Open Banking

Operational Governance Rules and Guidelines for March 2017 Open Data

Date: 6th February 2017

Contents

1 SUMMARY

The development of an Open Banking Service (OBS), comprising of the Banking API Standards and Governance framework required by the Competition and Markets Authority (CMA), has the potential to dramatically improve competition and innovation in UK banking for customers and businesses.

Open Banking Limited has been created as the Open Banking Implementation Entity (Open Banking) to meet and deliver the CMA's mandate, help shape open standards and to ensure the interest of customers, API Providers and API Users are represented. Open Banking will be overseen by the "Open Banking Implementation Trustee" (OBIT). The initial delivery is to implement an open data standard for the provision, sharing and transmission of certain open data from March 2017. This is to be followed by the delivery of certain read/write data, no later than January 2018.

The CMA full report (Sections 13.68 to 13.71)[1] mandates that the Open Banking address four broad areas[2]. This information is formalised in the CMA Order on Retail Banking Market Investigation (updated on 23 January 2017). To meet the CMA Order, this document sets out the Operational Governance Rules and Guidelines as a governance framework for delivery of the Open Banking ecosystem delivery for March 2017 for open data only.

The "Operational Governance Rules & Guidelines Working Group" (OGRGWG) has been established to provide operational support for the implementation of standards for the provision and sharing of March 2017 open data for Participants and includes:

- The roles and responsibilities of Open Banking.
- The roles and responsibilities of Participants, including rules regarding access to and use of the OBS ecosystem from March 2017.
- API Providers to provide the most up-to-date data for API Users to consume and to reflect what the Providers have in the market
- The API, Data and Security standards they need to adhere to.
- The withdrawal, complaints, and disputes processes required to support Open Banking and its ecosystem.
- The handling of breaches, suspension and exclusion of Participants.
- Service Levels applicable to the rules governing the OBS ecosystem from March 2017. (These will be defined in a separate document called "Open Banking Service Levels March 2017for Open Data -" and will apply to all Participants as appropriate.

The Operational Governance Rules and Guidelines are based on work stream activities across the development of Open Banking and therefore may be subject to any changes to scope or decisions made within these areas. Currently the work streams are:

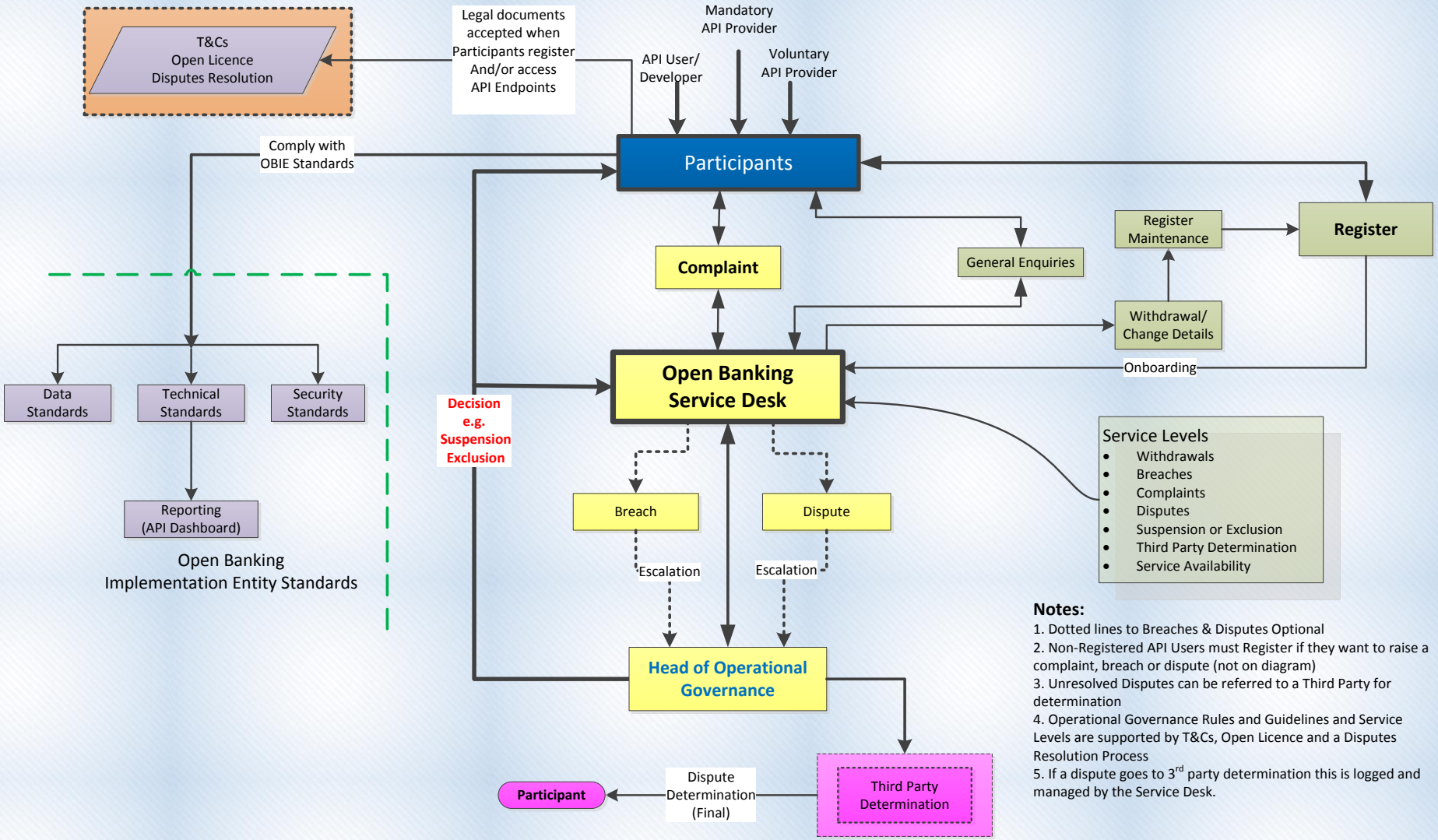
- Operational Governance - Target Operating Model (TOM) definition

[1] The CMA Retail Banking Market Investigation Report

[2] The 4 broad areas are API Standards, Data Standards, Security Standards and redress and Governance arrangements.

- Operational Governance - Central Register and Accreditation processes
- Regulatory and Legal (Compliance)
- Technical Development and NFR's
- Standards (Data and API)
- Security Information
- Customer

Open Banking Operational Governance Model



Notes:

1. Dotted lines to Breaches & Disputes Optional
2. Non-Registered API Users must Register if they want to raise a complaint, breach or dispute (not on diagram)
3. Unresolved Disputes can be referred to a Third Party for determination
4. Operational Governance Rules and Guidelines and Service Levels are supported by T&Cs, Open Licence and a Disputes Resolution Process
5. If a dispute goes to 3rd party determination this is logged and managed by the Service Desk.

2 Introduction

2.1 Background

In the 2015 Budget, Her Majesty's Treasury (HMT) announced its commitment for delivering an open standard for APIs and data sharing in UK Retail Banking as a measure to increase the opportunity for competition in the retail market, facilitating the development of an effective FinTech intermediary sector and increased customer choice.

In May 2016 the CMA published a provisional decision on remedies which required the banks to adopt a subset of the Open Banking proposals. In August 2016, the full CMA report was issued which mandated the implementation of the Open Banking Implementation Entity core proposals as foundation remedies.

In September 2016, Open Banking issued a paper outlining the Programme approach to achieve an OBS ecosystem. The paper was approved by the Implementation Entity Steering Group (IESG) and provided an initial view of the scope and delivery mechanisms to address the CMA remedies and meet the Open Banking core proposals for the creation of the OBS.

The concept is to deliver certain open data utilising standardised API technology with participation available to API Providers and API Users. This document sets out Operational Guidelines to support the ecosystem. All Participants are subject to the Participation Conditions as defined in the Terms and Conditions. These Operational Guidelines are supplementary to the Participation Conditions and are intended to aid the operational aspects of the Open Banking ecosystem. In the event of any conflict or omission the Terms, the Standards, the Licences and the Dispute Resolution Procedure will take priority over the Operation Guidelines (all as defined in the Terms).

2.2 Scope for March 2017

- Open Banking Role and Responsibilities
- API Provider and API User Participant roles and responsibilities
- Data Standards for Open Data (with up to date data dictionary)
- API Standards for Open Data
- Security Standards
- Set up of a Central Register
- Establish an Open Banking Operations Service Desk - with operators cross-skilled to perform multiple functions on start-up and to include:
    - Manage and Maintain Central Register
    - Complaints Handling
    - Disputes Resolution
    - Service Levels (will be documented with activity timings in an Service Level document (and supported by detailed process flows / procedures)

3 Definitions

The following words and phrases will have the following meaning within these Rules and Guidelines (and refer to the T&C's definitions):

Breach means a breach by a Participant of the Open Banking Rules and Guidelines, T&C's, Open Data Licence or the Data, Technical or Security standards as defined by Open Banking. It may or may not constitute a breach of contract.

It could be (without limitation):

a) An omission or action which is a breach of the rules or Participation Conditions.
b) A serious omission or action whether or not it causes an imminent material threat to a Participant.
c) Grounds for suspension or exclusion.

Central Register is an Open Banking Register of Participants (API providers and API Users) who have joined the ecosystem and in the case of API Users have chosen to register. By registering, Participants will be given access to support services such as complaints and disputes resolution. The register will also store Participants who are suspended or excluded.

Complaint Handling Process will be created and communicated to all Participants following registration, setting out the process for:

a) Initiating and raising complaints due to a breach
b) Service Level response times
c) Escalation

Complaints can only be submitted by Participants who have registered and will follow a 3 stage process:

1. A participant will raise a breach complaint with the Open Banking Service Desk, who may provide a response subject to the Disputes and Resolution Policy set out in the T&C's.
2. A complaint can be escalated to the Head of Operational Governance (as delegated by the OBIT), who will make a determination, e.g. suspension with a plan of action or exclusion.
3. If a participant is unhappy with the decision they can use the services of a Third Party Referee for determination. This course of action will be logged and managed by the Open Banking Service Desk.

Dispute is disagreement of one party to another party. In Open Banking, this could be an API User to an API Provider or vice versa. The dispute could also be a Participant dispute with Open Banking. The Disputes Resolution Procedure documented as part of the T&Cs is the basis of the Disputes section in this document. Open Banking will mediate on disputes raised with the Service Desk and provide a determination. For disputes against Open Banking, the Head of Operational Governance (as delegated by the OBIT) will make an initial determination and engage a Third Party for determination where deemed necessary. In the first instance Participants will use their best endeavours to resolve any dispute between themselves. Participants will not be able to resolve issues directly with the 3rd party

until the dispute is raised via the Open Banking Service Desk. Disputes can only be managed for registered Participants. An unregistered User will be requested to register if they wish to use the Dispute service. If they fail to resolve a dispute one or both parties can raise the issue with the Open Banking Service Desk for determination by the Head of Operational Governance (as delegated by the OBIT). If a determination is not possible, the dispute can be referred for Third Party Determination by any party.

Exclusion is when a decision is made to exclude a Participant who has or is in the opinion of Open Banking likely to intentionally, habitually or seriously breach any of the rules or guidelines in the Participation Conditions. The excluded Participant will no longer have permission to access Provider APIs or Open Banking Support Services. They will have the right to initiate Third Party Determination. An exclusion decision may exclude a Participant with immediate effect. Participants that are required to be part of the Open Banking ecosystem cannot be excluded.

Participant Conditions - the agreement governing the Participants roles and responsibilities in the Open Banking Services comprising the:

a) Terms
b) Standards
c) Licences
d) Operational Guidelines
e) Dispute Resolution Procedure.

Participant Role - A registered Participant can be one or more of the following roles:

a) Mandatory API Providers - the CMA9 banks mandated under the CMA full report[3] that will provide open data. These are also known as API Providers
b) Voluntary API Providers - all other providers of open data. These are banks and financial service organisations (including Challenger Banks, ATM providers, Non-Bank Lenders) that are not one of the CMA9 banks. These are also known as API Providers.
c) API Users – individuals or organisations that choose to access open data. These may be known as Third Parties, Data Users, API Developers, and Intermediaries and may include Participants that are Mandatory API and Voluntary API Providers.

Suspension is when a decision is made to suspend a Participant who has intentionally, habitually or seriously breached any of the rules or guidelines defined in the Participation Conditions. An investigation could lead to a number of outcomes, including exclusion from Open Banking. A suspension could be immediate or within the Service Level, determined on a case by case basis and is a temporary state whilst under investigation by Open Banking.

Withdrawal is an option for any registered participant who wishes to withdraw from the Open Banking central register, although this will not be available to the CMA9. Withdrawal should be communicated in writing. The terms of notice defined in the Service Levels.

[3] The CMA Retail Banking Market Investigation Report

4 Operational Governance Rules and Guidelines

This section presents the rules and guidelines necessary to implement open banking for March 2017, for each area within scope of the delivery for March 2017 as defined within Section 2.2.

4.1 Open Banking Role and Responsibilities

Open Banking will provide operational governance for the OBS Ecosystem from March 2017 to:

a) Create a Standards Governing Body to define and maintain the necessary Data, Technical and Security Standards related to the OBS ecosystem.

b) Provide Open Banking Services and perform its obligations under the Participant conditions and the CMA Order with reasonable care in accordance with Applicable Law.

c) Implement, operate, maintain and make available at no charge, the open and common banking standards for API read only access.

d) Define the rules around access to the Central Register process and assignment of appropriate roles for all Participants of the OBS.

e) The Head of Operational Governance (as delegated by the OBIT) will define the rules and adjudicate on Complaints.

f) The Head of Operational Governance (as delegated by the OBIT) will define the guidance on and act as a referral point for Participant breaches. This includes investigation and possible referral to a Third Party Referee for determination.

g) The Head of Operational Governance (as delegated by the OBIT) will be to act as mediator for disputes between Participants and between Participants and Open Banking (with onwards referral to a Third Party Referee for independent determination where required).

h) Where the Head of Operational Governance (as delegated by the OBIT) is required to make a determination, he may consult with relevant regulatory bodies where necessary.

i) Publish the Providers APIs as URL's on the Open Banking website.

j) Implement and provide ongoing assurance for all Operational Governance rules and guidelines for March 2017.

4.2 Open Banking Obligations

Open Banking in consultation with the Working group is empowered to amend the rules and guidelines within this document in order to comply with any forthcoming changes to regulatory or legislative obligations or when required. Notice of any amendment or change to this document will be provided to Participants via the OBS website and email if practical using the nominated contact.

4.3 Participant Responsibilities

4.3.1 API Provider

a) Each Provider must comply with the rules and obligations laid down by Open Banking for the Registration agreement and comply with the Participation Conditions.

b) Each Provider has a duty to ensure that where the contact details for their trade name, organisation, entity or nominated individual change, and they must communicate this to the Open Banking Service Desk.

c) Each Provider agrees and acknowledges that they may be required to co-operate with regulatory bodies from time to time, or as required by law, as part of their participation in the OBS.

d) Each registered Provider will have a link on the Open Banking website of details of their API and API connectivity for any participant who requests it from the website within the defined Service Level. Where a Provider fails to comply with the Service Level, the requesting Participant may submit a formal complaint via the Open Banking Service Desk.

e) Each Provider is required to develop their API in line with the Technical Standards guidelines outlined in this document (refer to Section 7).

f) Each Provider is required to adhere to the Security Standard guidelines outlined in this document (refer to Section 7).

g) Each Provider is required to provide open data, within the required format and structure, as defined within the Data Standards guidelines (refer to Section 7).

h) Each Provider is required to make open data available in accordance with the Participant Service Levels.

i) Where a Provider has a concern about the operation or conduct of an API User, then this should immediately be raised to Open Banking, who will invoke an investigation and deliver a decision on the issue via the Disputes Resolution guidelines outlined in this document.

4.3.2 API User

a) Each User must comply with the rules and obligations laid down by Open Banking for the Register agreement and comply with the Participation Conditions.

b) Each User agrees and acknowledges that they may be required to co-operate with regulatory bodies from time to time, or as required by law, as part of their participation in the OBS.

c) Each User is required to call an API in line with the Technical Standards guidelines outlined in this document (refer to Section 7).

d) A User does not have to be registered to access Provider APIs, but will still be required to accept the Participation Conditions on the Open Banking website prior to access through Open Banking.

e) Each User is to request open data from an API Provider in the specified format as defined within the Open Data Standards guidelines (refer to Section 7).

f) Each User should adhere to the Security Standard guidelines outlined in this document (refer to Section 7)

g) Where there is a dispute between registered Participants, both Participants have a duty to remedy this dispute between them. If this cannot be achieved within a reasonable time frame, either party can invoke the Disputes Resolution guidelines outlined in this document.

h) Where a User has a concern about the operation or conduct on an API Provider, then this should immediately be raised to Open Banking, who will invoke an investigation and deliver a determination on the issue. Open Banking may pass on information to other participants and Regulators where deemed necessary.

i) Open Banking shall have absolute discretion to refuse an application for entry on the Central Register from a prospective API User provided it is acting reasonably.

5 Open Banking Register

5.1 API Provider - Validation and Registration

a) All stages of the Registration process will be **compulsory** for both Mandatory and Voluntary Providers. Any Provider who does not register will not be able to take advantage of any support services offered by Open Banking as defined in these Rules and Guidelines or provide access to its APIs via Open Banking. This includes, but is not limited to the access to the Sandbox, disputes resolution, complaints handling, sanctions application and security monitoring. (Possible sanctions to Voluntary Providers could be limited to suspension, exclusion and removal from the register).

b) Any Provider who wishes to join the OBS for March 2017 must provide the requested detail required under the Registration and Validation stages of the Registration process, for Open Banking to satisfy itself of the Provider's compliance and ability to comply with the rules as a Provider of the OBS. (Note that registration for open read only data could remain in place and continue into 2018 and not be superseded by read/write access).

c) Open Banking will determine whether the Provider can comply with the Pre-Registration and Validation stages of the Registration process for the OBS. If satisfied, Open Banking will allow them to complete the Registration process.

d) Providers may be subject to light independent checks as part of the Validation stage of the Registration process, to include name, address, point of contact details and company details. These will be defined by the Provider Role within the Registration process documentation.

e) Providers that succeed through the full Registration process are considered a live Provider for OBS ecosystem and will be entered on the Central Register.

f) Once the Participant role has been assigned on completion of registration, a link to the API Provider's end points will be published on the OBS website and the Participant will be notified by email.

5.2 API User - Validation and Registration

a) The Registration process will be **optional** for Users who will in all cases be required to accept the Participation Conditions via a tick box on the OBS website.

b) Any User that does not register will be required to accept the Participation Conditions via a tick box on the OBS website, but will not be able to take advantage of any support services offered by Open Banking as defined in these rules and guidelines. This includes disputes resolution, complaints handling and application and security monitoring.

c) Any User who wishes to join the OBS for March 2017 will be exempt from the initial validation stages of the Registering, but will have an automatic check of email contact details.

d) Users that succeed through the full Registration process are considered a live Participant for the OBS ecosystem and will be entered on the Central Register.

e) An open data licence and terms and conditions will be presented to all Users wishing to access a published API end point, and to proceed, they must confirm acceptance.

5.3 Central Register Maintenance

5.3.1 Vetting

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

b) Where Open Banking requests a Participant to provide information to support maintenance of the Central Register, this is to be provided to the Open Banking Service Desk within the deadline notified in the communication to the Participant.

c) Where a Participant merges with or is divested to another Participant, then Open Banking will determine what action to take in regards to the registration. Open Banking will request a Participant to provide the required criteria to meet the Central Register process under their new Participant name or entity.

d) Registered Participants will be required, under the Central Register process, to provide updates of contact details or nominated contact points within their organisation.

e) Participants who register will be given access to community updates, support facilities, communications, dispute resolutions and bound by the Open Banking rules, guidelines, T&Cs and the Open Licence.

f) Any personal data held on the Central Register as part of the Registration process for Participants will be stored and secured in line with the Data Protection Act 1998 (DPA) until GDPR comes into force, when it will be held in accordance with GDPR.

5.3.2 Breaches

a) If at any point a Participant breaches the Open Banking Standards (refer to Section 7) they are obliged to inform the Open Banking Service Desk (as defined in the Service Levels) of any breach being discovered (refer to the Registration Process T&Cs for details on the criteria). Notification should be by one of the communication mediums specified in the Service Level. Upon receipt of the notification, Open Banking will invoke an investigation process to make a decision.

b) Where Open Banking has discovered that as part of the vetting process or from any other communication, that a Participant has breached the standards for the Central Register, Open Banking will invoke an investigation process to make a determination. At the same time this will be communicated to the Participant who is deemed to be in breach (refer to Service Levels).

c) Where a Provider has identified a breach or suspected breach by an API User they are to inform the Open Banking Service Desk and raise a complaint, which will initiate an investigation.

d) Where Open Banking is unable to make a determination regarding a breach, they will refer details of the breach with any associated documentation to the Head of

Operational Governance (refer to Disputes section 6 for details) to make a recommendation and advise the Participant of this determination.

e) Where guidance has been issued to the Participant for a breach, Open Banking may set a deadline within which they expect the Participant to be compliant with the rules and/or any specific guidance issued. Participants that breach the Open Banking Standards may be subject to suspension or exclusion from the Central Register, depending on the severity of the breach.

5.3.3 Withdrawal from the Central Register

a) Mandatory API Providers will not be permitted to withdraw from the OBS. If exceptional circumstances were to occur, which may include, but is not limited to, revocation of a banking license, exclusion by a regulatory body, or withdrawal of products defined under the CMA ToR. Withdrawal must be agreed by all governing bodies of Open Banking (i.e. the IESG).

b) Where a Voluntary API Provider requests withdrawal from the Central Register, this must be communicated in writing to the Open Banking Service Desk, stating a proposed date of withdrawal. The Service Desk will acknowledge the receipt of any request from a Participant to withdraw from the Central Register as soon as reasonably practicable.

c) Voluntary API Providers, must give a minimum term of notice to withdraw from the OBS (refer to Service Levels). Failure to comply will result in the Open Banking imposing a fair and reasonable withdrawal date necessary to preserve the integrity of the OBS.

d) API Users will be permitted to withdraw from the OBS at any point following the withdrawal process via their access to the Central Register (refer to Service Levels).

e) Where an API Provider or an API User has withdrawn from the OBS, the Central Register must be updated (refer to Service Levels).

5.3.4 Retention of Records

Where a Participant is withdrawn from the Open Banking Register, the retention period for records to withdraw them upon a request to be de-registered will be for 6 years for audit purposes unless subject to statutory or regulatory change. The exception is ATM data (refer to T&Cs).

Personal data (which includes corporate contact details) will be deleted on request from the relevant Participant. The only exception is where the Participant is identified solely by personal details, as may be the case for a sole trader, where these details will be held as their corporate identity for the 6 years mentioned above.

At least two sets of details will be taken for each Participant senior manager for redundancy (apart from in cases where this is not possible, such as sole traders). Where a Participant asks to delete either contact, the Participant must provide a replacement contact before the requested deletion can be made.

5.3.5 Suspension and Exclusion from the Central Register

a) Where a Participant has breached the rules defined for registered Participants, they may be suspended and marked as such on the Central Register.

b) A suspension could be immediate or within the defined Service Levels and applied on a case by case basis.

c) Open Banking has the authority to suspend any Participant and remove from the Open Banking Register with immediate effect if found in breach of OBS Rules and Guidelines. The suspended Participant will have the right to employ the 'Third Party Determination' to challenge a suspension or exclusion. The CMA9 will not be suspended without CMA agreement or in exceptional circumstances post facto ratification.

d) Participants who are marked as **Suspended** must receive guidance and a plan for remedial action to be taken by the OBS Head of Operational Governance within the Service Levels. The outcome of the investigation may result in:

   i. The Participant being re-instated on the Central Register.

   ii. The Head of Operational Governance (as delegated by the OBIT) issuing a recommended resolution and plan for the Participant to comply in order to lift the suspension.

   iii. Participants that fail to comply with the recommended actions and/or deadlines may be considered for exclusion by the Head of Operational Governance (refer to Service Levels and Suspension and Exclusions Policy in Appendix A).

e) Open Banking will have the right to add any Suspended Entity Brand, API set or API User linked to a website to a Suspended list for publication onto the Open Banking website (refer to Service Levels).

f) Participants who are Mandatory API Providers must continue to be active on the Central Register for the provision of open data. Open Banking would seek counsel from the relevant regulator, e.g. CMA or FCA.

g) Any Suspended Participants must be flagged as such on the Central Register. Suspended Participants will be added to a Suspended list for publication on the OBS website (refer to Service Levels).

h) Where an API Provider or an API User is suspended, any API Developer attached to that entity will not be subject to suspension where they have relationships with other API Providers or Users.

j) A Voluntary API Provider or API User will be reinstated at the end of a suspension period to full participation, unless the Provider or User has not implemented a remedy, in which case they will be excluded from participating in Open Banking.

k) A Participant could be suspended if they are both a provider and a User, but could be suspended for one particular role and not necessarily for the other role.

l) An API User will be excluded if they have committed a material breach of the Participation Conditions that is capable of remedy, and not resolved the breach within the specified number of days of receipt of notice of the breach (refer to Service Levels).

m) An API User will be excluded immediately if they have committed a serious and persistent breach of the Participation Conditions.

n) Where the OBS decision is a recommendation for **Exclusion** (refer to T&C's) this must be communicated to the participant as soon as the determination occurs.

o) Any excluded Participants will be notified to all other Participant. Open Banking will have the right to add Excluded Participants to an Excluded list for publication on the OBS website (refer to Service Levels).

6 OPEN BANKING SUPPORT SERVICES

6.1 Complaints Handling

6.1.1 Administration

a) A Complaints Handling Process will be created and communicated to all Participants following registration and will apply only to breaches of the Open Banking Standards, T&C's, Open Licence and these Rules and Guidelines setting out the process for:

   i. Initiating and raising complaints

   ii. Service Level response times

   iii. Escalation

b) The Open Banking Service Desk will administer the OBS Complaints Handling Process.

c) Participants must be able to initiate the complaints process via multiple channels setting out full details of the complaint, e.g. by email or phone.

d) A complaint as a result of a reported breach is a starting point for the Open Banking to investigate and could potentially lead to a suspension, exclusion or dispute.

e) Complaints can only be submitted for registered Participants.

f) If a Participant is not registered, they will be asked to register before a complaint can be considered. Issues that occur before their Registration date can then be investigated.

g) Where a complaint has been raised with the Open Banking Service Desk, acknowledgement of receipt and determination response of that complaint will be confirmed back to the Participant raising the complaint (refer to Service Levels).

6.1.2 Decisions and Escalation

a) The Open Banking Service Desk will advise the Participant of its decision regarding the complaint and communicated to the Participant within the Service Levels.

b) Where the Open Banking Service Desk is unable to make a decision on a complaint, they will refer the complaint to the Head of Operational Governance (as delegated by the OBIT) as the adjudicator OBS for complaints and disputes.

6.2 Disputes and Resolution

Where there has been a breach or other matter concerning the Participation Conditions that could lead to a dispute, the operation of the Open Banking Services (a Dispute) will be dealt with by the Dispute Resolution Procedures.

6.2.1 Outline of Disputes Procedure

The parties to a dispute will make an effort to resolve a dispute in accordance with the Disputes Resolution Procedure as follows:

a) In the first instance Participants will use their best endeavours to resolve any dispute between themselves regarding open data. Participants will not be able to resolve issues directly with the 3rd party until the dispute is raised via the Open Banking Service Desk.

b) Escalation of Dispute - Where disputing parties fail to resolve any dispute between themselves**,** either Participant can escalate the dispute by referral to the Open Banking Service Desk to invoke an assessment by OBS Head of Operational Governance on a case by case basis.

c) Third Party Determination - If the Head of Operational Governance cannot make a determination, the dispute can be referred to a third party for determination.

6.2.2 Escalation of Dispute

a) Each participant will notify Open Banking in writing of contact details (by name or role) to who disputes will be referred.

b) Any dispute will be referred to the nominated representative of “each disputing party” for assessment and resolution within the Service Level from when the dispute escalation was initiated.

c) If any dispute is not resolved by the disputed parties, the dispute will be logged by the Open Banking Service Desk and referred to the OBS Head of Operational Governance for assessment (refer to Service Levels).

d) Following the OBS Head of Operational Governance being appointed, each disputing party will submit a written summary to Open Banking and to each other (refer to Service Level).

e) The assessment will take place following submission of the written summaries (refer to Service Levels). The disputing parties can agree to extend these periods at any time).

f) Where a determination cannot be made by the OBS Head of Operational Governance (as delegated by the OBIT), the dispute can be referred for Third Party Determination.

g) The costs of the assessment (including the Dispute Resolution expenses but excluding the Disputing Parties' own costs, which will be borne by the Disputing Party incurring those costs) and will be borne equally by the Disputing Parties, except where agreed in writing in the settlement agreement.

h) Open Banking shall have the right to direct that the costs of the assessment are born by the Disputing Parties in different proportions, including wholly by one Disputing Party, where it considers that the Dispute has been started unfairly or one of the Disputing Parties is found not to be at fault. In making its assessment Open Banking may give consideration to the relative resources of the Disputing Parties.

i) Except where the procedure for dealing with Disputes where Open Banking consider it to be business critical for Participants, Open Banking shall have the right, at any time to make an interim or final determination in relation to any Dispute pending resolution by a third party determination.

6.2.3 Third Party Determination

a) Where a dispute is referred to a third party for determination, the disputing parties will agree a suitably qualified third party - a Referee (refer to Service Levels).

b) If the appointed Referee does not accept the appointment, the disputing parties will agree an alternative Referee (refer to Service Levels).

c) If the Disputing Parties fail to agree the identity of a Referee within the Referee Appointment Period (refer to Service Levels), any Disputing Party may apply to the "Centre for Effective Dispute Resolution" (CEDR) to select a Referee.

d) Following acceptance of a Referee accepting an appointment the disputing parties will each submit a written report on the dispute (refer to Service Levels). The disputing parties can agree to extend these periods at any time).

e) The Referee is to deliver a determination following submission of written report (refer to Service Levels). The Referee's determination will be final.

f) The costs of the Referee's determination (including the Referee's fees and expenses and the Disputing Parties' own costs and expenses) will be borne as the Referee directs (having regard to the actions of the Disputing Parties). In the absence of such direction the Referee's fees and expenses will be borne equally by the Disputing Parties and each Disputing Party will bear its own costs.

6.2.4 Provision of Information

On the occurrence of a Dispute, each relevant Party will at the request of any Disputing Party, the Head of Operational Governance (as delegated by the OBIT), or any Referee promptly:

a) Disclose to the Disputing Parties and/or Referee its full Audit Trail, Service Level performance records and any other information relevant to the resolution of the Dispute.

b) Each Party agrees that Open Banking will not have an Audit Trail to be disclosed but will be entitled to produce and rely on any audit trail relating to communications sent by Open Banking to, or received by Open Banking from any other Party.

c) Otherwise co-operate fully with the Disputing Parties and/or Referee as reasonably required for the prompt resolution of the Dispute.

d) Each API Provider must retain its Audit Trail for a minimum period of six years from the date on which the Open Data is made available and is called through the Open Banking APIs (refer to T&C's).

6.3 Service Levels

All Service Levels relating to the areas within this document are defined within the "Open Banking Service Levels for Open Data – March 2017".

7 OPEN BANKING STANDARDS

7.1 Data Standards

7.1.1 Data Standards Industry Compliance

a) The Open Banking Standards Governing Body must ensure that Data Standards for open data are defined and agreed in collaboration with Participants, to enable consistency and standardisation to facilitate open data. Please refer to Open Banking Roles and Responsibilities.

b) The Standards Governing Body must ensure that Data Standards for open data must be compliant with:
   i. 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.
   ii. The Data Protection Act, where this is applicable
   iii. Data will be transmitted via "Read only" access for March 2017[4]

c) The Standards Governing Body must ensure that Data Standards are adhered to and comply with, clear and explicit versioning policies and procedures for:
   i. The use of an open repository to maintain and manage major and minor releases or changes.
   ii. Prescription of minimum support time periods for major releases.
   iii. Backwards compatibility for all minor – and where possible – major releases.
   iv. Forward compatibility design to provide a roadmap for compatibility with future standards and products.
   v. Ensuring that the data dictionary does not stifle innovation and competition.
   vi. Ensure openness to avoid too much rigidity of data fields with risks of tying providers to 'vanilla' products that fit the template but cannot evolve to meet customer expectation.

7.1.2 Participant Compliance

a) All Participants must adopt and maintain the agreed Data Standards for open data issued by the Standards Governing Body for the Open Banking.

b) API Providers must supply open data for products available for sale on or after January 2016.[5]

c) Participants will be granted "read access" only for open data via the Open Licence.

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

e) API Providers must supply Open Data for PCAs, BCAs, SME Lending, ATM and Branch Locations reference data for March 2017 as set out in the CMA Order.

[4] As defined in The Open Banking Standard document Section 5.3.1
[5] As defined in The Open Banking Standard document Section 5.3.1

7.2 Technical Standards

7.2.1 Industry Compliance – API Providers

The Open Banking Standards Governing Body must ensure that Technical Standards for open data must be compliant with:

- All functional and non-functional technical standards published by Open Banking, 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.
- World Wide Web Consortium (W3C) specifications that are considered relevant.
- The DPA and GDPR, where applicable.

Where these standards change from time to time (e.g. in line with Open Banking's policy for release management and versioning), the API provider will ensure that they support the latest published version as defined in the SLA.

API providers will also be required to support backward compatibility up to and including the previously published last major release.

7.2.2 Industry Compliance - API Users

- All API Users will be bound by the terms of the Open Banking Licence.

7.3 Security Standards

7.3.1 Security Best Practice Guidelines

The expectation of Open Banking is that Participants should adhere to the following standards as a "best practice" guideline from March 2017 in terms of open data only:

a) Mandatory and Voluntary Providers – these organisations should be in compliance with ISO27001 as 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.

b) Third Party Providers - these organisations could be smaller Voluntary Providers than a Challenger Bank and should be in compliance with the IASME Governance standard which is based on international best practice. The IASME Standard is written along the same lines as the 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 SME's to demonstrate their level of cyber security and that they are able to properly protect their customers' information.

c) API Users and Developers – this type of Participant should be in compliance 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

forms of 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.

7.3.2 Security Monitoring

a) Open Banking will carry out monitoring of services provided in line their legal obligations, for the purposes of detecting, monitoring and preventing malicious activity or service misuse.
b) In cases where malicious activity or abuse is suspected, Open Banking may choose to suspend the OBS, to protect the service from potential damage.
c) Open Banking expects that organisations using or supplying information to the service will have similar, appropriate monitoring regimes in place for similar reasons.
d) Where legally permissible, Open Banking may request from or supply to, monitoring information from affiliated organisations for the purposes of purposes of detecting, monitoring and preventing malicious activity or service misuse. Information will not be supplied for day to day business management purposes.

7.3.3 General Information Security Statement

Open Banking seeks to provide a high level of information security protection for information under its control. As such, its operation aligns with and will become certified to ISO27001, the International Standard for Information Security. All activities will be governed by this regime with risk based decision making guiding the implementation of the service. Whilst the standards above do not mandate compliance, if Open Banking deems that a Participant's Information Security regime is of a nature that represents an unacceptable threat to the service, it may suspend the Participants affiliation.

8 REPORTING

a) All of the Provider endpoints will be connected to a service dashboard which monitors performance Service Levels and publishes a RAG status for each endpoint based on its behaviour.

b) Open Banking will provide an API dashboard for summary information relating to API Usage.

c) Open Banking will produce a simple report to summarise incidents raised.

9 GLOSSARY AND DEFINITION OF TERMS

API	Application Programming Interface
API Providers	Each of the Mandatory API Providers and Voluntary API Providers.
API Users	Individuals or organisations that choose to access the Open Banking APIs.
Applicable Law	All applicable laws, rules, regulations, orders, regulatory policies, guidelines, regulatory permits and licences, and any mandatory instructions or requests by a Regulator, in each case which are in force from time to time.
ATM	Automated Teller Machine
Backward Compatibility	A property of a system, product, or technology that allows for interoperability with an older legacy system, or with input designed for such a system. Backward compatibility is sometimes abbreviated to BC, or called downward compatibility
BCA	Business Current Account
Breach	A breach by a Participant of the Open Banking Rules and Guidelines, T&Cs, Open Data Licence or the Data, Technical or Security standards as defined by Open Banking. It may or may not constitute a breach of contract. It could be (without limitation): a) an omission or action which is a breach of the rules or Participation Conditions. b) A serious omission or action whether or not it causes an imminent material threat to a Participant c) Grounds for suspension or exclusion
CEDR	Centre For Effective Dispute Resolution, a unique professional services consultancy which provides access to expertise.
Central Register	The register of API Providers and API Users to be created and maintained by Open Banking pursuant to these Terms.
CMA	Competition and Markets Authority
CMA Order	The Retail Banking Market Investigation Order 2017 (as amended).
CMA9	Royal Bank of Scotland Group plc, Lloyds Banking Group plc, Barclays Bank plc, HSBC Group, Nationwide Building Society, Santander UK plc in Great Britain and Northern Ireland and Northern Bank Limited, trading as Danske Bank, Bank of Ireland
Complaint	Complaint Handling Process will be created and communicated to all Participants following registration, setting out the process for: a) Initiating and raising complaints due to a breach b) Service Level response times c) Escalation Complaints can only be submitted by Participants who have registered.
Dispute	A disagreement of one party to another party. In Open Banking, this could be an API User to an API Provider or vice versa. The dispute could also be a Participant dispute with Open Banking. The Disputes Resolution Procedure documented as part of the T&Cs that is the basis of the Disputes section in this document. Open Banking will mediate on disputes raised with the Service Desk and provide a determination. For disputes against Open Banking, the Head of Operational Governance (as delegated by the OBIT) will make an initial determination and engage a Third Party for determination where deemed necessary.
DPA	Data Protection Act 1998
Excluded Participant	When a decision is made exclude a Participant who has or is in the opinion of Open Banking likely to intentionally, habitually or seriously breached any of the rules or guidelines in the Participation Conditions. The excluded Participant will no longer have permission to access Provider APIs or Open Banking Support Services. They will have the right to initiate Third Party Determination. An exclusion decision may exclude a Participant with immediate effect. Participants that are required to be part of the Open Banking ecosystem cannot be excluded.
FCA	Financial Conduct Authority
FinTech	Financial Technology companies
Forward Compatibility	Concept that strives for methods that will continue to work with newer and future products. Design that is forward-compatible usually has a roadmap for compatibility with future standards and products

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
HMT	Her Majesty's Treasury
IA-SME	Information assurance standard for small and medium-sized enterprises
IESG	Implementation Entity Steering Group
ISO20022	ISO standard for electronic data interchange between financial institutions. It describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content.
ISO27001	A specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
MI	Management Information
NFR	Non Functional Requirements
OBB	Open Banking Body
OBIE	Open Banking Implementation Entity
OBIT	Open Banking Implementation Trustee
OBS	Open Banking Services
Open Banking	Open Banking Limited (company number 10440081)
Open Banking Services	The open banking services to be provided iaw Article 12 of the CMA Order as further described in the Participation Conditions.
Open Banking Website	The Open Banking website URL as notified to Participants.
OGRGWG	Operational Governance Rules & Guidelines Working Group
Open Data	All Reference Data and Product Data referred to in Article 12 of the CMA Order that is made available through the Open Banking APIs in accordance with the Standards in each case whether as images, text or otherwise.
PCA	Personal Current Account
Participant Role	An API Provider or an API User (as the case may be) that participates in the Open Banking Services.
Participant Conditions	The agreement governing the Participants roles and responsibilities in the Open Banking Services comprising the: (a) Terms; (b) Standards; (c) Licences; (d) Operational Guidelines; (e) Dispute Resolution Procedure.
PoC	Point of Contact
Sandbox	The technology based test area for registered Participants created and maintained by Open Banking.
Service Levels	The service levels as set out in the Operational Guidelines.
SME Lending	Small Medium Enterprise lending
Suspended Participant	When a decision is made to suspend a Participant who has intentionally, habitually or seriously breached any of the rules or guidelines defined in the Participation Conditions. An investigation could lead to a number of outcomes, including exclusion from Open Banking. A suspension could be immediate or within the Service Level, determined on a case by case basis and is a temporary state whilst under investigation by Open Banking.
T&C's	Terms and Conditions
TOM	Target Operating Model
ToR	Terms of Reference
URL	A **Uniform Resource Locator** (**URL**), commonly informally termed a web address is a reference to a web resource that specifies its location on a computer
Voluntary API Provider	All providers of Open Data other than the CMA 9. These are banks and financial services organisations (including Challenger Banks, Independent ATM Providers (IADs), Non-Bank Lenders) that are not one of the CMA 9.

Withdrawal	An option for any registered participant who wishes to withdraw from the Open Banking central register, although this will not be available to the CMA9. Withdrawal should be communicated in writing. The terms of notice defined in the Service Levels.
W3C	World Wide Web Consortium

.

10 APPENDIX A - SUSPENSION AND EXCLUSIONS POLICY

1. **Policy statement**

This policy is intended to inform Participants of the rules and procedures for Participant Suspension and Exclusion.

2. **Who is covered by the policy?**

This policy covers all Participants in Open Banking.

3. The scope of the policy

This policy covers breaches where a registered Participant may be suspended or excluded by the Head of Operational Governance (as delegated by the OBIT) and the procedures for where this occurs. Suspension or exclusion may be invoked when a Participant has intentionally, habitually or seriously breached any of the rules or guidelines defined in the Operational Government Rules and Guidelines, the Terms and Conditions or the Open Licence of the OBS.

4. Responsibility for implementation of the policy

Open Banking has overall responsibility for the effective controls and operation of this policy; however the Head of Operational Governance (as delegated by the OBIT) will be responsible for any determination and/or recommendation of action for suspension and exclusion subject to the Dispute Resolution Policy.

5. Suspension and Exclusion Procedures

The following sections apply to Participants regarding invocation of suspension, exclusion and the procedures that apply thereafter.

5.1 Open Banking may suspend or exclude a registered Participant for any reason such as where:

a) The Participant habitually or intentionally fails to adhere to the Data and Technical Standards defined and published by Open Banking.

b) The Participant habitually or intentionally fails to comply with the Security Standards defined and published by Open Banking.

c) The Participant intentionally manipulates open data sourced from another provider to their own commercial advantage.

5.2 Suspended Participants referred for Dispute Resolution will have the following procedures applied:

a) The Head of Operational Governance (as delegated by the OBIT) will make a decision or recommendation which must be communicated to the Participant within **10 business days** from the date the suspension is invoked.

b) If a Voluntary API Provider or an API User has committed a material breach of the Participation standards and/or conditions and, if such breach is capable of remedy, the Participant may be excluded if they fail to remedy the breach condition within **5 business days** of receipt of notice of the breach.

c) The Head of Operational Governance (as delegated by the OBIT) may re-instate the Participant as active on the Central Register, or to prescribe remedial action to be undertaken by the Participant within a defined deadline. In exceptional circumstances, it may recommend to exclude the Participant.

d) Suspended Participants will be added to a Suspended list for publication on the OBS website to all Participants within **1 business day** of the suspension being invoked by Open Banking.

e) Where an API Provider or an API User is suspended, any API Developer attached to that entity may not be subject to suspension where they have multiple relationships with other API Providers or Users.

f) Failure by the Participant to adhere to the remedial action within the prescribed timeframe may result in the Participant being suspended or excluded.

g) Where the recommendation is to "exclude" a Participant, the Head of Operational Governance (as delegated by the OBIT) will advise Open Banking and the Participant within **5 business days** of the reaching their recommendation.

h) Excluded Participants will be added to an Excluded list for publication on the OBS website to all Participants immediately.

i) Where any Participant is not satisfied with a determination to suspend or exclude them, they can request a Third Party determination in writing within **5 business days** of the outcome being received.

j) The appointed Third Party Referee's determination will be final.

5.3 Suspended Participants who are Mandatory API Providers will continue to be active on the Central Register only for the provision of open data:

a) A participant can be suspended if they are both a provider, but could be suspended for one role and not necessary for the other role.

5.4. Any Participants that have been suspended have the right to appoint a Third Party for Determination in accordance with the Disputes Resolution Procedure, where they feel the suspension or exclusion is unwarranted or unfair.

5.5. Where a Participant has been excluded, this will be notified to all other Participants of the OBS on the OBS website within 2 hours of the exclusion being invoked and they will be removed from the Central Register.

5.6 The appointed Third Party Referee's determination will be final where a Participant has been excluded.