OPEN BANKING

Open Banking

Guidelines for Open Data Participants

Date: July 2018
Version: 2
Classification: PUBLIC

© Open Banking Limited

Contents

© Open Banking Limited

1 An Introduction to Open Banking

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 for Personal Current Accounts (**PCA**), Business Current Accounts (**BCA**), **SME** Loans and Commercial Credit Cards via Open Data APIs, to include:
    - Product prices
    - All charges (including interest)
    - Features and Benefits
    - Terms and Conditions and customer eligibility
- The release of PCA service quality indicators via APIs showing the willingness of their customers holding a PCA to recommend:
    - the Brand to friends and family
    - the Brand's online and mobile banking services to friends and family
    - the Brands's branch services to friends and family
    - the Brands's overdraft services to friends and family
- The release of BCA service quality indicators via APIs showing the willingness of their customers holding a BCA to recommend:
    - the Brand to other SMEs
    - the Brand's relationship/account management to other SMEs
    - the Brand's online and mobile banking services to other SMEs

© Open Banking Limited

- the Brands's branch services and business centre to other SMEs
- the Brands's credit (overdraft and loan) services to other SMEs

- The release of PCA and BCA 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 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

In December 2017, the Financial Conduct Authority (**FCA**) published Policy Statement PS17/26 entitled Information about current account services (**FCA Policy Statement**) which requires the release of comparative PCA and BCA information and metrics via Open Data APIs, to include:

- service availability
- major incidents
- account opening metrics
- replacement of debit card metrics

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 would create 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

© Open Banking Limited

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 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 PCAs, BCAs (for SMEs), and SME Unsecured Lending, including Commercial Credit Cards. From 15 August 2018, the FCA requires the publication of additional Open Data elements, to include service availability and major incidents; and from February 2019, to include account opening and replacement debit card metrics.

The release of CMA Service Quality Indicators relating to PCA and BCA that are wholly based on survey responses collected by independent survey agencies, as defined in the CMA Order, will also commence on 15 August 2018.

The release of further API Standards for **Read/Write Data** that enabled Participants to publish API end points has been functional since 13 January 2018. These additional Read/Write API Standards, required by the CMA Order, enable third party providers, with the end customer's consent, to request account information such as the transaction history of PCAs and BCAs and/or initiate payments from those accounts.

A further programme of releases to build on the core requirements of the CMA Order will continue to be implemented throughout 2018 and 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 **Open Banking 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 Open Banking Directory and its constituent components
- The provision of an API for the publication of CMA Service Quality Indicators on behalf of **Mandatory API Providers**.
- 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**

© Open Banking Limited

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 API Providers 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 Information Security and Counter Fraud
- Open Banking Standards
- Open Banking for Open Data
- Maintaining the Integrity of the Open Banking 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 API Providers and the OBIE:

- the Complaints and Dispute Resolution Procedure
- the Open Data Service Level Agreement for API Providers
- the Open Licence
- the Privacy Policy
- the Standards
- the Terms and Conditions for API Providers

The Open Banking Ecosystem is also governed by UK and European regulations including Revised Payment Services Directive (PSD2), General Data Protection Regulation (GDPR), 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.

© Open Banking Limited

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.

© Open Banking Limited

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 Open Data Participants

API Providers

API Providers are service providers implementing an Open Data API. An API Provider provides Open Data via an API gateway. API Providers are split into two further categories: Mandatory API Providers and Voluntary API Providers.

Mandatory API Providers

Mandatory API Providers are entities that are required by the CMA Order to enrol with the OBIE as API Providers. The following entities are Mandatory API Providers 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 API Providers must publish APIs in accordance with the Standards, enrol onto the Open Banking Directory, and may use the associated OBIE operational support services.

Voluntary API Providers

Voluntary API Providers 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.

OBIE as an API Provider

OBIE will provide an API for the publication of PCA and BCA CMA Service Quality Indicators, as defined by the CMA Order, on behalf of the Mandatory API Providers via a single API.

API User

An API User is any person or organisation who develops web or mobile apps which access data from an API Provider.

© Open Banking Limited

3 The Open Banking Information Security and Counter Fraud

3.1 Security Good Practice Guidelines

The expectation of OBIE is that Participants should read and implement the recommendations detailed in the documents 'Participant Guide: Information Security operations' and 'Participant Guide: Counter Fraud operations'[1].

In summary, these suggest the following industry standards:

- Large Participants – these organisations should align to ISO27001, the International Information Security standard that defines guidance and controls required to establish an effective Information Security Management System to govern the information security regime of a large organisation.

- Small, Medium and Micro Enterprise Participants - these organisations should align with the IASME Governance standard which is based on international best practice. The IASME Standard is written along the same lines as ISO27001 but tailored specifically for small companies. It is risk-based and includes aspects such as physical security, staff awareness, and data backup thus allowing SMEs to demonstrate their level of cyber security and that they are able to properly protect their customers' information.

- API Users– this type of Participant should be aligned with Cyber Essentials which defines an entry level set of controls which will, when properly implemented, provide these participants with basic protection from the most prevalent threats coming from the Internet. This focuses on threats which require low levels of attacker skill, and which are widely available online and Participants should be aware that this will not consider more complex, advanced attacks.

In all cases, external assurance and certification of the Information Security adherence is preferable to self-certification.

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 (and will become certified to) ISO27001:2013, the International Standard for Information Security. The OBIE's systems are regularly assessed and assured by internal and external specialists. All 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

[1] See https://www.openbanking.org.uk/about-us/documents/page/2/

© Open Banking Limited

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.

© Open Banking Limited

4 Open Banking Standards

4.1 The Open Data Standards

All API Providers must adopt and maintain the agreed Data and Technical Standards for Open Data issued by the OBIE. API Providers will, in accordance with the **Terms and Conditions for API Providers**, make their own Open Data available. API providers will also be required to support backward compatibility up to and including the previously published last major release.

All Participants must ensure that data is provided or requested in line with the Data Standards issued by the OBIE and published on the Open Banking website at www.openbanking.org.uk

The Open Banking Technical Standards for Open Data must be compliant with:

- All functional and non-functional technical standards published by OBIE, including (but not limited to) the RAML and/or Swagger specifications, naming standards, versioning, error messages, availability, performance, caching, throttling, security ciphers, and use of headers/meta data
- ISO20022 standards for data structure as a primary requirement. Where this is not possible, the data structure must contain data elements that are ISO20022 compliant as a minimum
- World Wide Web Consortium (W3C) specifications that are considered relevant
- The Data Protection Act 2018 and General Data Protection Regulation (EU 2016/679), where applicable
- Data will be transmitted via “Read only” access
- The Open Banking Security Profile

Where these standards change from time to time API Providers 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

© Open Banking Limited

5 Open Banking for Open Data

Open Data APIs enable API Users to access Open Data, as defined by the CMA Order and FCA Policy Statement, when published by API providers.

5.1 Open Data Participant Roles

The following Participants operate within the Open Banking Ecosystem specifically for Open Data:

- API Providers
- API Users

5.2 Enrolling with the Open Banking Implementation Entity for Open Data

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

Open Banking shall have absolute discretion to refuse an application for entry on to the Open Banking Directory from a prospective Participant provided it is acting reasonably.

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

- Legal status and entity details, such as:
  - Legal entity or natural person name, registered address and correspondence 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 Open Banking Directory, including:
  - A **Primary Contact**. This should be a formal business point of contact and a senior member of staff responsible for systems and controls related to Open Banking.
  - An **API Administrator:** This should be a main point of contact on technical enablement.

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

© Open Banking Limited

provided. If the entity is enrolling to perform an API Provider role, the entity will be expected to agree to the **Terms and Conditions for API Providers** 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 a link to the API Provider's end points will be published on the Open Banking website.

API Users will be required to provide contact details of one Primary Contact for enrolment. Any API User that does not enrol will be required to accept the **Terms and Conditions for API Users** and the **Open Licence** via a tick box on the Open Banking website, but will not be able to take advantage of any support services offered by OBIE.

Participants must provide any changes to their details held on the Open Banking Directory as soon as practicable to the Open Banking Service Desk; this will invoke an update process.

5.3 Post-Enrolment Open Banking Directory Withdrawal and Revocation

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

If a Participant has been revoked or has voluntarily withdrawn from the Open Banking 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.

5.3.1 Withdrawal of a Participant from the Open Banking Directory

A Participant wishing to withdraw will need to follow the withdrawal process which may be initiated by a Primary Contact contacting the Open Banking Service Desk.

- Voluntary API Providers may withdraw from the Open Banking Directory by providing a minimum of 20 Business Days' written notice to the OBIE.

- API Users will be permitted 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 Contacts and API Administrator email addresses. In order to complete the withdrawal request, the OBIE will require confirmation of withdrawal by another Primary Contact or API Administrator.

© Open Banking Limited

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

The OBIE will publish details of the removal of API Providers on the Open Banking website.

5.3.2 Revocation of a Participant from the Open Banking Directory

A Participant may be revoked from the Open Banking Directory if their regulatory status 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 Open Banking 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 Open Banking Directory, as per the regulatory register. All other valid regulatory permissions will remain.

The OBIE will publish details of the removal of API Providers on the Open Banking website.

For the avoidance of doubt, revocation of an API Provider or API User will be in accordance with the Terms and Conditions for APIs Providers and API Users.

A Participant formerly enrolled for Open Data that has been revoked from the Open Banking Directory will be required to re-enrol to facilitate their reinstatement to full participation.

A Participant may raise a **Complaint** in accordance with the **Complaints and Dispute Resolution Procedure**.

© Open Banking Limited

6 Maintaining the Integrity of the Open Banking Directory

6.1 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.

6.2 Management of Personal Data Held on the Open Banking Directory

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

6.3 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.

© Open Banking Limited

7 Complaints and Disputes

7.1 Complaints against the Open Banking Implementation Entity

Complaints may be raised by API Providers and API Users 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 Contact or an API Administrator.

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 Contact or API Administrator 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.

© Open Banking Limited

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.

© Open Banking Limited