losses resulting from security breaches	Adoption of measures by 3PPs and ASPs to facilitate effective investigation of security breaches (e.g. time-synchronised audit logs, information-sharing) Clear policies governing the assignment of responsibility/liability for losses resulting from security breaches, with provisions for user compensation in circumstances where responsibility cannot be reliably assigned
Bad actors apply to become 3PPs, with malicious intent	Compromise of customer data and fraud Reputational damage to the API Standard Reduced customer confidence, limiting take-up	Organisations that wish to become 3PPs and gain access to APIs should be subject to appropriate vetting
Lack of public confidence in the security measures surrounding open data	Users may wish to opt out of allowing their data to be included in open data sets, making it more complicated and expensive to produce them, and limiting their utility c.f. Challenges experienced by the NHS due to large numbers of patients opting out of GP data-sharing http://www.pulsetoday.co.uk/your-practice/practice-topics/it/nhs-overriding-700000-patient-opt-outs-to-gp-data-being-shared/20009761.fullarticle	Minimise the grounds for individuals to have concerns/misgivings about the inclusion of their personal data in the creation of open data Foster confidence in open data by mandating specific processes that make it impossible to extract personal data from open data through analysis or reverse engineering
Reduction in the effectiveness of ASPs' existing customer ID&V processes	*Where an ASP's customer ID&V processes rely on the customer's knowledge of information that can be obtained via the API (e.g. recent transaction history), any compromise of that ASP's customers' data (e.g. through a malware attack or compromise of a 3PP's infrastructure) may allow bad actors to effect an account takeover* Fraud and account takeover	Individual ASPs should perform a risk assessment Establish a joint effort to define new, shared standards for ID&V that do not rely on knowledge of information that can be obtained via the API

Table A6.2 Pros and cons of open authorisation protocols

	Pros	Cons
OAuth 1.0	● Lots of client libraries ● Doesn't rely solely on TLS to secure bearer tokens	● Good for browser-based sites but not such a good story for mobile apps ● Concerns mixed-resource server and authorisation server, also request signing ● Harder for developers to get started with ● Not much further development going on ● OAuth 1 was officially deprecated in April 2012
OAuth 2.0	● Robust protocol with much better separation of concerns ● Newer, more forward-looking implementation ● OAuth 2.0 distinguishes between agents that can control their own security (typically server-side applications) and those that cannot (typically browser, client-side). This useful distinction helps to inform the token passing mechanism suitable for a given agent profile ● On track to become an IETF standard	● Not yet a good story around HoK/Proof of Possession ● Lots of options mean divergent implementations unless we define accepted profiles to limit complexity across the industry

OpenID Connect	● Builds on and standardises some of the shoulds in OAuth 2.0 ● Makes use of JWTs ● Introduces an identity token that helps the parties validate the legitimate user of the services ● OpenID is on track to be an accredited IETF standard	● Not yet an accredited IETF standard

Appendix 7. Governance rights of and obligations between participants

Please refer to Chapter 7c: Security for context.

1. Discovery

Table A7.1 Discovery

From To	Government, regulators, industry bodies and other relevant third parties	Independent authority	Data providers	3PPs	Customers
Government, regulators, industry bodies other relevant third parties		A central standards website from which all parties can access relevant, up to date and complete information relating to the operation of the overall ecosystem and the related participants and bodies Relevant content for inclusion on government/regulators’ websites and other third-party websites			

Independent authority	Relevant content, as requested, for inclusion on the central standards website Up to date, relevant and accurate content on their own website(s) about the standards and the ecosystem including a link to the central standards website. Content will be defined by/agreed with the independent authority and hence consistent with other details shown elsewhere		Relevant content, as requested, for inclusion on the central standards website	Relevant content, as requested, for inclusion on the central standards website	

Data providers		A central standards website from which data providers and their customers can access relevant, up to date and complete information relating to the operation of the overall ecosystem and the related participants and bodies Relevant content for inclusion on data providers’ own websites Clarity about the process that will apply to ensuring that content is provided where relevant by data providers and that the content is up to date, relevant and accurate			

3PPs		A central standards website from which 3PPs and their customers can access relevant, up to date and complete information relating to the operation of the overall ecosystem and the related participants and bodies Relevant content for inclusion on 3PPs' own websites Clarity about the process that will apply to ensuring that content is provided where relevant by 3PPs and that the content is up to date, relevant and accurate			
Customers		A central standards website that customers can access directly or via a link from government, regulators, data providers or 3PPs' websites, which will contain relevant, up to date and complete information relating to the operation of the overall ecosystem and the related participants and bodies Process of ensuring that information is provided by data providers and 3PPs where required and that the content is up to date, relevant and	Up to date, relevant and accurate content on their own website(s) about the standards and the ecosystem including a link to the central standards website. Content will be defined by/agreed with the independent authority and hence consistent with other details shown elsewhere	Up to date, relevant and accurate content on their own website(s) about the standards and the ecosystem including a link to the central standards website. Content will be defined by/agreed with the independent authority and hence consistent with other details shown	

		accurate		elsewhere	

2. Initial engagement

At the initial engagement stage, data providers will be able to obtain additional information and support that would include, for example, access to:

- details about the overall operation of the ecosystem, the role of the independent authority and the role and composition of the other related bodies and other participants;
- the technical details of the open data and open API standards;
- details of the SLAs/obligations between participating data providers and 3PPs;
- details of the rights of participants;
- details of the role of the independent authority and to whom it is ultimately responsible;
- details about the costs of participation;
- details of the sanctions that will apply for non-conformance to the standards and other SLAS/obligations (including existing regulatory provisions);
- a comprehensive set of FAQs covering questions of particular importance to data providers such as:
    - how do the standards and ecosystem overlap with or align with PSD2?
    - where does the consumer see liability falling?
    - how do banks ensure that data is secure?

  - how does the independent authority ensure that the 3PP has accreditation status in real or near real time?
  - what does the vetting and accreditation process cover?
  - what is the dispute resolution model?
  - what level of commitment is needed to maintain to 3PPs?
  - do 3PPs also have a duty of care to customers? If so, how is that enforced?
  - how does this governance process impact on “closed” APIs (including as the standard evolves)?
  - are the standards secure enough (particularly if they are below what is already in place)?
  - what is the benchmark standard? Has it been defined and how can it be divided up for products of single products, rather than applied as it would be applied to a bank with its full panoply of products, e.g. Squirrel?
  - does open data have to be standardised?
  - does open data have to be provided via an API?
  - what timeframes will apply for providing open data?
  - how or will requests for new open data from 3PPs be processed?
  - could an open data standard restrict innovation?
  - what service levels will apply regarding the provision of open data?
  - how will we handle the increased customer and 3PPs queries regarding open data?
  - how will we know who has accessed our open data if the access is not directly through my portal?
  - do we have to provide open data to a sandbox environment?
  - how can we be assured that solutions provided by a 3PP using our open data are reliable and accurate?
- a helpline number, contact details, email address and phone numbers for further questions.

For 3PPs, this additional information and support will include, for example, access to:

- details about the overall operation of the ecosystem, the role of the independent authority and the role and composition of the other related bodies and other participants;
- the technical details of the open data and open API standards;
- details of the SLAs/obligations between participating data providers and 3PPs;
- details of the rights of participants;
- details of the role of the independent authority and to whom it is ultimately responsible;

- details of the sanctions that will apply for non-conformance to the standards and other SLAs/obligations (including existing regulatory provisions);
- details about the criteria, process and costs applicable to participation including organisation accreditation and solution vetting;
- details about access to and use of the central and data provider's sandboxes;
- access to the relevant application forms;
- details about the SLAs applicable to the accreditation and vetting processes;
- a comprehensive set of FAQs covering questions of particular importance to 3PPs such as:
    - where do 3PPs access information about rights of access?
    - who do 3PPS need to apply to for access?
    - what do they need to become eligible?
    - how quick and easy is the process to be accredited?
    - how quick and easy is the solution vetting process?
    - are there any restrictions/prerequisites for 3PPs in gaining access to open APIs?
    - how will we be informed if new or updated data is available?
    - how will we be informed if new data providers are on board?
    - does it matter where 3PPs are based, e.g. the UK, EEA or outside EEA?
    - does it matter where data is stored, e.g. the UK, EEA or outside EEA?
    - how can I request a new data set (outside of standard APIs) or different format?
    - how can I ensure that I am protected (insurance) without it costing vast sums (smaller players), i.e. removing barriers to entry?
    - what happens if a 3PP is not or cannot get accredited, e.g. can they (still) use APIs to access data on behalf of customers?
    - what happens if accreditation is withdrawn, or a product is blacklisted?
    - what costs, if any, will be incurred in applying for accreditation and vetting?
    - will data providers comply with the SLAs and/or discriminate between participants and if so what levers do the governance arrangements provide to ensure compliance?
    - I am a small start-up – will the same requirements be imposed on me as on bigger, established companies?
    - how do I get access to sandbox environments – will be there one sandbox, or many?
- a helpline number, contact details email address and phone numbers for further questions.

For customers, this additional information and support will include, for example, access to:

- details of the type of solution and services that are available and from whom;
- how they can identify vetted 3PPs and accredited solutions/services (whitelist/kitemark details);
- a comprehensive set of FAQs covering questions of particular to customers such as:
    - how do I understand what benefit solutions developed by 3PPs will provide to me/my business, e.g. comparing different products, more informed decisions/choice?
    - how do I reassure myself of the reliability/trustworthiness of the 3PPs and the solutions/apps they provide, e.g. can I access ratings?
    - for how long do I give access to my data?
    - to which data do I grant access?
    - where and how do I grant access?
    - how can I access details about to whom I have given access, when, to what and for what purpose?
    - how do I withdraw/control access?
    - where do I go in case of issues?
    - if I have suffered damage as a result of using a solution delivered by a 3PP, to whom do I go?
    - if my data provider does not enable me to gain access to my data in order to use an approved 3PP, to whom do I go?
    - for solutions using only open data:
        - can I trust the data presented?
        - do I understand the data presented?
        - does the data presented meet my needs and can I act upon it?
        - has my privacy been taken into account?
        - if I have questions, to whom do I go?

The independent authority will play a key and central role in establishing the ecosystem to ensure it performs as set out, providing access to the relevant information and support necessary for all participants including but not limited to:

- accreditation and vetting submissions from 3PPs – ensuring that these are handled quickly and effectively and that any third parties engaged in the process, e.g. access organisations, standards bodies, perform their role in accordance with defined SLAs;
- queries arising from any participant.

Table A7.2 Initial engagement

From To	Government, regulators, industry bodies and other relevant third parties	Independent authority	Data providers	3PPs	Customers

Government, regulators, industry bodies and other relevant third parties		ToR for the independent authority and related bodies A clearly defined and effective set of risk-based SLAs applicable to all participants A clearly defined and effective process for handling queries, complaints or appeals arising from the performance of any participant against the SLAs Clear details of the sanctions that will apply in the context of persistent/egregious SLA breaches A working sandbox environment Clearly defined and effective risk-based processes for the accreditation of organisations and the vetting of 3PP solutions A clearly defined and effective process for handling queries, complaints or appeals arising from the accreditation/vetting process Clearly defined and effective processes through which 3PPs can request the addition of other data to the standard FAQs for all	APIs delivered in accordance with the standards and the defined SLAs	Solutions/services delivered in accordance with the standards	

		participants			

Independent authority	Mandate to operate Funding?		APIs developed, tested and delivered in accordance with the standards and the defined SLAs Contact for queries arising	Solutions/services developed, tested and delivered in accordance with the standards and the defined SLAs Contact for queries arising	
Data providers		As above, plus: A comprehensive set of FAQs covering questions of particular importance to data providers		Solutions/services delivered in accordance with the standards and the defined SLAs Helpdesk access/clear point of contact for queries arising	
3PPs		As above, plus: A comprehensive set of FAQs covering questions of particular importance to 3PPs	APIs developed and tested in accordance with the standards and the defined SLAs API access delivered in accordance with the standards and the defined SLAs Helpdesk access/clear point of contact for queries arising		

Customers		Additional relevant information on the central website including: ● details of the type of solution and services that are available and from whom ● how they can identify vetted 3PPs and accredited solutions/services (whitelist/kitemark details) ● a comprehensive set of FAQs relevant to customers	APIs delivered in accordance with the standards and the defined SLAs Clear advice and guidance in relation to transfer of data to 3PPs (in line with independent authority guidelines) Helpdesk access for queries arising	Solutions/services delivered in accordance with the standards and the defined SLAs Clear advice and guidance in relation to how the 3PP will use and look after customer data (in line with independent authority guidelines) Helpdesk access/clear point of contact for queries arising	

3. Active engagement

For data providers, this includes but is not limited to:

- providing 3PPs with timely and effective responses to legitimate API calls;
- providing 3PPs with support contact details should queries arise;
- providing customers with the ability to transfer their data to a 3PP.

For 3PPs, this includes but is not limited to:

- the presentation of clear, fair and transparent terms and conditions to the customer.

For customers, this includes but is not limited to:

- reading and accepting the terms and conditions presented by the 3PP for the service/solutions being provided;
- where relevant, providing their consent to the transfer (either one-off or ongoing) of their data from the data provider to the 3PP;
- the actual use of 3PPs' service/solutions.

Table A7.3 Active engagement

From To	Government, regulators, industry bodies and other relevant third parties	Independent authority	Data providers	3PPs
Government, regulators, industry bodies and other relevant third parties				
Independent authority				
Data providers		Enforce security standards Ensure use of data is fair and accurate Whitelist and PSD2 list Dispute resolution		Point of contact Store data security once shared Inform data breaches
3PPs		Enforce SLAs Enforce security standards Sandbox Dispute resolution	Point of contact Quality of data provided through API Security, reliability and scalability of API Open, non-discriminatory access Inform data breaches	
Customers		Trust and confidence Dispute resolution	Clearly written guidance Provision of secure API in accordance with standard and consent Visibility of consents and ability to retract Point of contact in	Provide fit-for-purpose solutions Store data securely once shared Point of contact in case of issues

			case of issues	

4. Issue resolution

Table A7.4 Resolution

From To	Government, regulators, industry bodies and other relevant third parties	Independent authority	Data providers	3PPs
Government, regulators, industry bodies and other relevant third parties				
Independent authority				
Data providers		Point of contact for escalation Dispute resolution		Point of contact in case of issues
3PPs		Point of contact for escalation Dispute resolution Deny access	Point of contact in case of issues	
Customers		Point of contact for escalation	Point of contact in case of issues	Point of contact in case of issues

		Dispute resolution		

Appendix 8. Existing data standards

There are a number of existing data standards. Two of the main ones are International Standards Organisation (ISO) standards and W3C standards. Other such examples are CEN and BSI.

ISO data standards

ISO as a standards organisation has a wide range of industry standards that are relevant to the financial services industry and are widely used. The relationship between the Open Banking API Framework and ISO is both as a user of ISO standards, as well as a contributor. For example, some ISO standards, such as country codes or currency codes, could be used within the Open Banking Data Standard. Concepts of more complex data semantics and data structures, such as an account, could be taken from the ISO 20022[31] financial repository and missing structures of information could be contributed to the ISO 20022 organisation to define a version of the Open Banking reference data model in the ISO 20022 Financial Repository. Note that usage of the ISO 20022 Financial Repository is according to RAND principles; it is not restricted, does not involve cost and is freely and publically available.

ISO is an independent, non-governmental organisation made up of members from the national standards bodies of 165 countries. It develops international standards through its worldwide network of national standards bodies. Work is performed within technical committees, their subcommittees and working groups. ISO develops standards in 263 areas including technology, product safety, energy management and more. The ISO standards development process is carried out through experts participating in committees and working groups. As a result, the agreement/approval of a standard reflects a double layer of consensus – first within the industry (market players) and then across ISO member countries. Formal governance is published in a rulebook titled ISO Directives.[32]

W3C standards

Most W3C work revolves around the standardisation of Web technologies. To accomplish this work, W3C follows processes that promote the development of high-quality standards based on the consensus of the community. W3C processes promote fairness, responsiveness and progress: all facets of the W3C mission.

The W3C technical report development process is the set of steps and requirements followed by W3C working groups to standardise Web technology. Through this process, W3C seeks to maximise consensus about the content of a technical report, to ensure high technical and editorial quality, to promote consistency among specifications and to earn endorsement by W3C and the broader community.

[31] see https://www.iso20022.org/intellectual_property_rights.page)

[32] www.iso.org/directives

Appendix 9. Landscape of open bank APIs

1. Existing open bank API – Open Bank Project

Open Bank Project (OBP) is an open source API for banks that provides RESTful JSON interfaces aimed at customer-centric retail banking applications that require access to resources such as customer information, accounts, transactions, payments, entitlements and related metadata as well as open data such as bank branches, ATMs and products. It natively supports both account "owner" and guest access. Delegated authentication by default is via OAuth 1.0a. OBP has a connector layer that abstracts away differences in core banking systems (via Kafka MQ, JDBC, REST and SOAP etc). A sandbox connector provides a simple "bank in a box" functionality without any connection to core banking required.

TESOBE Ltd (a UK company with an independent subsidiary, TESOBE Ltd, Germany) has funded the OBP since early 2010 and owns the IP.

The core OBP API software is dual-licensed under the AGPL and commercial licences, which enables banks to either use the source code for free as long as they abide by the AGPL or fork the code base without restriction and receive commercial support from TESOBE and its partners.

Other OBP repositories are licensed under AGPL or Apache licences. TESOBE anticipates licensing the specification of the OBP API under Creative Commons Attribution-ShareAlike CC-BY-SA.

OBP assets include the following:

- API (allows a bank to plug on top of its core banking)
    - Source code: https://github.com/OpenBankProject/OBP-API/
    - Example: https://apisandbox.openbankproject.com/
    - Standard: https://github.com/OpenBankProject/OBP-API/wiki/REST-API-V1.4.0
    - Architecture: https://github.com/OpenBankProject/OBP-API/wiki/Open-Bank-Project-Architecture
- Sandbox (so developers can test, no connection to core banking required)
    - Instructions: https://github.com/OpenBankProject/OBP-API/wiki/Sandbox
- API Explorer (lets developers interact with API)
    - Source code: https://github.com/OpenBankProject/API-Explorer
    - Sandbox example: https://apiexplorersandbox.openbankproject.com/
- Social Finance - a reference application using the API
    - Source code: https://github.com/OpenBankProject/Social-Finance
    - Live example: https://sofi.openbankproject.com/
- Client SDKs (Python, Node.js, IOS, Android etc)

  - Links to source code: https://github.com/OpenBankProject/OBP-API/wiki/OAuth-Client-SDKS

- Docker image (allows developers to easily run locally)
  - Download: https://hub.docker.com/r/openbankproject/obp-full/
  - Fork: https://github.com/OpenBankProject/OBP-Docker

2. Existing public bank API – Fidor Bank

Fidor Bank AG is a fully licensed online bank, located in Germany and the UK with global partnerships and customers. Fidor TecS AG is a 100% subsidiary company that provides banking software (FidorOS) and services to Fidor Bank and other companies (banks and non-banks).

Fidor has provided public RESTful APIs since 2014 for the following major use cases:

1. Allowing existing bank customers to “remote control” their own data, accounts and use-related banking services;
2. Enabling third-party service providers (3PPs) to offer all kind of services (apps) to the bank customers, including access to customer and account data if the account holder gives their consent (technically based on OAuth2);
3. All current and future front-end development (mobile, Web, back office, branch terminals, etc) for Fidor Bank and all white label banking customers (no-stack banking) use the very same APIs.

For API discovering, testing and debugging, Fidor offers publicly accessible documentation (http://docs.fidor.de/ and https://developer.fidor.de/api-browser/), a developer community forum (https://developer.fidor.de/) and an application management environment with starter kits and sandbox (https://apm.fidor.de/). Depending of the type of application and scope of API usage, existing bank customers may even self-approve their application in order to switch to production systems.

GitHub resources:

- Documentation: https://github.com/fidor/api-docs
- API Schema: https://github.com/fidor/fidor_schema
- Starter kits: https://github.com/fidor/fidor_starter_kits

Appendix 10. International case studies

While the development of the open API could provide UK consumers and SMEs with innovative products not provided in any other market, there have been some successful international attempts at opening up banking data. These demonstrate some of the potential benefits that users in the UK could access. The development of an open API in the UK should, where possible, build on lessons from these attempts and seek to deliver the same value to UK users. This report illustrates two case studies.

1. Germany – Homebanking Computer Interface (HBCI)

HBCI was originally designed by the two German banking groups Sparkasse and Volksbanken und Raiffeisenbanken and German higher-level associations such as the Bundesverband deutscher Banken e.V. It is now managed by ZKA.[33] The result of this effort was an open protocol specification that is publicly available and supported by more than 2,000 financial institutions in Germany. The standardisation effort was necessary to replace the huge number of deprecated homemade software clients and servers. It has allowed the launch of a number of innovative services and service delivery approaches by financial institutions (such as Figo, Fidor Bank and the OBP etc.).

Fidor has been at the forefront of providing APIs in the German banking industry. It has developed an open approach where developers can access a sandbox and get to know the Fidor API. They can subsequently get in touch with Fidor to start using the APIs to enhance their own operations or to build applications for other consumers. One example is a product developed by Currency Cloud, a B2B international payments engine inside countless financial firms in partnership with Fidor. Fidor Bank's unique API allows Currency Cloud to more seamlessly integrate direct debits into its own payment processes and those of its customers. The new capability means Currency Cloud can provide a complete, end-to-end payment solution for its customers, from receiving funds to foreign exchange conversion and fund payout.

Where individual aspects of the payment lifecycle have traditionally been handled by specialist providers, forcing companies to work with multiple suppliers, Currency Cloud customers can now benefit from a one-stop, joined-up process. Take-up of the direct debit functionality has been strong since its soft launch in May – Currency Cloud is already processing thousands of transactions through Fidor's API.

The new feature will allow Currency Cloud's customers to pull funds directly from end-users' accounts with a "continuous authority" payment agreement, avoiding the high costs that the card schemes usually demand for this service.

2. France – Credit Agricole App Store

French bank Credit Agricole launched the CAStore in January 2012, an online marketplace that essentially crowdsources ideas for new banking applications from customers and gives developers the technological tools they would need to create apps that either fulfil the wishlist or are based on ideas they've dreamed up themselves.

[33] See http://www.hbci-zka.de/english

The financial application marketplace has proven to be something of a showpiece for what can happen when the banking industry works with third parties on technology advancements.

The CAStore uses an open API, in which technology is shared freely with outside developers so that it can be integrated into new programs, without compromising compatibility.[34]

One example of a solution developed using the Credit Agricole API is the “Whats-ThatLine” app developed by FinTech company Wassa. The app lets customers mark bank transactions that they have questions about and allows them to share the information with their financial advisers or any other contact they choose. The sharing application focuses on a very specific need that Wassa identified some customers have. The main rationale was to create a simple mobile solution for people who don't always need huge dashboards full of numbers when checking their account, but just want to check if everything is fine with their account.[35]

[34] See https://www.creditagricolestore.fr/castore-data-provider/docs/V1/index.html

[35] See http://www.americanbanker.com/magazine/123_8/open-api-for-bank-apps-can-credit-agricoles-model-work-1060535-1.html

Glossary

3rd Party App (3PApp): A software application provided by a 3PAP.

3rd Party App Provider (3PAP): Provides a software application that runs on the user's device (e.g. smartphone or PC) and makes use of the API (client-side) to access user data but does not process or store it anywhere other than on the user's device.

3rd Party Provider (3PP): A counterparty making API requests, with the end intention of providing a product or service to a user (as defined above). These counterparties can be both FinTechs and existing banks and financial service providers. Either a 3PAP or a 3PSP.

3rd Party Service Provider (3PSP): Provides a service (and, optionally, a software application to interact with that service) that makes use of the API (client-side) to access user data, and processes (and, optionally, stores) it on the 3PSP's servers. e.g. mint.com.

Access token: An access token contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges and, in some cases, a particular application.

Account-Servicing Provider (ASP): A current provider of financial services (e.g. banks) that manages existing customer accounts and retains and hosts customer data that could be made available upon consent through APIs; and therefore in the context of OBWG - will likely act as a data attribute provider.

Aggregated data: Sets of averaged or aggregated data across transactions, balances or other data. No individual customer data discernible (at least in principle - see Chapter 9, Regulatory and Legal). Examples include: average number of cash withdrawals per month across a group of customers.

API: Application programming interface. It is a means of accessing data based on a standard. The data accessed via an API may be closed, shared or open data.

APX: API developer experience.

Authentication: The process by which one party proves their identity to another.

Authorisation: The process of granting permissions to another party to carry out certain activities (NB: Not FCA-style authorisation).

Big data: A vendor-driven term often used to describe large quantities of rapidly changing data being collected from various sources.

Closed data: Data that can only be accessed by its subject, owner or holder.

Customer-facing data (non-public): Data and attributes about account use for an individual data subject's account

Customer-related data (non-public): Data about a data subject not directly related to the use of an account. Examples include data relating to a customer derived from KYC/KYB processes, AML checks or credit score checks.

Data attribute provider: The counterparty who is responding to an API request for information, or who is publishing a set of Open Data to the market. These will include ASPs.

Data subject: The personal or commercial party who is the subject of the data.

Deprecation: Deprecation is an attribute applied to a computer software feature, characteristic, or practice to indicate that it should be avoided (often because it is being superseded).

End-user device (EUD): An end-user device is any device such as a computer, smartphone or tablet that a person can use to store digital information. Other examples of an EUD are a personal digital assistant, or removable storage media such as a USB flash drive, memory card, external hard drive, writeable CD or DVD).

General Data Protection Regulation: The GDPR is a single law that the European Commission plans to unify data protection within the EU.

Governance standard: Documents that describe the procedures, processes, rules and operation of the independent authority, including, but not limited to, decision-making, roles and responsibilities, and participation.

Group-based access: Data that is made available to special groups or people who meet certain criteria with their access authenticated.

Internal access: Access to data that is limited to those inside an organisation or team.

JSON: A lightweight format that is easy for computers to parse and generate, and relatively easy for humans to read and write. It is programming language-independent, and is widely adopted.

Legal entity identifier (LEI): A unique 20-character alphanumeric code based on the ISO 17442 standard developed by the International Organization of Standardization, which is assigned to legal entities that are counterparties to financial transactions. The LEI code itself is neutral, with no embedded intelligence or country codes that would create unnecessary complexity for users.

Named access: Data that is shared with specific people or organisations for a specific purpose, typically explicitly assigned in a contract.

OBWG Data Standard (reference data model): Describes a standardised ontology of business data semantics, data elements and data types. It is a standardised representation of the data in scope of the Open API Standard.

Online Certificate Status Protocol: OCSP is an internet protocol used for obtaining the revocation status of an X.509 digital certificate.

Open API: A public interface that provides a means of accessing data based on an open standard. The data accessed via an open API may be closed, shared or open data.

Open API Standard: An open standard is developed and maintained collaboratively and transparently, and can be accessed and used by anyone. The OBWG Authority will be responsible for ensuring that the Open API for banking will be developed in this manner.

Open data: Data that anyone can access, use and share. For data to be considered “open”, it must be: accessible, which usually means published on the Web; available in a machine-readable format; and have a licence that permits anyone to access, use and share it – commercially and non-commercially.

Out-of-band (OOB): Out-of-band is activity outside a defined telecommunications frequency band, or, metaphorically, outside some other kind of activity such as a separate stream of data from the main data stream, or user authentication over a network or channel separate from the primary network or channel; used in multi-factor authentication.

Patent rights: Patent rights are defined as patents, utility models and other statutory rights based on inventions, including any published applications for any of the foregoing.

Payment Services Directive: The EU’s 2007 Payment Services Directive (PSD) regulates payment services and payment service providers throughout the EU and EEA. Its purpose is to increase pan-European competition and participation in the payments industry, including the involvement of non-banks, and to provide for a level playing field by harmonising consumer protection and the rights and obligations for payment service providers and users. PSD2 is in progress.

Permissions: Rules that grant access to data (e.g. an account balance) or functions (e.g. the ability to instruct a payment).

Personal data: Data from which a person can be identified (as per UK Data Protection Act definition). Note: personal data can be closed, shared with specific people or organisations, or made public.

Proprietary data: Sensitive data including documents, strategy, price-setting, policies and algorithms that are not in scope for the OBWG. At a data subject level, this may include data about overall customer portfolio performance or bank profitability that reveals proprietary or competitive insight about a player's performance, e.g. the average credit score across a customer population, average margin.

Public access: Data that is available to anyone but not under terms and conditions that are open. Usage may be restricted by either the terms and conditions, or the licence, e.g. data may only be used for non-commercial purposes, data may not be adapted etc.

RAND: Reasonable and non-discriminatory terms. There is currently no universally agreed definition.

Read access: Permission that is granted to a counterparty/counterparties enabling them to read but *not* modify a file, set of files, set of data.

REST (REpresentational State Transfer): REST is a lighter-weight alternative to SOAP that describes the architectural style of the Web. So-called RESTful APIs follow REST style and use URIs to address resources, HTTP methods and headers for actions, and representations for transferring state.

Roles: Collections of permissions.

Service level agreement: A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end-user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.

Shared data: Data that is shared specifically with named individuals and organisations, specifically with groups that satisfy certain criteria, or anyone else, but under terms and conditions that are not open. Named access, group-based access, and public access are three types of shared data.

SOAP (Simple Object Access Protocol): A popular and standardised RPC protocol originally developed by Microsoft as a replacement for older technologies that weren't optimised for the internet. SOAP is based on XML, which works better over the internet than older RPC protocols that used binary messaging.

Two-factor authentication (2FA): Two-factor authentication (also known as 2FA or 2-Step Verification) is a technology that provides identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. For example, to withdraw money from a cash machine, only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.

User: A user of (and/or account holder of) commercial products or services offered through digital channels. For the purposes of this report these will primarily relate to financial services propositions.

Vishing: Voice phishing (vishing) is the criminal practice of using social engineering over the telephone to gain access to private personal and financial information from the public for the purpose of financial reward. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Write access: Permission that is granted to a counterparty/counterparties to modify or execute a file, set of files, set of data. In the context of work conducted by the OBWG, write access includes payment initiation.

Acknowledgements

Editor

Louise Bolotin

Open Banking Working Group

Steering Committee

Chairs: Matt Hammerstein (Barclays), Gavin Starks (ODI)

Claire Calmejane (Lloyds Banking Group), Christophe Chazot (HSBC), Kate Frankish (Tesco Bank), Imran Gulamhuseinwala (EY), Paul Hollands (RBS), Guy Levin (Coadec), Andy Maciver (Financial Data and Technology Association), John MacLeod (Santander UK), Patrick Mang (HSBC), Nick Middleton (Nationwide Building Society), Matt Stroud (Digital Catapult), Chris Taggart (OpenCorporates), Cameron Yorston (HMT).

Secretariat

Rhiannon Butterfield (Payments UK), Daniel Cichocki (BBA), Irene Graham (Scale-up Institute (current); BBA (former)), Sameer Gulati (Innovate Finance), Matthew Herbert (BBA), Henry Kuang (EY), Walter McCahon (BBA), Dan Morgan (Innovate Finance).

Sub-group: User reference

Chairs: Peter Baeck (Nesta), Jason O'Shaughnessy (Yodlee)

Simon Alderson (Handelsbanken), Toby Bateman (CBI), Paul Beard (Credit Safe), Louise Beaumont (GLI Finance), Tom Blomfield (Mondo), Mark Bradbury (Apply Financial), Glenn Collins (ACCA), Judith Crawford (Electronic Money Association), James Dear (iwoca), Erin Flood (Federation of Small Business), Marcus Gruenwald (FinPoint), Vicki Harris (Aldermore), Andrew Hopkins (Building Societies Association), Stephan Hurlotz (Fidor Bank), Saket Jasoria (Lloyds Banking Group), Guy Levin (Coadec), Clive Lewis (ICEAW), John MacLeod (Santander), Michael Maier (Fidor Bank), Duncan McEwen (UK Cards Association), Eric Mouilleron (Bankable), Carl Pheasey (Money Advice Service), Dan Posner (Barclays), Simon Redfern (Open Bank Project), Mark Rosel (Capital One), Giles Sergant (Atom), Suren Thiru (Chamber of Commerce), James Varga (MiiCard), Sarah Williams-Gardener (Starling Bank).

Sub-group: Governance

Chairs: Fedelma Good (Barclays), John Midgley (Intuit)

Louise Beaumont (GLI Finance), Adrian Black (Contego), Mark Bradbury (Apply Financial), Claire Calmejane (Lloyds Banking Group), Serge Eaton (HSBC), Jan Heinsbroek (SWIFT), Louise Johnston (Tesco Bank), Sarah Lynch (JPM), James McMorrow (Lloyds Banking Group), Eric Mouilleron

(Bankable), Jason O'Shaughnessy (Yodlee), Giles Watkins (Digital Catapult), Nicholas Webb (FCA, observer), Phil Whelan (ThinkMoney), Sarah Williams-Gardener (Starling Bank), Stephen Wright (RBS).

Sub-group: Data

Chairs: Gary Sanders (Lloyds Banking Group), James Varga (MiiCard)

Liz Brandt (Ctrl-Shift Ltd), Garreth Cameron (ICO, observer), Christophe Chazot (HSBC), James Dear (iwoca), Justin Fitzpatrick (DueDil), Bernie Grady (Experian), Jo Green (Santander), Nick Hall (Barclays), Celia Hannon (Nesta), Stuart Lang (EY), Ian Major (Runpath), Patrick Mang (HSBC), Andy McComb (Danske Bank), Lorraine McDerment (Clydesdale Bank), Rob McKendrick (EY), Nick Middleton (Nationwide), John Rendle (RBS), Mark Rosel (Capital One), Chris Taggart (Open Corporates), Leanne Willis (AIB).

Sub-group: Security and authentication

Chair: Simon Grant (Santander), Jack Gavigan (Gavigan Consulting)

Kevin Barron (HSBC), Mark Bradbury (Apply Financial), Barry Glenn (Clydesdale Bank), Jez Goldstone (Barclays), Ali Imanat (FFA UK), James Kent (Leeds Building Society), Ben Lindgreen (Payments UK), Dimitrios Marakakis (Flawless Money / EMA), David McRoberts (Virgin Money), Adam Moulson (SWIFT), Mark Stanhope (Paym), Matt Stroud (Digital Catapult), Rob Tharle (TSB), Dave Tonge (Momentum), Simon Vans-Colina (Mondo), Damian Ward (Vocalink).

Sub-group: Standards and technical design

Chairs: John Phenix (Barclays), James Whittle (Payments UK / ISO)

Oliver Beattie (Mondo), Diane Beddingfield (ThinkMoney), Philip Clark (Santander), Becky Clements (Metro), Nick Fleming (British Standards Institute), Allan Flint (Tesco), Julian Gevers (Lloyds Banking Group), Kevin Hart (BASDA), Mark Hartley (Clear2Pay), Mike Kelly (Stateless Consulting), Stephen Lindsay (SWIFT), Dimitrios Marakakis (Flawless Money / EMA), Michele Nati (Digital Catapult), Simon Redfern (Open Bank Project), Chris Taggart (Open Corporates), James Tasker (RBS), James Varga (miiCard), Jonathan Vokes (Worldpay), Damian Ward (Vocalink), Stefan Weiss (Fidor Bank), Lu Zurawski (ACI).

Sub-group: Regulation and legal

Chair: Paul McCormack (HSBC), Patrick Mason (Tesco Bank)

Wendy Allen (Metro Bank), Adrian Black (Contego), Garreth Cameron (ICO, observer), Elena Fiorio (Bankable), Qazi Jalisi (E-MA), Vedrana Kovacevic-Jalisi (E-MA), Deborah Mackay (Clydesdale Bank), John Midgley (Intuit), Eric Mouilleron (Bankable), Lisa Moyle (Tech UK), Polly Quinn (Bank of America ML), Kate Shattock (Santander), Ruth Wandhofer (Citi), Nicholas Webb (FCA, observer), Sharon Williamson (Danske Bank), Justine Wootton (Barclays), Tomas Xavier (Nationwide).

Sub-group: Communications team

Henry Kuang (EY), Andy Maciver (FDATA), Sanjay Odera (BBA), Anna Scott (ODI), Gavin Starks (ODI), Emma Thwaites (ODI), Adam Tresolve (Tesco Bank).