# Introduction

1.1 Background
1.2 About Open Banking
1.3 About Open Banking Limited
1.4 About the Guidelines

# The Open Banking Ecosystem

2.1 The Open Banking Directory of Participants

# Open Banking Security Standards

3.1 Security Practice for Participants
3.2 Security within the Open Banking Implementation Entity

# Open Banking Standards

4.1 The Open Banking Standards
4.2 Publication of the Open Banking Standards

# Open Banking for Read/Write API Standards

5.1 Read/Write Data Participant Roles
5.2 Enrolling with Open Banking for Read/Write Data
5.3 Enablement of Identity Records and Digital Certificates
5.4 Post-Enrolment Directory Revocation and Withdrawal

# Maintaining the Integrity of the Directory

6.1 Changes to Participants’ Enrolment Information
6.2 Management of Personal Data Held on the Directory
6.3 Retention of Records

# Complaints
1 Introduction

Unless defined herein, all terms shall have the same meaning given to them in the Terms and Conditions.

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.

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.

1.3 About Open Banking Limited

Open Banking Limited 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.

Open Banking is responsible for:

• The prescribed format for the Open Banking Standard 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
Open Banking Limited 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 APIs.

1.4 About the Guidelines

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

This document is a Guidelines document prepared to provide guidance to Participants who wish to commence enrolment for Read/Write Data prior to 13 January 2018. This document will be replaced by a full Open Banking Guidelines document as at 13 January 2018 when Payment Services Regulations come into effect as national law and third party providers can commence engaging in the provision of account information and payment initiation services.

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 APIs
- Maintaining the Integrity of the Directory
- Participant Adherence to the Open Banking Standards

These Guidelines should be read in conjunction with the following documents that together with these Guidelines form the suite of Participation Conditions and form part of the contractual obligations on ASPSPs:

- the Terms and Conditions
- the Standards
- the Complaints and Dispute Resolution Procedure
- the Service Level Agreement
- the MI Reporting Document
- 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.

Open Banking, in consultation with the relevant Working Groups, is empowered to amend the documents that form the suite of Participation Conditions in order to comply with any forthcoming changes to regulatory or legislative obligations or when required.

Any change or amendment to these documents will be made utilising the Open Banking Limited governance process, which includes consultation with the following Working Groups:

<table>
<thead>
<tr>
<th>Document</th>
<th>Working Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines</td>
<td>Guidelines Working Group</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Regulatory &amp; Legal Working Group</td>
</tr>
<tr>
<td>Standards</td>
<td>Read/Write Data Working Group</td>
</tr>
<tr>
<td></td>
<td>Information Security Working Group</td>
</tr>
<tr>
<td></td>
<td>Directory Working Group</td>
</tr>
<tr>
<td></td>
<td>Technical Design Authority</td>
</tr>
<tr>
<td>Complaints and Dispute Resolution Procedure</td>
<td>Regulatory &amp; Legal Working Group</td>
</tr>
<tr>
<td></td>
<td>Guidelines Working Group</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>Service Working Group</td>
</tr>
<tr>
<td>MI Reporting Document</td>
<td>Service Working Group</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>Data Privacy Working Group, as part of the Regulatory &amp; Legal Working Group</td>
</tr>
</tbody>
</table>

Depending on the nature of the change, the Working Group may recommend a review of the changes by the Programme Management Group and Implementation Entity Steering Group. The Implementation Entity Trustee has powers under the CMA Order to agree changes if consensus cannot be agreed.

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.

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 Open Banking 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 Open Banking operational support services.

Voluntary ASPSPs

Voluntary ASPSPs are those entities who, although not obliged to enrol with Open Banking, 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)
o 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 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 payment service user 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 payment service user or to the payment service user and to another person in accordance with the payment service user’s instructions.

2.1 The Open Banking Directory of Participants

The Open Banking Directory is the key architectural component that enables Participants to enrol with Open Banking 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

Open Banking seeks to provide a high level of information security protection for information under its control. As such, its operation aligns with ISO27001, the International Standard for Information Security.

Operational activities will be governed by this regime with risk-based decision-making guiding the implementation of the service. An Information Security Management System is in place.

Open Banking has also worked with experts within Financial Services, Fintech and Security organisations to develop rigorous security in the Open Banking Directory and APIs.

3.1 Security Practice for Participants

The Open Banking Security Standard defines how the Read/Write APIs are secured using a multi layered approach. The OAuth 2.0 authorisation framework and Open ID Connect identity authentication are layered over multiplexed transport layer security 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.

Open Banking Limited 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. Open Banking 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 Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) are currently in draft form and are expected to come into force in July 2019 (at the earliest). 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 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.

Open Banking is working with expert organisations across the Finance and Banking sectors on combating the likelihood of fraud and cyber security issues. This includes identifying fraud and cyber threats, developing mitigating responses and the sharing of intelligence and information to build capability across all Open Banking Participants.

3.2 Security within the Open Banking Implementation Entity

Open Banking also recognises the need for strong Information Security within its operations and is operating in alignment with ISO27001. User access is controlled and all systems have information asset owners who regularly monitor and manage access control lists for their systems. Systems are regularly assessed and assured by internal and external specialists.

Open Banking will be monitoring its operational environment using Security Operations Centre capability. The Security Operations Centre is a centralised unit that deals with security issues on an organisational and technical level. This will include 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 24x7, and access to the Open Banking Ecosystem is secured through implementation of a multi factor authentication mechanism.
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 Open Banking. Mandatory ASPSPs must provide access to read/write data for payment initiation and account information services as set out in the CMA Order.

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

Where these standards change from time to time ASPSPs will ensure that they support versions in line with Open Banking’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 Open Banking 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 Open Banking for Read/Write Data

Entities wishing to enrol with Open Banking 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 Open Banking 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 Open Banking, 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 configuration 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. The 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

  - Act as an Agent for a firm which holds the relevant services under the Payment Services Regulations or Electronic Money Regulations

An entity may submit an enrolment form prior to completion of their authorisation/registration with a Competent Authority in order to commence the Open Banking 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 Open Banking Limited to make enquiries to verify the information provided. If the entity is enrolling to perform an ASPSP role, the entity will need to agree to the Terms and Conditions and Participation Conditions specified.

On submission of the enrolment form Open Banking 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.

Open Banking 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 complete technical configuration of their identity records and digital certificates in order to operate within the Open Banking Ecosystem.

Technical configuration will allow ASPSPs to configure the Directory to provide access to API end points for the multiple 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 configuration activities provide the ability for the TPP to identify themselves to the ASPSP for each transaction. Within the details presented, Participants will specify a contact name for Business Enquiries Contact Details and Technical Enquiries Contact Details. This will include a name or role description, telephone, and email. These may be tailored for each application.

5.4 Post-Enrolment Directory Revocation and Withdrawal

To ensure the integrity of the Directory, Open Banking 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 Open Banking support services.

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

5.4.1 Withdrawal of a Participant from the Directory

A Participant (enrolled for Read/Write Data) may withdraw from participation in the Directory at any time after completion of their initial enrolment.

A Participant wishing to withdraw will need to follow the withdrawal process which may be initiated by visiting the Open Banking Website at www.openbanking.org.uk
The withdrawal request must specify a proposed date of withdrawal, taking into account the required minimum notice period. ASPSPs will be subject to a minimum of 60 Business Days' written notice either way. ASPSPs should notify relevant TPPs as specified within the MI Reporting Document.

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. Open Banking will publish details of the withdrawal of ASPSPs on the Open Banking Website.

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.

5.4.2 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.

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, than 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.

In addition, if an ASPSP has committed a serious and persistent breach of the Participant Conditions Open Banking Limited may, having consulted with the Trustee and relevant Competent Authority, revoke or suspend access to the Directory. For the avoidance of doubt, a Mandatory ASPSP cannot be revoked without explicit agreement from the CMA.

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

6.1 Changes to Participants' Enrolment Information
From the period of enrolment up until 13 January 2018, Participants must provide any changes to their details held on the Directory as soon as practicable to the Open Banking Service Desk. This will invoke an update process.

From 13 January 2018 Participants will have access to self-service facilities to request changes to enrolment information.

6.2 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.

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.
7 Complaints

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

On receipt of a complaint, the Open Banking Service Desk will send an acknowledgement of receipt, 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 Open Banking 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.