OPEN BANKING

Open Banking

Guidelines for Read/Write Participants

Date: May 2018
Version: 3.2
Classification: PUBLIC

1 Introduction

1.1 Background

In the 2015 Budget, Her Majesty's Treasury (**HMT**) announced its commitment to delivering an **open standard** for **Application Programme Interfaces** (**APIs**) and data sharing in UK Retail Banking (commonly referred to as **Open Banking**) as a measure to increase the opportunity for competition in the retail market with the ultimate aim of improving outcomes for customers of the UK banking industry.

Following on from HMT's announcement, in May 2016 the Competition and Markets Authority (**CMA**) published a provisional decision on **remedies** it deemed appropriate to introduce to address a number of key features of the UK Retail banking market considered to be having an adverse effect on competition. These remedies included a requirement for the UK banking industry to adopt a subset of HMT's proposals for Open Banking.

In August 2016, the CMA published its final report on its investigation into the UK Retail Banking market, entitled Retail Banking Market Investigation: Final report. This report mandated the implementation of a number of core proposals as foundation remedies and resulted in the creation of the Retail Banking Market Investigation Order 2017 (also known as The **CMA Order** and hereafter referred to as "the Order").

The Order mandated the delivery of an open and common banking standard to allow for the following:

- The release of reference information via Open Data APIs, to include:
    - all branch and business centre locations;
    - all branch opening times;
    - all ATM locations
- The release of specific product information via the Open Data APIs, to include:
    - Product prices
    - All charges (including interest)
    - Features and Benefits
    - Terms and Conditions and customer eligibility
- The release of Personal Current Account and Business Current Account transaction sets via Read/Write APIs, to allow:
    - Access to account information at the request of a customer by a third party provider
    - The Initiation of a payment from a customer's account at the request of a customer by a third party provider.

The Order also specified the product types and specific data items which the Standard for access to account information was required to include:

- The 'Read/Write Data Standard' which has the features and elements necessary to enable Providers to comply with the requirements to provide access to accounts subject to Part 2 of the Order under PSD2

and further mandated delivery of:

- whitelisting as a system for approving third party providers fairly and quickly;
- governance arrangements

The **Open Banking Implementation Entity** (OBIE) was created in line with the terms of the Order to develop and deliver the open and common banking standards for APIs as detailed within the Order and to work with the industry and to implement and maintain those Standards.

In the 2017 Budget, HMT announced that the OBIE will now be creating Standards for all payment account types covered by PSD2. This means customers using credit cards, e-wallets and prepaid cards could also take advantage of Open Banking services. In parallel, the CMA approved amendments to the agreed arrangements under the CMA Order to include a programme of enhancements to ensure that Open Banking delivers maximum benefits for retail customers and SMEs.

The full details of the enhancements can be accessed on the Open Banking website at www.openbanking.org.uk.

1.2 About Open Banking

Open Banking enables Account Servicing Payment Service Providers (known as ASPSPs) including banks and building societies, to allow their personal and small business customers to share their account data securely with third party providers. This enables those third parties to provide customers with services related to account information such as product comparison or payment initiation using the account and product information made available to them.

This is achieved by the development, maintenance and publication of Standards for Application Programming Interfaces (APIs). APIs are an established technology that uses defined methods of communication between various software components; they are used by many well-known online brands to share information for a variety of purposes.

March 2017 saw the introduction of the first Open Banking Standards for APIs to support access to defined elements of **Open Data,** as defined in the CMA Order, specifically information on ATM and Branch locations, and product information for Personal Current Accounts, Business Current Accounts (for **SMEs**), and SME Unsecured Lending, including Commercial Credit Cards.

As required by the CMA Order, this was followed in July 2017 by the release of further API Standards for **Read/Write Data** that enabled Participants to publish API end points which must be functional by 13 January 2018. These additional Read/Write API Standards enable third party providers, with the end customer's consent, to request account information such as the transaction history of Personal and Business Current Accounts and/or initiate payments from those accounts.

Following the 2017 Budget, announcement a programme of releases to build on the core requirements of the CMA Order will be implemented throughout 2018 and into 2019.

1.3 About the Open Banking Implementation Entity

The OBIE is the custodian of the Open Banking Standards for APIs and owns and maintains the **Directory of Open Banking Participants** (also referred to as the **Directory**), which provides a "whitelist" of Participants able to operate in the Open Banking Ecosystem, as required by the CMA Order.

OBIE is responsible for:

- The prescribed format for the Open Banking Standards for APIs and associated documentation and artefacts
- The governance processes for how the prescribed format is managed, including change and release management
- The support structures and processes for all users of the prescribed format, including the set up and operation of the Directory and its constituent components
- Any applicable **Terms and Conditions** for certain categories of Participants in Open Banking
- Any applicable **Guidelines** and other documents and artefacts for Participants of the **Open Banking Ecosystem**

The OBIE also maintains the Open Banking Ecosystem in which the Standards are used in accordance with relevant law and regulation, and creates security mechanisms and governance structures for Participants using the Open Banking Standards for APIs.

Currently the CMA Order requires Mandatory ASPSPs to fund the OBIE. However, it is envisioned that the funding model will likely evolve to diversify the funding base of the OBIE.

1.4 About the Guidelines

These Guidelines are owned and administered by the OBIE. The Guidelines describe and provide direction on the roles and responsibilities of Participants.

Where these Guidelines provide that a party or Participant (or other similar term relating to an entity to whom the Guidelines apply) “should” undertake an action or implement a process, compliance with the relevant guideline will be voluntary and non-compliance will not give rise to a breach of the Guidelines.

The document is split into sections covering:

- An Introduction to Open Banking
- The Open Banking Ecosystem
- Open Banking Security Standards
- Open Banking Standards
- Open Banking for Read/Write API Standards
- Maintaining the Integrity of the Directory
- Complaints and Disputes

These Guidelines should be read in conjunction with the following documents that together with these Guidelines form the suite of **Participation Conditions** which set out the contractual obligations operating between ASPSPs and the OBIE:

- the Terms and Conditions
- the Standards
- the Complaints and Dispute Resolution Procedure

- the Directory Service Level Agreement
- the Read/Write API Reporting and MI Service Level Agreement
- the Privacy Policy

The Open Banking Ecosystem is also governed by UK and European regulations including Revised Payment Services Directive (PSD2), General Data Protection Regulation (GDPR), Draft Regulatory Technical Standards (RTS) on Strong Customer Authentication, and the Payment Services Regulations (PSR). These Guidelines should therefore also be read in conjunction with that legislation and are intended to be both compliant with, and not construed as going beyond, existing legislation.

All Participants are solely responsible for their compliance with the relevant regulations applicable to their service offering and are encouraged to seek external legal advice. These guidelines are purely advisory and do not in any way constitute legal advice.

If you are unsure of the guidelines for Participants outlined within this document, including any specific questions on security and/or technical matters, please contact the Open Banking Service Desk at ServiceDesk@openbanking.org.uk.

Any changes to the Participation Conditions will be made in accordance with the OBIE change control process which includes consultation with relevant working groups.

Notice of any amendment or change to this document will be provided to Participants via the Open Banking website and remain on the website for at least 30 days from the date of publication.

2 The Open Banking Ecosystem

The Open Banking Ecosystem refers to all the elements that facilitate the operation of Open Banking. This includes the API Standards, the governance, systems, processes, security and procedures used to support Participants.

2.1 Read Write Data Participants

Account Servicing Payment Service Providers (ASPSPs)

ASPSPs are payment service providers who provide and maintain a payment account for a payer as defined by the PSRs and, in the context of the Open Banking Ecosystem, are entities that publish Read/Write APIs to permit, with customer consent, payments initiated by third party providers and/or make their customers' account transaction data available to third party providers via their API end points.

ASPSPs are split into two further categories: Mandatory ASPSPs and Voluntary ASPSPs.

Mandatory ASPSPs

Mandatory ASPSPs are entities that are required by the CMA Order to enrol with the OBIE as ASPSPs. The following entities are Mandatory ASPSPs under the CMA Order:

- AIB Group (UK) plc trading as First Trust Bank in Northern Ireland
- Bank of Ireland (UK) plc
- Barclays Bank plc
- HSBC Group
- Lloyds Banking Group plc
- Nationwide Building Society
- Northern Bank Limited, trading as Danske Bank
- The Royal Bank of Scotland Group plc
- Santander UK plc (in Great Britain and Northern Ireland)

Mandatory ASPSPs must publish APIs in accordance with the Standards, enrol onto the Open Banking Directory, and may use the associated OBIE operational support services.

Voluntary ASPSPs

Voluntary ASPSPs are those entities who, although not obliged to enrol with the OBIE, have elected to do so in order to utilise the Standards to develop their own APIs, to enrol onto the Open Banking Directory, and to use the associated operational support services.

Third Party Providers

Third Party Providers (TPPs) are organisations that use APIs developed to Standards to access customer's accounts, in order to provide account information services and/or to initiate payments.

Third Party Providers are either or both of the following types:

- Payment Initiation Service Providers (PISPs)
- Account Information Service Providers (AISPs)

A PISP is defined under PSRs, and for the purposes of Open Banking, as a payment service provider which provides payment initiation services, where payment initiation services means an online 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.

An AISP is defined under PSRs, and for the purposes of Open Banking, as a payment service provider which provides account information services, where account information services means an online service to provide consolidated information on one or more payment accounts held by the PSU with another payment service provider or with more than one payment service provider, and includes such a service whether information is provided—(a) in its original form or after processing;(b) only to the PSU or to the PSU and to another person in accordance with the PSU's instructions.

2.2 The Open Banking Directory of Participants

The Open Banking Directory is the key architectural component that enables Participants to enrol with the OBIE and participate in payment initiation and account information transactions through APIs. At its core the Directory is an identity and access management service providing identity information supporting natural persons, entities and software identity classes.

The Open Banking Directory will provide the necessary functional capabilities required for ASPSPs to provide whitelisted Participants with access to APIs, and for Participants that have been authorised or registered with their Competent Authority to enable them to identify and to facilitate on-boarding with ASPSPs so that they can use the APIs provided by the ASPSPs.

The functional capabilities can be broken up broadly into three capability groups:

- **Manage Identities and Access**: The ability to issue and manage identity records for entities and natural persons that interact with the Open Banking Directory
- **Manage Certificates**: The ability to issue, manage and revoke digital certificates
- **Manage Directory Information**: The ability to update and find information maintained in the Directory, either through APIs and / or a user interface delivered as a web application.

The requirements and process for enrolment to the Directory are described in the Read/Write Data section of this document.

3 Open Banking Security Standards

3.1 API Security Practice for Participants

All Participants must implement the Open Banking Security Standard. This defines how the Read/Write APIs need to be secured using a multi layered approach. The OAUTH 2.0 authorisation framework and Open ID Connect identity authentication are layered over mutually authenticated transport layer security (MATLS) to provide a robust and secure security profile. The Security Profile (the Open Banking Security Standard) is published on the Open Banking website at www.openbanking.org.uk and contains details on:

- UK Open Banking Security Profile
- Security Architecture
- JSON Security Suite Information
- Implementation Guide

The Security Profile also uses the OpenID Foundation's Financial API (FAPI) Read and Write API Security Profile. This specification is published on the OpenID Foundation website at openid.net.

The OBIE is a member of the OpenID Foundation, a non-profit international standardisation organisation of individuals and companies committed to enabling, promoting and protecting OpenID technologies. The OBIE is working with the OpenID Foundation to ensure that the profile is maintained as a world class security standard which provides the very best protection available for all users.

The Standards for APIs specify risk indicators that can be included in the API payload to aid fraud detection and prevention. All Participants are strongly advised to include completed risk indicators within their payload to facilitate strong security across the Open Banking Ecosystem.

The Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) are expected to come into force towards the end of 2019. In July 2017, HMT produced a document entitled: "Expectations for the third party access provisions in Payment Services Directive II". It advised that the view of HM Treasury and the Financial Conduct Authority (FCA) is that the Open Banking approach will become the most suitable option for firms once the Open Banking Implementation Entity has delivered a solution that enables them to comply with all their obligations under PSDII and the RTS. HMT therefore encourages Participants to work towards using the Standards as the basis on which secure API access to other payment accounts is provided in future. It further stipulates that while the RTS might prescribe how safety and security is to be delivered in future, it is expected that Participants adhere to the principles of safety and security from 13 January 2018.[1] The Read/Write APIs have been designed to create a framework to enable compliance with the RTS SCA.

[1] HMT, July 2017: "*Expectations for the third party access provisions in Payment Services Directive II", p2, para1; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf*

Security Approach for Participants

The OBIE has worked with experts within Financial Services, Fintech and Security organisations to develop rigorous security within the Read/Write APIs and the wider Open Banking Ecosystem. In order to protect the confidentiality, integrity and availability of information and data in the Open Banking Ecosystem, all Participants should ensure that security is given sufficient profile and influence in their organisation.

Recommended areas of security capability include (but are not limited to):

- Specialist information security function
- Security Operation Centre (SOC)
- Experienced external penetration testing supplier
- Information security assurance of third party suppliers, their processes and contractual obligations
- People controls, including vetting, and secure joiners, movers, leavers processes
- IT systems controls around the infrastructure and applications
- Information security controls covering but not limited to ISO27001:2013 or an appropriate equivalent standard
- Information security requirements embedded in the development lifecycle
- Dedicated cybersecurity function
- Specialist counter fraud function

Information Security

On 12 December 2017, the EBA issued the final report on guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)[2]. All Participants are solely responsible for their compliance with the relevant EBA guidelines applicable to their service offering.

All Participants should build and implement capability appropriate for their organisation to ensure a secure operating environment. This capability should include robust security coverage for any services they provide and the third parties they contract with. All Participants should identify, control and review Information Security risks in their organisation – with board oversight of the most significant risks. Implementing an Information Security Management System (ISMS) is a key control to information security risk within an organisation.

The recommended Information Security Management System for Mandatory ASPSPs is ISO27001:2013. Voluntary ASPSPs and TPPs should implement an information security framework appropriate to the scale and maturity of their organisation, the services they provide, and the third party suppliers they contract with. A recommended alternative for smaller organisations is Information Assurance for Small, Medium Enterprises (IASME). IASME is designed to bridge the gap between having no ISMS in place and

[2] http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

ISO27001:2013 accreditation. Both systems take a risk based approach to managing information security risk using a wide range of controls.

Security Operations Centre

All Participants should implement a Security Operations Centre (SOC) to monitor and manage security incidents, threats and alerts. A Security Operations Centre means a dedicated facility for monitoring, assessing and defending enterprise information systems (web sites, applications, data servers, networks, hardware, software and other endpoints). Using specialist tools (including security incident and event management systems) enables an organisation to identify, investigate and resolve security incidents and alerts. All systems should be logging activity by individuals – to sufficient granularity (such as IP addresses, date/time stamp etc) that root causes of problems can be identified and remediated. A SOC should run 24/7/365 with incident escalation and response processes (including timeframes for responding) being clearly defined. Participants could review analysis undertaken by both Gartner Inc and Forrester Research Ltd into commercial providers of security incident and event monitoring systems.

Regardless of the infrastructure deployed, all Participants should ensure they use good industry practice in implementing information security controls. All Participants should deploy strong controls around:

Data Access and Handling

All Participants should ensure a clear policy and rules are in place around access to data and systems. This should include but not be limited to technical policies (such as throttling, timeout rules and role based access). The National Cyber Security Centre in the UK (NCSC) and National Institute of Standards and Technology in the US (NIST) regularly provide updated information relating to latest recommendations on passwords and technical controls to reduce risks relating to data access.

All Participants must define a clear set of data handling policies and rules, in order to protect the confidentiality, integrity and availability of all data handled by the Participant.

Credentials management

All Participants should ensure that they have the appropriate infrastructure in place for secure storage and management of Open Banking security credentials. This obligation will always be applicable, irrespective of whether the services they provide are hosted in house or outsourced to a third party. These credentials include (but are not limited to):

- Identity keys
- Signing keys
- OAuth client IDs and secrets
- Usernames and passwords
- Access tokens

Where authentication processes are handed off or redirected to other sites and apps, the technical processes should avoid the potential for disclosure or interception of the credentials. You should also maintain the ability for the user to verify the authenticity of the site into which they are entering their credentials. An example of poor practice approach which would contravene these guidelines would

be the use of an embedded web-view within a mobile application which suppresses the display of a url bar / lock icon.

Penetration testing

All systems and infrastructure should be regularly tested for vulnerabilities by an external penetration testing expert. Penetration testing systematically probes for vulnerabilities in applications and networks, and should be undertaken in a controlled manner (to minimise any impact on live operations). It is recommended that such an expert is professionally accredited (such as CREST, IISP, TIGER scheme or OSCP Offensive Security). The benefits of penetration testing include:

- Accurately evaluate organisational ability to defend against attack
- Obtain detailed information on actual, exploitable security threats
- Intelligently prioritise remediation activity, apply necessary security patches and allocate security resources

The OBIE has an active Information Security Working Group (ISWG) consisting of Information Security experts from Participant organisations. All Participants are encouraged to nominate a member of staff to attend the ISWG and support ongoing security in the Open Banking Ecosystem. The working group is chaired by a representative of the OBIE. Participants should contact the Open Banking Service Desk for more information.

Cybersecurity

Strong cybersecurity defences are critical to the success of Open Banking. A comprehensive approach to cybersecurity should combine industry standards and best practice with processes to assess current and future threats to protect systems and information. All Participants should implement cybersecurity strategies that protect networks, hardware, applications and data from being stolen, compromised or attacked.

Recommended areas for a strong cybersecurity strategy include (but are not limited to):

- Strong Firewall defences
- Vulnerability and Threat management
- Antivirus and malware protection
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) protection
- Patch management
- Email filtering
- Web filtering
- Administration privileges
- Access control
- Intelligence and information sharing

Cybersecurity capability can be assessed in many ways. Mandatory ASPSPs should consider ISO27032:2012 accreditation alongside ISO27001:2013 (as a broader suite of information security controls). Voluntary ASPSPs and TPPs should consider the assessment framework of CyberEssentials and CyberEssentials Plus as part of their IASME certification.

The Cyber Information Sharing Partnership (CiSP) is a joint industry and government initiative set up by the National Cyber Security Centre (NCSC). The aim is to exchange cyber threat information in real time and in a secure, confidential and dynamic environment. This will increase situational awareness and reducing the impact on UK business. The CiSP platform is owned and operated by the NCSC.

The OBIE is a member of the CiSP and has created an Open Banking node. The node is designed specifically to enable Participants to benefit from CiSP information sharing arrangements. Using a Traffic Light Protocol (TLP) system, Open Banking CiSP members can exchange threat information and collaborate on cybersecurity related issues. This collaboration includes but is not limited to alerting the NCSC and other members to cyber related incidents either in an open forum or under private/closed exchange arrangements.

The CiSP is also the forum for Participants to share details of attacks or exploitable defects in the design of their APIs which impact the services provided through them. Notifying other Participants as soon as reasonably practical will increase the strength and security of the Open Banking Ecosystem.

Some of the benefits of Participants joining the CiSP are:

- Engagement with other industry sectors and government cyber security specialists in a secure environment.
- Early warning of cyber threats (both general and those focused specifically on Open Banking targets).
- Ability to learn from experiences, mistakes, successes of other users and seek advice, either on a one-to-one basis, within a safe and controlled environment or across the whole CiSP membership.
- Enhanced ability to protect the organisation's network infrastructure and applications.
- Access to free network monitoring reports tailored to the organisations' requirements.

Membership of CiSP is free of charge and can only be secured once approval has been granted by the Open Banking administrator. Membership is not mandatory, but Participants are encouraged to join the CiSP upon enrolment in the Open Banking Directory. Many Mandatory ASPSPs and Voluntary ASPSPs are already CiSP members.

To become a member of the CiSP, a Participant must agree to the CiSP terms and conditions, which can be found at https://www.ncsc.gov.uk/cisp.

Counter Fraud controls

The introduction of new products and services in the Open Banking Ecosystem could be a potential target for the perpetration of fraud. Fraud can occur both in payment initiation and account information transactions and has a significant negative impact on trust in services when fraud is identified. All Participants should include a specialist counter fraud operation as part of their approach to information security.

The Read/Write APIs specify risk indicators that can be included in the API payload to aid fraud detection and prevention. All Participants are strongly advised to include completed risk indicators within their payload to facilitate strong security across the Open Banking Ecosystem.

All Participants should develop a counter fraud strategy to identify, control and mitigate fraud threats facing their organisation and customers. The counter fraud strategy should therefore start with a threat assessment to understand where fraud threats exist, their proximity and potential impact.

This threat analysis should then be used to determine appropriate fraud controls and mitigation measures. In a technology led product or service, many controls can be implemented without the user being aware. Participants should consider the use of two (2) factor authentication methods for access to products and services and the use of behavioural analytics to identify normal and abnormal user patterns.

Employing a dedicated counter fraud unit that can work closely with the OBIE, information security, cyber security and SOC colleagues to prevent and detect fraud is highly recommended to all Participants.

The OBIE has worked with Financial Fraud Action UK (FFA UK) to develop an information and intelligence sharing platform for Participants. This builds upon the services FFA UK offer existing members on sharing intelligence and information on known, attempted and actual fraud. FFA UK has links into regulators and law enforcement agencies to build good practice and counter fraud capability across UK financial services. Participants are strongly recommended to join FFA UK and take advantage of their knowledge and expertise in financial services fraud.

False emails purporting to be from the original organisation are a common way to launch phishing and social engineering attacks. Membership of the Domain Message Authentication Reporting & Conformance (DMARC) organisation provides a strong mitigation for this, as well as affording a mechanism for copyright detection and enforcement.

On 19 December 2014, the EBA issued final guidelines on the security of internet payments[3]. Given the level of (and potential for) fraud in internet payments, all Participants are solely responsible for their compliance with the relevant EBA guidelines applicable to their service offering.

The OBIE also has a Counter Fraud Strategy Group which works to assess potential fraud in Open Banking products and services from a counter fraud perspective. The group also influences Participants to refine and adapt counter fraud models to take account of new and emerging threats. The OBIE Counter Fraud Strategy Group will implement the Open Banking counter fraud strategy in 2018 – following completion of scoping and analysis of potential counter fraud controls in the Open Banking Ecosystem.

3.2 The Open Banking Implementation Entity's Approach to Security

The OBIE seeks to provide an elevated level of information security protection for information under its control. As such, its operation aligns with ISO27001:2013, the International Standard for Information Security. The OBIE's systems are regularly assessed and assured by internal and external specialists. All

[3] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments/-/regulatory-activity/consultation-paper

system releases are penetration tested, with any vulnerabilities reviewed by an in-house Security Operations Centre (SOC).

The OBIE's SOC monitors its operational environment with a 24 hour service. This includes alerting and incident event monitoring and response.

The operating environment is protected by native application security, Distributed Denial of Service (DDOS) protection capability and a web application firewall. The infrastructure is protected with intrusion prevention/detection and host anomaly detection systems. All alerts undergo secure monitoring 24x7x365, and access to the Open Banking Ecosystem is secured through implementation of a multi factor authentication mechanism.

Internal threats are mitigated by strong people-vetting controls and well defined business roles and processes. The OBIE uses well known industry IT suppliers with a proven track record around managing security and associated threats. Security requirements are included in clearly defined security schedules within contracts and reflect the service being provided as well as the size and scale of the supplier organisation.

The OBIE is working with expert organisations across the Finance and Banking sectors on combating the likelihood of fraud and cyber security issues. This includes but is not limited to identifying fraud and cyber threats, developing mitigating responses and the sharing of intelligence and information to build capability across all Participants. The OBIE has also taken a proactive approach to Cybersecurity and is associated with various intelligence groups sharing information and monitoring emerging threats.

4 Open Banking Standards

4.1 The Open Banking Standards

All ASPSPs must adopt and maintain the agreed Data Standards for read/write data issued by the OBIE. ASPSPs will, in accordance with the Terms and Conditions for ASPSPs, make the API data available via its Read/Write APIs to TPPs, technical service providers or any agent acting on behalf of a TPP in the provision of payment services.

All Participants must ensure that data is provided or requested in line with the Data Standards issued by the OBIE.

Where these standards change from time to time ASPSPs will ensure that they support versions in line with the OBIE's service levels and policy for release management and versioning.

4.2 Publication of the Open Banking Standards

The Open Banking Standards are published on the Open Banking website at www.openbanking.org.uk

5 Open Banking for Read/Write API Standards

Read/Write APIs enable TPPs, with the customer's consent, to obtain the account information and transaction history of Personal and Business Current Accounts and/or initiate payments from those accounts.

Payments Initiation

The Payments Initiation APIs enable TPPs to initiate payments on behalf of customers with their consent and, once authorised by the customer at their ASPSP, submit the payment for processing. The Payments Initiation API specification currently caters for the submission of a single, immediate, domestic payment from UK Personal and Business Current Accounts and is payment scheme agnostic.

Accounts and Transaction Information

Accounts and Transaction Information APIs enable TPPs, with the customer's consent, to access account information and transactional history from the customer's account for the provision of account information services.

5.1 Read/Write Data Participant Roles

The following Participants operate within the Open Banking Ecosystem specifically for Account and Transaction Information Data and Payment Initiation:

- Account Servicing Payment Service Providers (ASPSPs - Mandatory and Voluntary)
- Third Party Providers:
    - Payment Initiation Service Providers (PISPs)
    - Account Information Service Providers (AISPs)

5.2 Enrolling with the Open Banking Implementation Entity for Read/Write Data

Entities wishing to enrol with the OBIE for Read/Write Data will need to follow the enrolment process which may be initiated by visiting the Open Banking website at www.openbanking.org.uk

An entity should first apply for authorisation or registration with their Competent Authority for the role(s) they wish to perform. The entity may start the enrolment process with the OBIE prior to obtaining Competent Authority authorisation/registration, however the authorisation/registration requirements must be met in order to complete enrolment.

During the enrolment process entities will be asked to provide information including:

- Legal status and entity details, including:
    - Legal entity or natural person name and registered address
    - For registered companies, the country of registration and legal entity identifier or company register details
    - For other types of entities, details of the legal status and registration (if appropriate)

Additional information may be requested by the OBIE, this will only be required in order to confirm the identity of the entity.

Note: The enrolment of a regulated legal entity will allow operation within the Open Banking Ecosystem for all trading/brand names associated with that regulated legal entity.

- Primary contacts nominated as users to access the Directory, including:
    - A **Primary Business Contact:** An individual nominated by the entity to have access to the Directory and will be able to nominate other Directory business users. This should be a formal business point of contact and a senior member of staff responsible for systems and controls related to Open Banking.
    - A **Primary Technical Contact:** An individual nominated by the entity to have access to the Directory and will be able to nominate other Directory technical users. This should be a main point of contact on technical enablement and a senior member of staff with responsibility for the management of the Open Banking digital identity.

  On completion of enrolment the primary contacts may nominate additional users, including agents, technical facing entities, and technical service providers. The regulated entity will be responsible for maintaining user access to the Directory, including removal of users that are no longer nominated by the entity.

  Note: User names and details will not be shared with other Participants. All data will be held securely in the Open Banking Directory.

- The regulatory status of the entity. In order to complete enrolment for the Open Banking Directory a Participant must be authorised or registered by a Competent Authority to:
    - Perform the relevant services under the Payment Services Regulations or Electronic Money Regulations
    - Perform the relevant services under the Financial Services and Markets Act
    - Hold a passport into the UK for the relevant services under the Payment Services Regulations or Electronic Money Regulations
    - Hold the relevant passport under the Capital Requirements Regulation

  An entity may submit an enrolment form prior to completion of their authorisation/registration with a Competent Authority in order to commence the OBIE's identity verification process. The enrolment process may only be completed for each role once the appropriate Competent Authority authorisation/registration has been granted related to that role.

  When an entity is authorised/registered with a Competent Authority the entity will provide details of the authorisation/registration number and details of their entry on the Competent Authority register.

- The person submitting the enrolment form will provide a **Declaration** that they are authorised to make the application on behalf of the entities named on the form, that the information provided is accurate and complete, and that they authorise the OBIE to make enquiries to verify the information provided. If the entity is enrolling to perform an ASPSP role, the entity will be expected to agree to the **Terms and Conditions** and Participation Conditions specified.

On submission of the enrolment form the OBIE will perform verification checks on the entity, the primary contacts specified, and the person submitting the form. These checks will be based on known standards and processes equivalent to levels that meet civil court requirements.

The OBIE will also verify details of the authorisation/registration of regulated entities on the relevant Competent Authority register, where appropriate.

On successful completion of the verification process, the details of the new Participant, including the nominated Primary Business Contact and Primary Technical Contact information, will be recorded in the Directory as a Participant of the Open Banking Ecosystem for the roles requested.

5.3 Enablement of Identity Records and Digital Certificates

Following successful enrolment, Participants will need to enter technical details and generate digital certificates in order to operate within the Open Banking Ecosystem.

Technical enablement will allow ASPSPs to provide access to API end points for the brands/trading names that relate to the legal entity enrolled.

TPPs will also need to register their applications with each ASPSP that they wish to obtain access to API end points.

These enablement activities provide the ability for the TPP to identify themselves to the ASPSP for each transaction. Within the details presented, Participants will specify named contact details for business and technical enquiries. This will include a name or role description, telephone number, and email.

5.4 Onward Provisioning

Within the Open Banking Ecosystem, a number of different TPP business models are supported. This allows multiple TPPs, which may include technical service providers, to work collectively in order to enable payment initiation and account information transactions for PSUs. The responsibilities with regard to the arrangements put in place by the regulated TPP with other (potentially unregulated) firms, including outsourcing arrangements, are included within the regulatory obligations of TPPs.

It is an important requirement for PSUs to be kept informed about which parties in any transaction are accessing their account.

Onward provisioning allows for the presentation of this information to the PSU, making them aware of the specific parties in the transaction chain. This will include the regulated TPP, as well as another TPP (regulated or unregulated) or technical service provider that has been engaged in the provision of the payment initiation or account information transaction.

When enrolling with the OBIE, the regulated party may specify the name of another TPP which they would like the PSU to be informed about using a consumer familiar name. The OBIE recommends that only the

key consumer facing TPP and the ASPSP facing party names are identified. ASPSPs must make available to the PSU the name of the regulated party, however it is at their discretion to present the other party details to the PSU at the ASPSP authorisation or authorisation dashboard stages.

The completion of the other party field is in the competitive space for the TPPs and ASPSP, the OBIE's view is that the PSU experience might be improved if the optional other party attribute is completed by the regulated TPP and that the ASPSPs present the names of both the mandatory regulated party and the optional other party, if completed by the TPP, to the PSU.

5.5 Post-Enrolment Directory Revocation and Withdrawal

To ensure the integrity of the Directory, the OBIE will manage revocation and voluntary withdrawal of Participants from the Directory.

If a Participant has been revoked or has voluntarily withdrawn from the Directory, they will no longer be able to operate within the Open Banking Ecosystem, access the Open Banking Directory, or use the OBIE's support services.

All existing technical certificates associated with the Participant will be revoked.

5.5.1 Withdrawal of a Participant from the Directory

A Participant may withdraw from the Directory at any time after successful completion of their initial enrolment.

A Participant wishing to withdraw will need to follow the withdrawal process which may be initiated by a Primary Business Contact visiting the Open Banking website at www.openbanking.org.uk.

ASPSPs may withdraw by providing a minimum of 60 Business Days' written notice to the OBIE. Within 5 Business Days of providing such notice to withdraw to the OBIE, the withdrawing ASPSP should also notify TPPs that have registered their applications with the withdrawing ASPSP of their intention to withdraw.

TPPs may request to withdraw at any time and will be asked to specify a proposed effective date.

On receipt of the withdrawal request, the Open Banking Service Desk will respond with an acknowledgement email to the Primary Business Contacts and Primary Technical Contacts email addresses. In order to complete the withdrawal request, the OBIE will require confirmation of withdrawal by another Primary Business Contact or Primary Technical Contact.

Once the Service Desk is in receipt of all the required information supporting the withdrawal request, the Directory will be updated and a confirmation email sent to the Primary Business Contacts and Primary Technical Contacts email addresses confirming successful withdrawal.

The OBIE will publish details of the withdrawal of ASPSPs on the Open Banking website.

The OBIE will provide email notification to ASPSPs of the withdrawal of a TPP.

5.5.2 Revocation of a Participant from the Directory

A Participant may be revoked from the Directory if their regulatory status, for all roles held on the Directory, is revoked by the relevant Competent Authority and this revocation is reflected on their regulatory register.

In addition, if a Participant from an EEA member state has passported into the UK then access may be revoked temporarily if the FCA, as host state Competent Authority, takes precautionary measures in

relation to that Participant that have an impact on the provision of access to account information and/or initiation of payments.

Note: If a Participant holds multiple roles on the Directory, and only one or more but not all of the roles are revoked by the relevant Competent Authority, then only permission to perform that particular role/s will be revoked from the Directory, as per the regulatory register. All other valid regulatory permissions will remain.

The OBIE will provide email notification to ASPSPs of the revocation of a TPP.

For the avoidance of doubt, revocation of an ASPSP will be in accordance with the Terms and Conditions for ASPSPs.

A Participant formerly enrolled for Read/Write Data that has had access revoked from the Directory will be required to re-enrol to facilitate their reinstatement to full participation.

6 Testing

All Participants should undertake rigorous application and security testing appropriate for their organisation and the services that they will provide. On 15 July 2015, the EBA issued final guidelines on product oversight and governance arrangements for retail banking products[4]. All Participants are solely responsible for their compliance with the relevant EBA guidelines applicable to their service offering.

The OBIE has defined multiple test phases supported by tools developed in conjunction with Financial Services and Fintech experts. Taking advantage of these test phases and tools may assist TPPs in delivering robust and high quality applications to access the Read/Write APIs.

TPPs are strongly encouraged to participate in testing activities and to utilise the OBIE's test tools and the Directory Sandbox to ensure:

- Integration with the Open Banking Directory and tools (Open Banking testing)
- An extension of Open Banking testing to include onboarding and integration with ASPSPs (Ecosystem testing)
- A controlled launch into the Ecosystem utilising an increasing volume approach (Managed rollout)

The OBIE can provide guidance on which of these test phases are appropriate and provide support with the scope of testing for each phase, use of the test tools and queries raised during testing.

Entities that have submitted an enrolment form may participate in testing activities on successful completion of the verification checks on the entity, the primary contacts specified on the enrolment form, and the person submitting the form. On successful completion of these phases of the enrolment process the OBIE will provide the primary contacts with details on how to participate in testing activities.

Please note that access to the test tools does not provide the entity with access to the Open Banking Directory as a Participant. The full enrolment process will only be completed once the appropriate Competent Authority authorisation/registration has been granted.

[4] https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products

7 Maintaining the Integrity of the Directory

7.1 Changes to Participants' Enrolment Information

From the submission of an enrolment request up until the completion of enrolment, Participants must provide any changes to their details as soon as practicable to the Open Banking Service Desk. This will invoke an update process.

After completion of enrolment, Participants will have access to self-service facilities to view and request updates to enrolled entity information.

7.2 Management of Personal Data Held on the Directory

Any personal data held on the Directory for Participants will be processed in accordance with data protection law.

7.3 Retention of Records

Where a Participant is withdrawn or revoked, for whatever reason, from the Open Banking Directory, the retention period for records will be a minimum of 6 years from the date of withdrawal, or such longer period as required by law, for audit purposes unless subject to statutory or regulatory change.

8 Complaints and Disputes

8.1 Complaints Against the Open Banking Implementation Entity

Complaints may be raised by ASPSPs and TPPs where the complaint is against the OBIE.

A complaint may be raised with the OBIE by sending an email to the Open Banking Service Desk at ServiceDesk@openbanking.org.uk.

Complaints raised by Participants should be raised by a Primary Business Contact or a Primary Technical Contact.

On receipt of a complaint, the Open Banking Service Desk will send an acknowledgement of receipt within one business day, record the complaint and may instigate an investigation into the circumstances of the complaint. On completion of the investigation, the Service Desk will provide a response.

The OBIE will liaise with the person who raised the complaint on any aspects of the complaint, including where relevant any steps within the Open Banking Complaints and Dispute Resolution Procedure. In the event that the person who raised the complaint is unavailable, a Primary Business Contact or Primary Technical Contact may nominate another contact person.

Any Participant who is unsatisfied with the response can escalate their complaint using the Complaints and Dispute Resolution Procedure. This procedure is available to all Participants as well as any entity for whom enrolment has been unsuccessful. Once initiated, it is a mandatory procedure and each step must be followed. The outcome is non-binding on all parties. Parties remain free at any time to pursue other available options for resolution.

All communication with the OBIE and/or The Trustee in relation to complaints and disputes should be sent by email to the Open Banking Service Desk.

The OBIE Programme Management Group will be notified if a complaint is received from an entity for whom their enrolment has been unsuccessful, or from an entity that has had access revoked or suspended.

8.2 Enquiries, Complaints or Disputes received by a TPP or ASPSP from a PSU

The Dispute Management System (hereafter known as DMS) and accompanying Code of Best Practice are available for TPPs and ASPSPs to follow when handling an enquiry, complaint, or dispute raised by a PSU . Details of the process and accompanying code can be found on the Open Banking website.

Those signed up will benefit from consistency, commonality and efficiency. Key principles are to exercise good faith, communicate fairly and transparently with each other and the complainant and to coordinate their respective efforts.

The mechanism involves a self-service set of standardised complaint forms, reason codes and a clear process for communication to support dispute and complaint management and enquiries.

The DMS does not replace any existing and new regulatory or legal requirements imposed on organisations.

The Code also makes reference to ADR solutions (Alternative Dispute Resolution) where necessary. The independent adjudicator for eligible PSUs (individuals or micro-enterprises) would be the Financial

Ombudsman Service (FOS), or an OBIE-endorsed adjudicator nominating body for business-to-business or SMEs.

8.3 Enquiries, Complaints or Disputes raised by a TPP or ASPSP against another TPP or ASPSP

A TPP or ASPSP is able to raise an enquiry, complaint or dispute against another TPP or ASPSP in relation to a payment initiation or account information service transaction.

Where all parties are participants in the DMS, the case will be handled in line with the accompanying Code of Best Practice. Details of the DMS and accompanying code can be found on the Open Banking website.

Appendix: Glossary

For further information on the terms used within this document please refer to the Glossary on the Open Banking website at www.openbanking.org.uk.