CENTRAL BANK OF OMAN

OPEN BANKING REGULATORY FRAMEWORK

V1.0

TABLE OF CONTENTS

CENTRAL BANK OF OMAN – OPEN BANKING REGULATORY FRAMEWORK

1. OVERVIEW

1.1. Preamble

1.1.1. This Framework provides the licensing criteria, process, and ongoing obligations imposed on Open Banking Service Providers in relation to the provision of Open Banking Services in the Sultanate of Oman and the marketing or promotion thereof.

1.1.2. The document is to be read under the provisions of the National Payment Systems Law 08/2018, the Executive Regulation 1/2019, the circulars, instructions, notices, and guidelines issued thereunder and with the applicable provisions of Banking Law 114/2000 and its related regulations.

1.1.3. The principles of sound governance, effective management, operational and control considerations shall be used as the overarching principles while implementing this Framework.

1.1.4. The Central Bank will update this Framework periodically (as and when deemed necessary) to provide further guidance to the market participants and new applicants.

1.2. Applicability

1.2.1. This Framework, along with its annexures, will be effective from the date of issuance, unless otherwise specified.

1.3. Scope

This Framework sets out the following:

1.3.1. Conditions for granting and maintaining a License for the provision of Open Banking Services in the Sultanate of Oman.

1.3.2. Rights and obligations of Open Banking Service Providers and the Customers.

1.3.3. Contractual arrangements allowing AISPs and PISPs to access Customer Data held with Banks, PSP Licensees and Financial Institutions.

1.3.4. Powers of the Central Bank with regard to the supervision of Open Banking Service Providers.

1.3.5. In exercising its powers and functions under this Framework, the Central Bank has regard to the following objectives:

(a) Ensuring the safety, soundness and efficiency of Open Banking Services;

(b) Adoption of effective and risk-based licensing requirements for Open Banking Service Providers;

(c) Promoting the reliability and efficiency of Open Banking Services as well as public confidence in Open Banking Services;

(d) Promoting innovation and creating a level playing field for market participants.

(e) Reinforcing the Sultanate of Oman's status as a leading payment hub in the region.

1.4. Definitions
For the purposes of this Framework, the following words and phrases shall have the meaning assigned to each of them unless the context requires otherwise:

1.4.1. **Account Information Service (AIS)**- an electronic or online service which provides consolidated Customer Data on Payment Accounts. For the avoidance of doubt, AIS does not involve the holding of Customer funds at any point in time.

1.4.2. **Account Information Service Provider (AISP)**- a Licensee providing Account Information Service.

1.4.3. **AML/CFT Laws and Regulations**- Royal Decree No. 30/2016 promulgating the Law on Combating Money Laundering and Terrorism Financing, as may be amended from time to time, and any instructions, circulars, guidelines and notices issued by the Central Bank relating to their implementation or issued in this regard.

1.4.4. **Applicant**- a legal person, duly incorporated under the Commercial Companies Law, submitting an application for a License.

1.4.5. **Bank**- any local or foreign bank licensed by the Central Bank to conduct banking activities in the Sultanate of Oman.

1.4.6. **Board of Governors**- Board of Governors of the Central Bank of Oman.

1.4.7. **Central Bank**- the Central Bank of Oman.

1.4.8. **Framework**- this framework [XX] of [XX]

1.4.9. **Commercial Companies Law**- Royal Decree No.18/2019 promulgating the Commercial Companies Law.

1.4.10. **Controller**- a natural or legal person who:

(a) Holds 20% or more of the shares in the Licensee or is able to exercise (or control the exercise of) 20% or more of the voting power in the Licensee;

(b) Holds 20% or more of the shares in a parent undertaking of Licensee, or is able to exercise (or control the exercise of) 20% or more of the voting power in the parent undertaking; or

(c) Is able to exercise significant influence over the management of the Licensee or parent undertaking.

1.4.11. **Customer**- any natural or legal person who obtains, or purports to obtain Open Banking Services from a Licensee, whether for a consideration paid to the Licensee or free of charge.

1.4.12. **Customer Data**- personal and non-personal data, including data related to Customer Payment Accounts that is received, collected, stored, and otherwise processed by a Bank, PSP Licensee, Financial Institution or Licensee through interaction, engagement, communication or in the normal course of business, with Customers, which covers both, data provided by a Customer and data generated as a result of Customer interaction with Banks, PSP Licensees, Financial Institutions and Licensees.

1.4.13. **E-KYC Circular**- Instructions on Digital Onboarding and Electronic-KYC (e-KYC) issued by Circular BM 1191.

1.4.14. **Financial Institutions**- any person that is licensed to conduct financing activities in the Sultanate of Oman as defined by the Central Bank from time to time.

1.4.15. **Framework Contracts**- a contract for the Open Banking Services which is entered into between the Customer and the Licensee, to govern the relationship between them.

1.4.16. **License**- a license issued to the Licensee in accordance with Article 2.3 of this Framework.

1.4.17. **Licensee**- the legal person granted a License under this Framework.

1.4.18. **Open Banking Service Providers**- collectively AISP and PISP.

1.4.19. **Open Banking Services**- collectively AIS and PIS.

1.4.20. **Payment Account**- an account held in the name of the Customer with a Bank, PSP Licensee or a Financial Institution which is used for the execution of Payment Transactions.

1.4.21. **Payment Initiation Service (PIS)**- an electronic, digital or online service, which is used to initiate a Payment Transaction at the request of the Customer from the Payment Accounts. For the avoidance of doubt, PIS does not involve the holding of Customer funds at any point in time.

1.4.22. **Payment Initiation Service Provider (PISP)**- a Licensee providing Payment Initiation Service.

1.4.23. **Payment Service Provider (PSP) Licensee**- an entity duly licensed under the NPSL, Executive Regulations and instructions issued thereunder in the Sultanate of Oman.

1.4.24. **Payment Transaction**- an act, initiated by the payer or payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and payee.

1.4.25. **Personalised Security Credentials**- personalised credentials or features provided by an Open Banking Service Provider to a Customer, or generated by the Customer, for the purposes of the Customer's secure authentication while accessing Open Banking Services.

1.4.26. **Senior Management**- the Licensee's senior officers that are involved in the daily management, supervision, and control of the conduct of the Licensee's business and affairs, including the chief executive officer or general manager, compliance officer, money laundering reporting officer, data protection officer, chief information security officer, chief information technology officer, internal audit officer, and any other position designated as such by the Central Bank.

1.4.27. **Strong Customer Authentication (SCA)**- an authentication based on the use of two or more elements categorised as:

(a) knowledge (something only the Customer knows);

(b) possession (something only the Customer possesses); and

(c) inherence (something the Customer is);
that are independent, such that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.

1.4.28. **Sultanate of Oman**- the territory of the Sultanate of Oman.

1.4.29. **Banking Law**- the Banking Law 114/2000.

1.4.30. **Executive Regulations**- the Decision No. 1/2019 promulgating the Executive Regulation of the National Payment Systems Law.

1.4.31. **NPSL**- the National Payment Systems Law promulgated under Royal Decree No. 08/2018.

2. LICENSING AND APPROVAL

2.1 General Prohibition

2.1.1 No person shall provide or engage in the marketing, promotion or advertising, as explained under Article 8.5 (Marketing and Advertisement), of Open Banking Services within the Sultanate of Oman without obtaining a prior License from the Central Bank unless exempted in accordance with Article 2.2.1.

2.1.2 A PSP Licensee seeking a License under this Framework may approach the Central Bank to be exempted from specific licensing and on-going compliance requirements listed under this Framework.

2.1.3 Any governmental or semi-governmental entity in the Sultanate of Oman may approach the Central Bank to be exempted from specific licensing and on-going compliance requirements listed under this Framework.

2.2 Exemptions

2.2.1 Banks licensed in accordance with the Banking Law shall be deemed to be authorized to provide Open Banking Services and shall therefore be exempt from the prohibition laid down in Article 2.1. Banks shall be required to notify the Central Bank in writing if they intend to market or provide Open Banking Services in the Sultanate of Oman and obtain a no objection letter prior to commencing the marketing or provision of such services in the Sultanate of Oman. The Central Bank reserves the right to withdraw a no objection letter granted to a Bank under this Article.2.2.

2.2.2 The Central Bank may, from time to time, grant an exemption to any Applicant that is a Bank, which it deems fit, through a no objection letter. The exemption granted shall be for specific requirements of the licensing process. The Central Bank reserves the right to withdraw the exemption granted under Article 2.2.1. Banks shall pay [OMR X] to obtain the exemption, along with annual renewal fees of [OMR X].

2.2.3 Notwithstanding Article 2.2.1, Banks will be required to comply with the requirements set out in Article 4 (Technical Standards and Specifications), Article 5 (Cybersecurity and Information Security), Article 7 (Fair Business Conduct), Article 8 (Customer Protection) and any other requirements and conditions set out in this Framework and as specified by the Central Bank in the no objection letter.

2.2.4 The Central Bank may request from a person applying for exemption to provide any information or documentation that it considers necessary to determine the eligibility for exemption or continued exemption, respectively.

2.3 Licensing

2.3.1 A natural person shall not be granted a License under this Framework.

2.3.2 To be granted a License, an Applicant shall fulfil the following requirements with respect to its legal form:

Permitted Shareholding (i.e., ownership structure)	Omani/foreign nationals who is/are natural person(s), directly or indirectly via a company, can hold 100% ownership and control in a Licensee.
Legal Forms for the Licensee	Commercial companies under the Commercial Companies Law, adopting either of the following legal forms: 1. Limited Liability Company. 2. Joint Stock Company (public/closed).

2.3.3 The Applicant shall establish and maintain an operational office in the Sultanate of Oman. The Applicant shall ensure that at least two (2) key personnel necessary to maintain its operations are ordinarily residing within the Sultanate of Oman at all times.

2.3.4 Licensing Categories

License Category	Services Permitted	Base Capital	On-Going Capital
Open Banking Service Provider	▪ Account Information Services (AIS), and/or ▪ Payment Initiation Services (PIS)	OMR 100,000	Licensees will be required to maintain the applicable base capital requirement throughout the provision of the Open Banking Service. In case the base capital falls below the respective base capital amount during the provision of Open Banking Services activities, the Licensee will be required to infuse the appropriate base capital within seven (7) business days.
Existing NPSL Category 1 PSP Licensee	In addition to the activities permitted to be undertaken by the PSP Licensee: ▪ Account Information Services (AIS), and/or ▪ Payment Initiation Services (PIS)	In addition to the base capital requirement applicable to the PSP Licensee: OMR 100,000	
Existing NPSL Category 2 PSP Licensee			
Existing NPSL Category 3 PSP Licensee	In addition to the activities permitted to be undertaken by the PSP Licensee: ▪ Account Information Services (AIS), and/or ▪ Payment Initiation Services (PIS)	No additional capital is required.	

2.3.5 After receiving the in principle approval, the Applicant shall submit (a) details and proof, by way of deposit slips, that the base capital requirement has been met, and (b) information regarding the sources of funds to meet the base capital requirement.

2.3.6 In the event the Licensee wants to become a PSP Licensee then it shall seek approval from the Central Bank as per the applicable provisions of the NPSL.

2.4 Licensing Conditions

2.4.1 An Applicant or Licensee (as applicable) shall pay the following fees to the Central Bank:

Application Fee (Non-Refundable)	One Time Fee Payable by Applicant	OMR 500
Annual License Fee (Non-Refundable)	Payable by Licensee	OMR 1,000 Annual licensing fee shall be fully waived during the first three (3) calendar years of operations of the Licensee

2.4.2 In addition to the fees stated above, the Central Bank may charge the Licensee specific additional fees as may be required to supervise the Licensee and its operations in the Sultanate of Oman or based on the size of the business operations of the Licensee. Where additional fees are charged, the reasons for the same shall be clearly enumerated by the Central Bank and conveyed to the Licensee in writing.

2.4.3 Central Bank at its sole discretion may waive full or part of any supervision or licensing fees. The Central Bank may also at its discretion consider relaxation of capital requirements for a Licensee (as specified in Article 2.3.4).

2.5 Licensing Process

2.5.1 Each Applicant must fulfil the criteria prescribed in this Framework and demonstrate the capabilities/ competence and resources to comply with the requirements stipulated in the NPSL and the Executive Regulations.

2.5.2 The Central Bank will evaluate each Applicant in accordance with the NPSL, Executive Regulations, and any rules, directions, guidelines, or circulars issued by the Central Bank. Such evaluations will take into account both financial and non-financial parameters.

2.5.3 Application Process

(a) Pre-application: Meeting with the Central Bank to provide a detailed proposal about the business and for the Applicant to gain an understanding of the requirements. The Applicant shall contact the licensing department for a pre-application meeting to discuss: their proposals, business plans, application/licensing process, and requirements. The submission of a meeting request must be sent to the email address: openbanking@cbo.gov.om or through any other mode specified by the Central Bank from time to time.

(b) Submitting application: An authorised representative of the Applicant may submit a new application to the Central Bank for the issuance of a License. The Applicant will submit their application attached with the supporting documents listed in Article 2.5.9 and payment of the requisite application fees. The

submission of application documents must be sent to the email address: openbanking@cbo.gov.om or through any other mode specified by the Central Bank from time to time.

(c) Application review: The Central Bank will review the submitted application and, where necessary, hold further discussions or request additional information/documents from the Applicant. The Central Bank may liaise directly with the Applicant or the Applicant's duly appointed representative when processing the application to seek any further information or clarification.

(d) Evaluation: The Central Bank will conduct a full evaluation of the application, scrutiny under the fit and proper criteria, and make a recommendation to executive management / Board of Governors.

(e) In principle approval/rejection of application: The Applicant will be notified in writing if their application has been approved or rejected.

(f) Fulfil in principle approval requirements: Successful Applicants will be required to comply with the in principle approval conditions and complete technical integration.

(g) Go-live: On readiness, the Applicant is to submit needed compliance and provide go-live information. The Central Bank will then issue the final authorisation and Licence upon satisfactory compliance.

2.5.4 Document Preparation

The Applicant is permitted to appoint a duly authorized representative, such as a law firm or a professional consultancy firm, to prepare the feasibility study as part of the application. The Applicant continues to retain full responsibility for the accuracy and completeness of information/documents provided and is required to certify the details in the application form.

2.5.5 Material Changes

An Applicant must immediately notify the Central Bank during the application review process if there is any material change to the information provided in their application.

2.5.6 Communication of Decision

The Central Bank will communicate the decision to grant, amend, deny, or cancel a License to the Licensee/Applicant or publish the same as it deems necessary.

2.5.7 License Withdrawal or Amendment

(a) The Central Bank may cancel or amend a License based on the Licensee's voluntary surrender of the License or by a decision taken by the Central Bank in accordance with Article 9.1.

(b) The Central Bank may, at its discretion, revoke the License and instruct a Licensee to mandatorily discontinue providing Open Banking Services, including but not limited to the following reasons:

i. Failure to satisfy any of the license conditions.

ii. Violation of the laws and regulations of the Sultanate of Oman, instructions or directives from the Central bank, and the rules contained under this Framework.

iii. If it is proved that the licence was granted on the basis of false, misleading or inaccurate information.

iv. If the Licensee fails to inform the Central Bank of a change in circumstances that the Central Bank considers to be materially relevant to its compliance with any of the requirements of this regulation.

v. The local authorities withdraw any license issued in favour of the licensee.

vi. Ceasing to carry out Open Banking Services within the Sultanate of Oman.

vii. Posing an inordinate risk or threat to the legitimate interests of the Customers.

viii. Posing an inordinate risk or threat to the public interests.

2.5.8 The Central Bank may implement any or all requirements stipulated under Article 9.2 in such a case. Additionally, the Central Bank retains the right to issue any requirements as it may deem necessary for such a withdrawal.

2.5.9 Application Documents and Requirements

The following shall be submitted to the Central Bank by the Applicant for obtaining the License.

(a) The formal application letter, signed by the Applicant's authorized signatory.

(b) Duly completed application form as per Annexure [X].

(c) Governance arrangements and internal control mechanisms.

(d) Before obtaining the in principle approval, the applicant shall submit an anti-money laundering/counter-terrorism financing risk self-assessment report. After obtaining the in principle approval, the Applicant shall submit an anti-money laundering/counter-terrorism financing risk assessment report of the Applicant's business undertaken by an independent third-party expert.

(e) An internal anti-money laundering/counter-terrorism financing risk policy document, including internal control mechanisms to comply with anti-money laundering/counter-terrorism financing requirements under this Framework.

(f) A risk assessment report of the Applicant undertaken by an independent third-party expert, including technical capabilities, operation capabilities,

compliance, potential risks including fraud risks, and measures to mitigate such risks.

(g) An internal risk management policy document.

(h) An internal human resource policy document.

(i) Data protection policy document, including all controls of data classification, data protection, and data segregation to be applied.

(j) Business continuity and disaster recovery policy document, including acceptable recovery point objective/ recovery time objective values.

(k) Framework Contract in terms of Article 8.

(l) Customer complaints handling policy document.

(m) Information technology and information security policy document providing details of the proposed information technology, information security, penetration testing & vulnerability assessment report for the information technology systems, and cybersecurity infrastructure covering the hardware, software, primary and secondary sites, information technology operations, and outsourcing, if any.

(n) Business plan, which must contain the following information:

i. Name of the Applicant entity.

ii. Legal form of the Applicant entity.

iii. Name of owners/ partners/ shareholders of the Applicant entity with the proposed shareholding pattern.

iv. Fit and Proper form as per the format specified by the Central Bank and Curriculum vitae of the Senior Management, and the members of the board of directors (if any), along with their address, contact details, and copy of the identity document (copy of passport/ civil ID), details of Senior Management's experience in banking/ financial services or payments sector/ digital transformation, etc.

v. Business case and value addition that the Applicant will add to the financial industry in the Sultanate of Oman.

vi. Projected financial statements (balance sheet, profit and loss account, and cash flow statement) for the first five (5) years of operation of the Applicant.

vii. SWOT analysis of the Applicant's proposed business.

viii. Proposed organization structure including the proposed members of the boards of directors (if any), Senior Management, and Omanisation plan in line with the Central Bank's requirements.

ix. The proposed business should consist of a minimum of three plans – production, disaster recovery, and test. In addition, the solution architecture for all environments should follow a minimum 3-tier architecture with no access to the design-build team other than the application tier. The deployment architecture diagram should display high availability for each node/ tier with no single point of failure for all three environments.

x. Proposed business model with full transaction flow (end to end) for each service and its distribution channels and targeted customers.

xi. Future roadmap of products and services.

xii. Market segment that the Applicant intends to operate in, competition landscape, market potential, and price point/ monetisation model.

xiii. Compliance arrangements commensurate with the nature, scale, and complexity of its Applicant's business. Regardless of the setup of the compliance arrangements, the ultimate responsibility and accountability for ensuring compliance with applicable laws and regulations will still rest with the Applicant's shareholders, directors and Senior Management.

(o) Fit and Proper Criteria

The Controllers of the Applicant shall satisfy, the following fit and proper criteria:

i. The Controller(s) shall be persons of uprightness, repute, credibility, ability, and quality of judgment;

ii. They shall have sufficient capacity and experience or potential capacity to manage the areas of the business;

iii. They shall not have been convicted of an offence involving fraud or other dishonesty or violence;

iv. They shall not have been involved in, associated with or accused of money laundering or terrorism financing;

v. They shall not have acted in contravention of any statute of the Sultanate of Oman or provisions thereof established for the purpose of protecting members of the public from financial loss due to dishonesty, incompetence, or malpractice by the persons concerned;

vi. They shall not have been involved in any deceptive or oppressive practices that would cast doubt on their integrity and in the business;

vii. A Controller will not be considered to be a fit and proper person if such Controller:

- Is an undischarged bankrupt, currently subject to bankruptcy proceedings, or a bankrupt who has recently been discharged;

- Is subject to receivership or other similar proceedings; and
- Has failed to meet any judgment debt, having regard to the circumstances of such failure and the recency of such failure.

viii. They shall not have been involved associated with, or otherwise conducted themselves any business practices that would cast doubt on their competence and soundness of judgement.

ix. Provided that if the Controller is a legal person, then for the purposes of this Article 2.5.9 (o), the fit and proper criteria shall be fulfilled on behalf of the Controller by the Senior Management of the Controller, by way of an undertaking.

(p) In case the shareholder(s) is/are a juristic person(s), a board resolution from such juridical person(s), confirming the decision to become a shareholder in the Applicant entity.

(q) In case the shareholder is a juristic person, the certificate of incorporation issued by the competent authority in its country of incorporation, commercial license/registration, or any other similar official document.

(r) Details of other commercial activities pursued by all shareholders.

(s) Bank account statements of the Applicant for the previous six (6) months (where available), if specifically sought by the Central Bank.

(t) In case the significant shareholder(s) is/are part of a group of companies, copies of the audited financial statements of that group, for the immediately preceding three (3) years. Significant shareholders in this context means those who will hold 10% or more in the Applicant entity directly or indirectly.

(u) Bank account statement of the significant shareholders for the previous twelve (12) months, if specifically sought by the Central Bank.

(v) Any other requirement the Central Bank may call upon in specific circumstances.

2.5.10 Professional Indemnity Insurance

(a) To be granted a license, the Applicant shall, at the time of submitting an application, hold a professional indemnity insurance.

(b) The professional indemnity insurance referred to in Article 2.5.10 (a) held by an AISP shall cover their liability to Banks, PSP Licensees, Financial Institutions, or the Customers resulting from unauthorized or fraudulent access to or unauthorized or fraudulent use of a Customer’s Data.

(c) The professional indemnity insurance referred to in Article 2.5.10 (a) held by a PISP shall cover liabilities to Banks, PSP Licensees, Financial Institutions, or

the Customers for unauthorized Payment Transactions and non-execution, defective, or late execution of Payment Transactions.

2.5.11 Document Language and Currency Denomination

All documents submitted to the Central Bank as part of the application for a new License must be submitted in hard copy format and through any online methods stipulated by the Central Bank in the Arabic or English language. Additionally, the figures in budgeted financial statements, business plans, or other projections must be expressed in OMR.

2.6 Process of Approval and Timelines

2.6.1 The Central Bank reserves the right, within ninety (90) days of receiving a License application, to:

(a) Require the Applicant to provide additional documents/information that the Central Bank deems necessary to evaluate the application; or

(b) Reject incomplete applications.

2.6.2 An Applicant may withdraw its application at any time during the process by notifying the Central Bank in writing.

2.6.3 After the review of an application, the Central Bank may advise the Applicant in writing whether approval has been granted for the License or if the application has been rejected, including reasons thereof.

2.6.4 The Central Bank will notify the Applicant of the outcome of the License application within a period not exceeding thirty (30) working days from the date of issue of such decision by the Board of Governors.

2.6.5 The Board of Governors and/ or Central Bank reserves the right, at any point in time, to reject an application for a new License considering the interest of the public or if the Applicant fails/refuses to fulfil the licensing conditions and requirements set out by the Central Bank.

2.6.6 The Central Bank has the right to withdraw the license granted to the applicant if it is proved that the applicant has submitted false or inaccurate information or data for obtaining the license.

2.7 Employees

A Licensee must employ qualified and sufficient number of employees with the necessary knowledge and experience to effectively meet operational needs. The staff, as a whole, should possess a diverse range of skills and experience to manage the licensee's affairs in a sound and prudent manner.

3. DATA PROTECTION AND PRIVACY

3.1. Data in Scope

3.1.1. This Framework shall be applicable to Customer Data processed by Licensees and open data, aggregated data provided, generated, shared, or in any other way processed by Banks, PSP Licensees, Financial Institutions, and Licensees.

3.2. Data Processing Principles

3.2.1. The Licensee shall process Customer Data fairly and in a transparent manner in relation to the Customer.

3.2.2. The Licensee shall collect Customer Data for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.2.3. The Licensee's processing of Customer Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

3.2.4. The Licensee shall keep the Customer Data accurate and up to date. The Licensee shall take every reasonable step to ensure that Customer Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. Where Customer Data is obtained by the Licensee from a Bank, PSP Licensee, Financial Institution or any other third party, the Licensee shall not be held liable for inaccuracies therein.

3.2.5. The Licensee shall keep Customer Data in a form that permits identification of Customer only for that period of time that is necessary for the purposes for which the Customer Data is processed. The Licensee shall store and process Customer Data for longer periods of time insofar as the Customer Data is processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with requirements that the Central Bank may prescribe, subject to the implementation of the appropriate technical and organisational measures required in order to safeguard the rights of the Customer.

3.2.6. The Licensee shall process Customer Data in a manner that ensures appropriate security of the Customer Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.3. Customer Data Rights

3.3.1. Customers who are natural persons have the following rights with respect to their Customer Data:

(a) Cancel their consent for the processing of their Customer Data without prejudice to the processing that took place before the cancellation.

(b) Request to modify, update, or block their Customer Data.

(c) Obtain a copy of their processed Customer Data.

(d) Transferring their Customer Data to another controller.

(e) Request the erasure of their Customer Data unless such processing is necessary for national preservation and documentation.

(f) To be notified as the owner of their Customer Data of any hack or violation and the measures taken in this regard.

3.4. Data Governance

3.4.1. The Central Bank may issue directives on data oversight and governance frameworks for Customer Data and open data, and aggregated data to Licensees to ensure compliance with relevant legal and regulatory provisions.

3.4.2. Licensees shall ensure that Customer Data is accurate, up-to-date, and complete.

3.5. Open Data and Aggregated Datasets

In addition to Article 3.4.1, the Central Bank may provide a model to determine the fees, including maximum fees, that Banks, PSP Licensees, and Financial Institutions are entitled to charge for making open data and aggregated datasets available to Licensees, if requested by the Licensees and agreed to by the Banks, PSP Licensees, and Financial Institutions.

3.6. Access to Customer Data

3.6.1. Licensees shall, upon request from a Customer submitted by electronic means, make the Customer Data available to the Customer without undue delay, free of charge, continuously, and in real-time.

3.6.2. Banks, PSP Licensees, and Financial Institutions shall, as agreed between them with the Licensees, and upon request from a Customer submitted by electronic means, make available to a Licensee the Customer Data for which the Customer has granted permission to the Licensee. The Customer Data shall be made available to the Licensee without undue delay, continuously and in real-time. Where a request or service to access Customer Data has been denied or withdrawn by a Bank, PSP Licensee, or Financial Institution to a Licensee, justification must be provided based on the specific situation of the Licensee, to the Customer and the Central Bank.

3.6.3. Banks, PSP Licensees, and Financial Institutions may charge fees from a Licensee for making Customer Data available pursuant to Article 3.6.2, according to the modalities that may be fixed by the Central Bank as per Article 3.8.

3.6.4. When making Customer Data available pursuant to Article 3.6.2, Banks, PSP Licensees, and Financial Institutions shall:

(a) Make Customer Data available to Licensees in a format based on generally recognised standards and at least in the same quality available to the Bank, PSP Licensee, or Financial Institutions;

(b) Communicate securely with Licensees by ensuring an appropriate level of security for the processing and transmission of Customer Data;

(c) Request Licensees to demonstrate that they have obtained the permission of the Customer to access the Customer Data held by the Bank, PSP Licensee, or Financial Institutions.

3.6.5. A Licensee shall only access Customer Data made available under Article 3.6.2 for the purposes and under the conditions for which the Customer has granted permission to the Licensee. A Licensee shall delete Customer Data when it is no longer necessary for the purposes for which the permission has been granted by a Customer unless required to be retained in compliance with applicable regulations or Article 3.2.5.

3.6.6. To ensure the effective management of Customer Data, a Licensee shall:

(a) Not process any Customer Data for purposes other than for providing the Open Banking Services explicitly requested by the Customer.

(b) Put in place adequate technical, legal, and organisational measures in order to prevent the unauthorised or unlawful transfer of or access to Customer Data;

(c) Take necessary measures to ensure an appropriate level of security for the storage, processing, and transmission of Customer Data;

(d) Not process Customer Data for advertising purposes, except for direct marketing in accordance with regulations that the Central Bank may lay down.

(e) Save for the application of the AML/CFT Laws and Regulations and unless the Central Bank instructs otherwise, where the Licensee is part of a group of companies, Customer Data shall only be accessed and processed by the entity of the group that holds a License.

3.6.7. The Central Bank may issue additional rules, directions, guidelines, or circulars, including as provided under Article 3.8, to regulate access to Customer Data by Licensees and the sharing of Customer Data between and among Banks, PSP Licensees, Financial Institutions, and Licensees.

3.7. Data Access Permission Dashboards

3.7.1. Licensees, Banks, PSP Licensees, or Financial Institutions may provide the Customer with a permission dashboard to monitor and manage the permissions a Customer has provided to Licensees. If the Licensees, Banks, PSP Licensees, or Financial Institutions provide a permission dashboard to the Customer, then the following provisions in this Article 3.7 (Data Access Permission Dashboards) shall apply.

3.7.2. A permission dashboard shall:

(a) Provide the Customer with an overview of each ongoing permission given to the Licensee, including:

i. The name of the Licensees to whom access has been granted;

ii. The Customer Payment Account to which access has been granted;

iii. The purpose of the permission;

iv. The categories of data being shared;

v. The period of validity of the permission;

(b) Allow the Customer to withdraw a permission given to a Licensee;

(c) Allow the Customer to re-establish any permission withdrawn;

(d) Include a record of permissions that have been withdrawn or have expired for a duration of two (2) years;

3.7.3. Licensees, Banks, PSP Licensees, and Financial Institutions shall ensure that the permission dashboard is easy to find in its Customer user interface and that information displayed on the dashboard is clear, accurate, and easily understandable for the Customer.

3.7.4. The Banks, PSP Licensees, or Financial Institutions and the Licensee to which consent has been granted by a Customer shall cooperate to make information available to the Customer via the dashboard in real time. To fulfil the obligations in Article 3.7.2 points (a), (b), (c), and (d) above:

(a) Licensees shall inform Banks, PSP Licensees, or Financial Institutions of a new consent granted by a Customer regarding Customer Data held by that Bank, PSP Licensee, or Financial Institution, including:

i. The purpose of the consent granted by the Customer;

ii. The period of validity of the consent

iii. The categories of Customer Data concerned.

(b) Banks, PSP Licensees, or Financial Institutions shall inform the Licensee of changes made to a permission by a Customer via the dashboard, and vice versa.

3.8. Data Sharing Rules

3.8.1. The Central Bank may issue additional rules, directions, guidelines, or circulars to specify the following modalities under which Banks, PSP Licensees, and

Financial Institutions shall make available Customer Data to Licensees pursuant to Article 3.6.2:

(a) Common standards for the storing and processing of Customer Data and common standards for the technical interfaces provided by Licensees to Customers to request Customer Data sharing under Article 3.6.2.

(b) A model to determine the fees, including maximum fees, that Banks, PSP Licensees, and Financial Institutions are entitled to charge for making Customer Data available to Licensees.

3.9. Data Storage and Transfer

3.9.1. If a Licensee transfers or shares Customer Data outside the Sultanate of Oman, then the Licensee shall seek and obtain the approval of the Central Bank, and provide the following additional information:

(a) A statement indicating that the Customer Data would be used or disclosed in such manner;

(b) Sufficient information about the data handling/privacy policy of the Customer Data recipient;

(c) A guarantee that the Customer can obtain further information about such disclosures on request to the Licensee; and

(d) The Customer's consent for the storage or transfer of their Customer Data for one or more specific purposes.

(e) Any other information that the Central Bank may require, including but not limited to data sharing agreements executed by the Licensees on one hand, and Customer data recipient on the other hand.

3.10. Consent Management

3.10.1. Customers shall provide explicit consent to the Licensees for the use of Customer Data by them;

3.10.2. Licensees shall be able to access Customer Data held by Banks, PSP Licensees, and Financial Institutions only upon the explicit consent granted to Licensees by Customers.

3.10.3. Licensees shall disclose to Customers the implications of Customer Data sharing before the Customer authorises and agrees to the terms and conditions of consent.

3.10.4. Customers' consent shall be obtained in an electronic form, and a copy of the consent of the Customer shall be made available to the Customer and preserved by the Licensee.

3.10.5. The Licensee shall re-validate the consent of the Customer annually, except where the Customer has not used the Open Banking Services for 180 days. Then, the Licensee shall re-validate the consent of the Customer after the 180 days lapse from the last date of use.

3.10.6. Licensees shall ensure that the connection through which Customer Data is accessed is configured to terminate upon expiration or withdrawal of the Customer's consent;

3.10.7. Customers shall always have control over Customer Data and be able to access, manage, or withdraw their consent at any point in time; and

3.10.8. The Central Bank may develop and issue a consent management mechanism to the Licensee, which includes a clear set of policies and procedures for Customer consent management.

3.11. Customer Authentication

3.11.1. Licensees shall provide a mechanism to verify the identities of the Customers.

3.11.2. Licensees shall provide authentication mechanisms in an acceptable form that conforms in principle and architecture to the following requirements for authentication:

(a) Authentication must happen over pre-authorized channels (such as email, phone numbers, devices, applications, biometrics, etc.);

(b) Customer authentication endpoint should be verified prior to use for authentication (emails, phone numbers, or other Customer endpoints shall be verified using control information such as OTP verification prior to being used as a platform for procuring consent).

3.11.3. Licensees shall ensure that appropriate Customer authentication methods such as multi-factor authentication and the use of personalised security credentials shall be established to reduce the chance of identity theft or fraud.

3.11.4. Licensees shall implement effective controls to limit the number of login or authentication attempts (e.g., wrong password entries), implementing time-out controls and setting time limits for the validity of authentication. If a one-time password is used for authentication purposes, then Licensees shall ensure that the validity period of such passwords is limited to the strict minimum necessary.

3.11.5. Licensees shall perform adequate identity checks when any Customer requests a change to any contact details that are useful for the Customer to receive important information and monitor the activities of the Customer's Payment Accounts.

3.11.6. Following the receipt of consent by Customers, the Licensees shall activate authentication mechanisms to ensure the security of Customer Data.

3.12. Data Security Standards

The Licensees shall abide by the data and information security standards listed in Annexure [X] of this Framework.

3.13. Data Retention and Deletion

3.13.1. Licensees shall:

(a) Establish clear Customer Data protection and retention policies with protocols for safeguarding information;

(b) Ensure that Customer Data obtained for the purposes of providing Open Banking Services is retained for such minimum period as prescribed by the Central Bank;

(c) Enable methods for the Customers to exercise the right to withdraw consent; and

(d) Ensure that the use, access, or storage of Customer Data is as provided in this Framework.

3.14. Data Breach Policy

3.14.1. Licensees shall:

(a) Undertake regular risk assessment and risk monitoring in order to anticipate potential data threats, hazards, and impacts.

(b) Ensure that the procedures for managing data breach incidents are clearly set out, together with clear roles and responsibilities, lines of escalation, and communication for all parties involved in the Licensee's risk management procedures.

(c) Assess each data breach incident according to its impact in order to determine a proportionate response and trigger the most appropriate command and control arrangements.

(d) Activate the relevant processes and procedures to limit the impact of the incident.

(e) Ensure that affected Customers and all other relevant parties receive efficient, regular, and timely communication in the event of a data incident.

(f) Conduct a robust analysis of the underlying cause of the incident, the efficacy of the incident response, the lessons learned, and the actions required to prevent future similar incidents.

(g) Start the recovery process to ensure minimal disruption to service delivery.

(h) Regularly test adherence to their incident management policies and associated incident management procedures to ensure their adequacy and effectiveness.

3.15. Protecting Against Data Breach

3.15.1. Licensees shall:

(a) Implement strong password and access controls;

(b) Ensure secret credentials remain secret at all times within the Licensee's infrastructure;

(c) Classify all data assets appropriately according to risk, threat likelihood, and sensitivity, distinguishing between personal data and other classified/confidential data;

(d) Manage and monitor access to all data assets and review access quarterly;

(e) Use strong authentication to manage access to data systems and role-based access for data assets;

(f) Train staff appropriately and frequently;

(g) Restrict the ability to download and store data via portable/removable media;

(h) Assess new applications, processes, or services from a security perspective before implementation;

(i) Have a clear and documented data retention and destruction policy in line with extant laws and regulations; and

(j) Ensure that access to Customer Data is restricted to staff who have a demonstrable need to access such data for the performance of their duties.

4. TECHNICAL STANDARDS AND SPECIFICATIONS

The provisions in Annexure [X] on [insert name] shall be complied with by the Applicant for obtaining of License. The Licensee shall continue to comply with the provision of Annexure [insert name] for providing Open Banking Services.

5. CYBERSECURITY AND INFORMATION SECURITY

The provisions in Annexure [X] on [insert name] shall be complied with by the Applicant for obtaining of License. The Licensee shall continue to comply with the provision of Annexure [insert name] for providing Open Banking Services.

6. GOVERNANCE AND COMPLIANCE REQUIREMENTS

6.1. Management Structure

6.1.1. Appointment of Senior Management: Licensees shall appoint Senior Management, responsible for managing and operating the Licensee's current activities. The Senior Management team shall, at a minimum, include:

(a) Chief executive officer/general manager;

(b) Compliance officer;

(c) Chief information security officer;

(d) Chief information technology officer;

(e) Internal audit officer;

(f) Money laundering reporting officer; and

(g) Data protection officer.

6.1.2. Combination of functions: Considering the nature, scale, and complexity of operations, and subject to the Central Bank’s discretion, the same person may occupy the role of the compliance officer and money laundering reporting officer.

6.1.3. Expertise of Senior Management: Licensees shall ensure that individuals appointed as the Senior Management possess the requisite expertise and qualifications to fulfill their roles effectively. Further, Licensees shall ensure that Senior Management continues to meet the following criteria:

(a) Senior Management shall be persons of uprightness, repute, credibility, ability, and quality of judgment;

(b) They shall have sufficient capacity and experience or potential capacity to manage the areas of the business;

(c) They shall not have been convicted of an offense involving fraud or other dishonesty or violence;

(d) They shall not have been involved in, associated with or accused of money laundering or terrorism financing;

(e) They shall not have been involved in any deceptive or oppressive practices that would cast doubt on their integrity and in the business;

(f) They shall not have acted in contravention of any statute of the Sultanate of Oman or provisions thereof established for the purpose of protecting members of the public from financial loss due to dishonesty, incompetence, or malpractice by the persons concerned;

(g) They shall not have been involved in any deceptive or oppressive practices that would cast doubt on their integrity and in the business;

(h) An individual will not be considered to be a fit and proper person if such individual:

i. Is an undischarged bankrupt, currently subject to bankruptcy proceedings, or a bankrupt who has recently been discharged;

ii. Is subject to receivership or other similar proceedings; and

iii. Has failed to meet any judgment debt, having regard to the circumstances of such failure and the recency of such failure.

iv. Any other objectionable findings from the Central Bank of Oman on the applicant

(i) They shall not have been involved or associated with, or otherwise conducted himself any business practices that would cast doubt on their competence and soundness of judgement.

6.1.4. Additional appointments: Considering the nature, scale, and complexity of the Licensee's operations, the Central Bank may require the Licensee to appoint additional Senior Management roles. This may include positions such as a company secretary, chief financial officer, and chief risk officer.

6.1.5. Responsibilities of Senior Management: Senior Management of the Licensee shall monitor and manage the daily activities of the Licensee. These activities shall align with the business strategy, risk level, and policies established by the Licensee.

6.1.6. Authority of the chief executive officer/general manager: The chief executive officer/general manager shall have the authority to act generally in the Licensee's name, representing its interests in concluding transactions and issuing instructions to other senior managers and employees.

6.1.7. Resources for compliance officer: Licensees shall ensure that the compliance officer is provided with sufficient resources, including an adequate number of competent staff, to perform duties objectively and independently of operational and business functions.

6.1.8. Access for compliance officer: The compliance officer shall be granted unrestricted access to relevant records and to the Senior Management, ensuring the effective performance of compliance duties.

6.2. Omanisation

6.2.1. The Licensee shall ensure to comply with the Omanisation ratio as stipulated by the Central Bank from time to time.

6.2.2. The Central Bank may from time to time, specify the Senior Management positions which shall be held only by Omanis.

6.3. Internal Auditor

6.3.1. Establishment and responsibilities: A Licensee shall establish an independent internal audit unit. This unit shall exclusively perform internal audit functions and is strictly prohibited from being assigned or undertaking any responsibilities or tasks outside the scope of internal audit functions. This includes but is not limited to, operational duties, management responsibilities, or any other roles that may compromise the independence and objectivity of the internal audit process. The responsibilities of the internal audit unit shall include:

(a) Evaluating internal policies and controls, ensuring compliance with applicable laws, regulations, and internal procedures;

(b) Preparing quarterly written audit reports, detailing scope, findings, recommendations, and departmental actions on previous audit outcomes;

(c) Operating under a comprehensive, annually updated audit plan; and

(d) Maintaining transparent audit documentation, including results and recommendations, and tracking the implementation of these recommendations.

6.4. External Auditor

6.4.1. Appointment and duties: Licensees shall appoint an external auditor, subject to the prior approval of the Central Bank. The terms of appointment shall ensure the auditor:

(a) Audits financial statements in accordance with the International Financial Reporting Standards (IFRS);

(b) Submits audit reports to the Central Bank on an annual basis; and

(c) Submits separate audit reports for business activities not licensed by the Central Bank.

6.4.2. Central Bank requests: The Central Bank may require the external auditor to:

(a) Provide additional information relating to audits;

(b) Expand or extend the scope of the Licensee's audit; and

(c) Perform any additional examinations as required.

6.4.3. Auditor performance: If the Central Bank determines that the performance of an external auditor has been unsatisfactory, it may direct the Licensee to replace the auditor at the Licensee’s expense.

6.5. Books and Records

6.5.1. Mandatory record-keeping: Licensees shall create and maintain books and records (whether in electronic or hard copy form) that are required for demonstrating compliance with this Framework. These records include:

(a) Detailed financial information, including, financial statements, bank statements, and all accounting records utilized in the preparation, verification, and auditing of the Licensee's financial statements;

(b) Transaction records;

(c) Official minutes from meetings and recorded decisions made by the board of directors or owners/partners (in case there is no board of directors) and Senior Management;

(d) Information regarding any material security or operational incidents;

(e) Records pertaining to security measures, including but not limited to authentication records;

(f) Reports concerning measures taken by the Licensee in the realm of data protection and privacy;

(g) Records of Customer complaints, alongside any remedial actions undertaken in response to such complaints;

(h) Documented reports on occurrences of errors, delays, refunds, or other relevant issues that have been addressed and rectified;

(i) All Customer records required under the AML/CFT Laws and Regulations;

(j) Regularly compiled reports demonstrating the Licensee's compliance with this Regulation and other applicable regulations, rules, decisions, instructions, and circulars;

(k) Essential legal documents, including but not limited to, contracts for employment, contracts appointing external auditors, and;

(l) Agreements central to the Licensee's business continuity, and outsourcing arrangements, along with documents describing the Licensee's approach to corporate governance.

6.5.2. Duration of record retention: Licensees are required to maintain the records listed under Article 6.5.1 above for a minimum period of ten (10) years from the date of their initial creation.

6.5.3. Electronic storage requirements: Licensees shall establish systems and controls for electronic record storage, which should:

(a) Use reliable and secure storage media;

(b) Index and categorize records for easy reference;

(c) Regulate access to prevent unauthorized data access;

(d) Implement a robust backup policy with periodic testing;

(e) Employ digital certification and encryption;

(f) Store records in their original format without alteration; and

(g) Ensure confidentiality of records by authorized personnel.

6.6. Regulatory Reporting and Notifications:

6.6.1. Annual audited financial statements: Licensees shall submit their annual audited financial statements to the Central Bank within three (3) months of the end of their financial year. These statements must be in strict compliance with the International Financial Reporting Standards (IFRS).

6.6.2. Onsite inspection reports: In preparation for onsite inspections by the Central Bank, Licensees shall provide all requested documents and completed questionnaires, within the prescribed time period by the Central Bank from time to time, prior to the inspection team's date of inspection. Following the receipt of the draft inspection report, Licensees must review and submit a detailed assessment of the observations/issues raised within the prescribed time period by the Central Bank from time to time, including supporting documents.

6.6.3. Notification and reporting requirements: Licensees shall notify the Central Bank, and submit relevant reports where necessary, in the following scenarios:

(a) *Matters with serious supervisory impact*:

i. Any occurrence or potential occurrence that may severely undermine the Licensee’s reputation, including significant operational failures or public controversies;

ii. Situations that could critically impede the Licensee’s ability to deliver adequate services to Customers, potentially resulting in substantial harm or detriment to any Customer;

iii. Circumstances that may lead to material financial consequences for Banks, PSP Licensees, or Financial Institutions, including systemic risks or major market disruptions;

iv. Any violation or breach of legal, regulatory, directive, or instructional requirements as set forth by the Central Bank or other authorities;

v. Situations where the Licensee identifies or suspects that it has provided, or might have provided, information to the Central Bank that was or could be false, misleading, incomplete, or materially inaccurate in any respect; and

vi. Plans or intentions to suspend or cease business operations, including applying to the Central Bank for a withdrawal of the License according to Article 9.1, outlining the proposed methodology for such suspension or cessation, with a particular focus on the management and resolution of outstanding liabilities.

(b) *Legal, professional, administrative, or other proceedings*: Any legal, professional, administrative, or other significant proceedings initiated against the Licensee or its Controller that could materially affect the Licensee's financial resources or reputation.

(c) *Fraud, errors, and other irregularities*:

i. Incidents where there is knowledge or suspicion of fraud committed or intended against Customers or the Licensee itself, whether by internal or external parties;

ii. Major operational or security incidents that have or could have a significantly negative impact on the financial interests of Customers, Banks, PSP Licensees, or Financial Institutions, or the Licensee itself;

iii. Cases where an employee is suspected of committing fraud against a Customer;

iv. Identification of irregularities within accounting or other records, regardless of whether there is direct evidence of fraud;

v. Suspicions of serious misconduct by employees, particularly concerning honesty or integrity, that are connected with the Licensee's activities; and

vi. Identification of conflicts of interest that could potentially affect the operation of the Licensee.

(d) *Insolvency, bankruptcy, and winding up*:

i. The initiation of meetings or proceedings to consider resolutions for winding up the Licensee or its Controller;

ii. Applications for dissolution, petitions for winding up, or proposals for compositions or arrangements with creditors concerning significant debt amounts;

iii. The appointment of administrators, trustees in bankruptcy, or receivers to the Licensee or its controller, whether for the entire entity or specific assets.

(e) *External auditor changes*: Changes regarding the Licensee's external auditor, including but not limited to, removal, resignation, or a change in the partner responsible for the audit.

(f) *Capital requirement violations*: Failure to maintain the minimum capital requirements outlined in Article 2.3.4.

(g) *Issues with outsourcing arrangements*: Any material problems or changes encountered with an outsourced service provider.

(h) *Loss of fit and proper status of Controllers*: Any loss of fit and proper status of Controllers as stipulated under Article 2.5.9 (o) above.

(i) Such other reports concerning the condition of the licensee or of any one or more of its branch offices at such times and in such form as may be prescribed by the Central Bank.

6.6.4. Prior approvals: Licensees shall procure the prior approval of the Central Bank for the following:

(a) *Changes in legal status:* Any change in their legal form that might impact their relationship with Customers or alter their liability towards them.

(b) *Modifications to capital*: Any modifications to the Licensee's issued or paid-up capital.

(c) *Control and ownership changes*:

i. A person acquiring or ceasing to have control of the Licensee;

ii. An existing Controller acquiring additional types of control (e.g., ownership, significant influence) or ceasing to hold a type of Control;

iii. An existing Controller increasing their percentage of shares or voting power; and

iv. An existing Controller becoming or ceasing to be a parent undertaking of the Licensee.

(d) *Senior Management Changes:*

i. A change in the management structure of Senior Management;

ii. Appointment or removal of individuals from Senior Management positions.

(e) *Merger, acquisition, and organizational changes*:

i. Licensee merges with another undertaking;

ii. Licensee acquires or disposes of all or a major part of their assets and liabilities, whether within or outside the Sultanate of Oman; and

iii. Licensee modifies their constitutive documents.

(f) *Appointment of external auditor*: The appointment or re-appointment of an external auditor by a Licensee.

(g) *Cessation or suspension of services*: Cessation or suspension of any or all of their Open Banking Services, including applying to the Central Bank for a withdrawal of License according to Article 9.1, or liquidation of the Licensee's business.

6.7. Outsourcing

6.7.1. Definition of outsourcing: Outsourcing refers to an arrangement in which a third party performs an activity, process, or function on behalf of a Licensee, which typically would be conducted internally. This may include core or ancillary functions and services, such as data processing, cloud services, customer call centres, and back-office-related activities.

6.7.2. Notification: Licensees shall notify the Central Bank, within five (5) working days from the date of signing the outsourcing agreement, of any outsourcing to an intragroup entity or third party within or outside the Sultanate of Oman.

6.7.3. Prohibition on outsourcing compliance officer and money laundering reporting officer: The compliance officer and money laundering reporting officer functions shall not be outsourced by the Licensee. Nothing in this Article prohibits the Licensee from relying on a third party's customer due diligence measures, subject to compliance with the AML/CFT Laws and Regulations.

6.7.4. Outsourcing agreements: Licensees are required to execute a service level agreement (SLA), with every outsourcing service provider. This agreement shall explicitly outline the scope of service, rights, obligations, confidentiality and encryption requirements, reporting protocols, and the allocation of responsibilities. Further, the SLA shall allow the Central Bank, external auditors, and the Licensee's internal audit and compliance officer unrestricted access to all relevant information and documents held by the outsourcing service provider concerning the outsourced activities.

6.7.5. Cross-border outsourcing: Where the outsourcing service provider is not situated in the Sultanate of Oman, the Licensee shall ensure that such outsourcing arrangements do not impede the Central Bank's ability to supervise the Licensee. The following considerations, with respect to the jurisdiction in which the outsourcing service provider is located, shall be taken into account:

(a) Economic, political or social conditions;

(b) Differing legal or regulatory systems;

(c) Technology and infrastructure; and

(d) Reputational risk.

6.7.6. Internal policies and procedures: Licensees are required to maintain internal policies and procedures that address strategic, operational, logistical, business continuity, contingency planning, legal, and risk issues related to outsourcing.

6.7.7. Requirements for material outsourcing: 'Material outsourcing' refers to outsourcing arrangements that are significant enough to potentially impact the

Licensee's core operations, reputation, or obligations to its Customers and the Central Bank. Licensees shall seek the Central Bank's prior approval before entering into an SLA for material outsourcing. Licensees engaged in material outsourcing shall:

(a) Develop and maintain extensive outsourcing policies, contingency plans, and risk management procedures;

(b) Ensure that the outsourcing arrangements do not restrict their ability to meet its obligations to Customers and the Central Bank, or impede the Central Bank's supervision of the Licensee.

6.8. Risks, Systems, and Controls

6.8.1. Internal controls: The Senior Management shall assume full responsibility for the establishment, implementation, and oversight of effective internal control systems. The internal controls shall include, but not be limited to, those relating to the following:

(a) The development and or acquisition of the technology solutions to undertake Account Information Services and Payment Initiation Services;

(b) Testing of application program interfaces (APIs);

(c) Standards of communication and access and security of communication sessions;

(d) Safe authentication of Customers;

(e) Processes and measures that protect customer data confidentiality and personalised security credentials;

(f) Tools and measures to prevent fraud and errors;

(g) Security policy;

(h) Information security testing, including web applications testing, configuration reviews, penetration testing, and smart device application testing;

(i) Risk management controls;

(j) AML/CFT procedures;

(k) Record keeping and audit trails; and

(l) Operational and financial controls.

6.8.2. Risk management framework: Licensees shall establish and maintain a comprehensive risk management framework proportionate to the nature, size, complexity, and risk profile of the Licensee, enabling the identification, measurement, management, and monitoring of various risks, including the key

risks highlighted under Articles 6.8.3 to 6.8.9. Licensees shall establish and maintain:

(a) A risk management function;

(b) Risk management policies and procedures; and

(c) Risk measurement and internal reporting methodologies.

6.8.3. Cybersecurity risks: Cybersecurity risks arise from the use of APIs for interconnectivity between Licensees and Banks, PSP Licensees, or Financial Institutions. Licensees shall comply with the requirements outlined in Annexure [X] to mitigate these risks.

6.8.4. Third-party risk: Third-party risks arise from the non-fulfillment of the terms of a contract by third parties. To mitigate these, Licensees shall comply with the requirements stated under Article 6.7.

6.8.5. AML/CFT risks: Open APIs introduce vulnerabilities due to increased interconnectivity and ease of cross-border transactions. To mitigate these, Licensees shall comply with the requirements stated in AML/CFT Laws and Regulations.

6.8.6. Regulatory and compliance risks: Licensees face risks from non-compliance with laws, regulations, and internal policies. To mitigate these risks, Licensees shall:

(a) Adopt and implement a regulatory risk framework;

(b) Establish comprehensive internal controls, including policies, procedures, and risk limits; and

(c) Develop a compliance policy and compliance monitoring manual.

6.8.7. Data integrity risk: Data integrity risks refer to the risk that the data stored and processed by information technology systems are incomplete, inaccurate, or inconsistent across different systems. Licensees shall implement measures to ensure data integrity and availability across information technology systems, including:

(a) Implementing a full audit trail of all transactions; and

(b) Establishing access rules, approvals, revocations, and review procedures.

6.8.8. Product management risk: Product management risks refer to the potential risks associated with the development, offering, and management of Open Banking Services. Open banking increases the complexity of financial services delivery. Licensees shall:

(a) Identify and mitigate risks associated with their Open Banking Services;

(b) Establish policies and procedures for testing and approving new Open Banking Services; and

(c) Clearly communicate the benefits of their Open Banking Services to Customers.

6.8.9. Operational risk: Operational risks refer to the risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. In assessing such risks, the Licensee shall consider the following factors:

(a) Lack of governance and management oversight;

(b) Inadequate internal controls;

(c) Insufficient transaction monitoring;

(d) Failure of information technology through breakdown, incompatibility of legacy systems and poor scalability, poor security, etc.;

(e) Failure or insufficient cyber and information security controls;

(f) Internal and external fraud;

(g) Business continuity and disaster recovery; and

(h) Reputational risks.

6.8.10. Security and fraud incident management: Licensees shall establish comprehensive procedures for handling security and fraud incidents, including:

(a) Identifying individuals responsible for assisting Customers in cases of fraud or security incidents and disclosing the name and email addresses of point of contact for Customers;

(b) Establishing reporting lines for such incidents;

(c) Establishing procedures for escalating incidents internally and reporting such incidents to external parties such as the Central Bank; and

(d) Deploying fraud and security monitoring tools to mitigate risks.

6.8.11. Security policy documentation: Licensees shall maintain a detailed security policy document covering the following:

(a) Technology architecture and system documentation:

i. Detailed overview of the information technology systems supporting operational activities;

ii. Description of authorized external connections (e.g., partners, service providers, remote employees), including their purpose;

iii. Security measures for each external connection, detailing the Licensee's control over access, nature, and frequency of security checks; and

iv. Procedures for managing communication lines, including their opening/closing, security equipment configurations, key generation, Customer authentication, system monitoring protocols, and security features such as intrusion detection and antivirus systems.

(b) *Internal information security system security*: Logical security measures and controls for internal information technology system access;

(c) *Physical security measures***:** Security protocols for physical premises and data centers, including access control and environmental safety measures.

(d) *Account information and payment initiation security***:**

i. Security procedures for customer authentication;

ii. Protocols for secure delivery of tokens to legitimate customers; and

iii. Description of the integrity of authentication factors, tokens, and online and mobile applications.

6.8.12. Business continuity planning: Licensees shall have a comprehensive business continuity plan that includes:

(a) *Business impact analysis*: Analysis of business processes and determination of recovery objectives, including recovery time and point objectives, as well as identification of critical assets;

(b) *Disaster recovery infrastructure*: Identification of a backup site and necessary information technology infrastructure and details of key software and data crucial for recovery from disasters or disruptions;

(c) *Recovery and continuity procedures*: Description of the procedures that the Licensee will follow in the event of a disaster or incident, such as failure of key systems, loss of key data, inaccessibility of premises, and loss of key personnel; and

(d) *Testing*: Description of how the business continuity and disaster recovery plans will be tested and the frequency of such tests.

6.8.13. Independent system evaluation: Licensees shall ensure their systems and controls, including business continuity, disaster recovery, and cyber resilience, are independently tested upon implementation, after material changes, and at least every three (3) years.

6.8.14. Procedures for PISPs: PISPs shall establish procedures to ensure:

(a) *Customer information sharing*: PISPs shall not disclose any Customer Data to third parties, except to the payee and only with explicit consent from the payor;

(b) *Identification in Payment Transactions*: Each time a PISP initiates a payment order on behalf of a Customer, it shall securely identify itself to the Bank, PSP Licensee, or Financial Institution where the Customer holds a Payment Account;

(c) *Usage and storage of information*: PISPs are prohibited from accessing, using, or storing any Customer Data for purposes other than providing the Payment Initiation Service explicitly requested by a Customer. However, they may retain details of Payment Transactions initiated by the Customer, including payment amounts, Payment Account details, reference numbers, execution dates, times, and the payee's IBAN, as applicable for meeting the Central Bank's compliance requirements;

(d) *Integrity of transaction details*: PISPs shall not modify any aspect of a transaction as notified by the Customer, including the amount, payee, or other transaction features; and

(e) *Data encryption and access control*: All Customer Data accessed and stored by PISPs shall be encrypted during transmission and while at rest. Access to this Customer Data shall be strictly controlled to prevent unauthorized access within the Licensee's organization.

6.8.15. Procedures for AISPs: AISPs shall establish procedures to ensure:

(a) Provision of services based on consent: AISPs must ensure that Account Information Services are provided solely upon receiving explicit consent from the Customer;

(b) Data encryption and access control: All data accessed and stored by PISPs shall be encrypted during transmission and while at rest. Access to this data shall be strictly controlled to prevent unauthorized access within the Licensee's organization; and

(c) Secure Communication: For each communication session, AISPs shall communicate securely with the Banks, PSP Licensees, or Financial Institutions and the Customer, adhering to the regulatory requirements stipulated in this Framework.

6.9. AML/CFT

6.9.1. Compliance with AML/CFT Laws and Regulations: Licensees shall comply with the AML/CFT Laws and Regulations and address money laundering and terrorist financing risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, and detect money laundering and terrorist financing activities. All references in AML/CFT Laws and Regulations to "*Financial Institutions*" shall be read as references to "*Licensees*".

6.9.2. Digital onboarding: Licensees are allowed to digitally onboard Customers subject to compliance with the E-KYC Circular. All references in the E-KYC Circular to "*licensees*" shall be read as references to "*Licensees*" as defined in this Framework.

6.9.3. Customer due diligence tiers in E-KYC Circular: AISPs will be permitted to conduct simplified due diligence on Customers in accordance with Article 4 of the E-KYC Circular. PISPs shall follow a tiered approach to conduct Customer due diligence considering the nature, scale, and complexity of their operations, and subject to the Central Bank's discretion.

6.9.4. Tipping off: The following shall not be deemed to be a violation of the confidentiality requirement stated under Article 49 of Royal Decree No. 30/2016 promulgating the Law on Combating Money Laundering and Terrorism Financing:

(a) Sharing of Customer Data or information between the Licensee and Banks, PSP Licensees, or Financial Institutions, with respect to suspicious transactions; and

(b) Failing to initiate a Payment Transaction or to share Payment Account information because the Bank, PSP Licensee, or Financial Institution is currently investigating a Customer.

7. FAIR BUSINESS CONDUCT

7.1. Fair Treatment

7.1.1. The Central Bank shall aim to secure and maintain fair competition among all Licensees vis-à-vis Banks, PSP Licensees, and Financial Institutions.

7.1.2. Licensees shall treat their Customers equitably, honestly, and fairly.

7.1.3. In this regard, the Central Bank may, from time to time, issue guidance on prohibited conduct for Licensees, and prescribe affirmative obligations for Licensees.

7.2. Prohibited Conduct

7.2.1 Anti-competitive agreements: The Licensees shall be prohibited from entering into or implementing agreements that abuse, restrict, or prevent competition, in particular those agreements that aim to fix purchase or sale prices of Open Banking Services by causing increase, reduction, or fixing of prices, thereby adversely affecting competition, as well as collusion in bids or proposals in tenders, and other offers. Anti-competitive agreements shall include but shall not be limited to:

(a) Price fixing agreements

(b) Exclusivity agreement

(c) Tie in arrangements

7.2.2 The Licensees shall be prohibited from independently or in collusion with, Banks, PSP Licensees, and Financial Institutions engaging in discriminatory, exploitative, and abusive conduct in the market. Such conduct shall include but shall not be limited to:

(a) Limiting conduct: The Licensee shall be prohibited from unduly limiting, refusing, or hindering a Customer's ability to work with another Licensee, or to limit, refuse, or hinder the Customer's right to obtain Open Banking Services from another Licensee.

(b) Screen scraping: The Licensee shall be prohibited from gathering data shown on a web interface to use such data for a purpose other than for the provision of Open Banking Services to the Customers. All data processing shall be done in the manner prescribed in Article 3.

(c) Bundling: The Licensee shall not provide or make available any products or services collectively, such that the Open Banking Services are not available or accessible independently to the Customers.

(d) Any other denial of market access: The Licensee shall not involve or indulge in practices that result in denial of market access to other Licensees, Banks, PSP Licensees, or Financial Institutions in any manner.

7.3. Liability for Unauthorized Transactions

7.3.1. In case of a transaction that was not authorised and consented to by the Customer:

(a) The Bank, PSP Licensee, or Financial Institution shall refund the funds to the Customer that have been erroneously debited or credited in the payer Payment Account; and

(b) The Licensee shall immediately compensate the Bank, PSP Licensee, or Financial Institution if the Licensee is liable for the unauthorised Payment Transaction.

(c) For the purposes of this Article 7.3.1, the burden shall be on the Licensee to prove that, within its sphere of competence, the Payment Transaction was authenticated, accurately recorded, and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

(d) Any additional financial compensation may be determined in accordance with the agreement between the Bank, PSP Licensee, or Financial Institution and the Licensee.

8. CUSTOMER PROTECTION

8.1. General Principles:

A Licensee shall comply in spirit with the following principles, in all their dealings and interactions with the Customers:

8.1.1. Equitable and Fair Treatment

The Licensee shall treat all Customers equitably, honestly, and fairly at all stages of their relationship with the Licensee, as further enumerated in Article 8.3 below.

8.1.2. Disclosure and Transparency

The Licensee shall ensure that the information about the Open Banking Services provided to or offered to Customers is clear, comprehensible, updated, and concise manner. The information shared should be easy to access and understand and should not be incomplete or misleading. The information must include, amongst others, the details of the Licensee's licenses and permissions, the description of the rights and responsibilities of each party, the details of the prices and commissions charged by the Licensee, details of any outsourcing to any third parties utilised in the provision of Open Banking Services, any actual or potential instances of conflict of interest and the mechanism and consequences of terminating the relationship.

8.1.3. Education and Awareness

The Licensee shall develop appropriate programs and mechanisms to improve the knowledge and skills of the Customers, raise their level of awareness, enable them to understand major risks, and help them to make informed and effective decisions as well as help them know the concerned entity to obtain information if needed.

8.1.4. Systems of Licensee

The Licensee must work in a highly professional manner for the benefit of the Customers and implement systems and controls that protect the best interest of the Customer, including the protection of the Customer or Customer's funds against fraud. To this end, the Licensee shall employ or engage skilled and experienced personnel and implement adequate technical and control systems that are efficient and effective in limiting and detecting fraud, embezzlement, or misuse of Customer funds.

8.1.5. Protection of Data and Information Privacy

The Licensee must develop appropriate mechanisms to protect the privacy of the Customer Data as further enumerated in Article 8.4. The Licensee must also establish high-level control systems that include appropriate mechanisms specifying the purposes for which Customer Data is collected.

8.1.6. Complaints Handling

The Licensee must have an appropriate mechanism in place for Customers to submit their complaints, and the mechanism must be clear and effective. In addition, the Licensee must consider each complaint, take the measures and procedures necessary to fairly and effectively resolve the complaint, and provide the best and most appropriate solutions without delay in accordance with the relevant regulations and instructions, including in accordance with the articles of this Framework.

8.2. Exercise of Duties of Licensee

The Licensee shall, when conducting their business or operations from or through the territory of Sultanate of Oman, undertake its activities keeping the spirit of the principles stipulated under Article 8.1, without compromising on market integrity, the reputation of the Sultanate of Oman as a country and its ongoing legal and regulatory compliance under the extant laws of the Sultanate of Oman.

8.3. Fair Treatment of Customers

8.3.1. The Licensee must be able to evidence that it consistently delivers Open Banking Services, while treating all its customers fairly. The policies and practices of the Licensee must:

(a) Give Customers confidence that they are dealing with a Licensee where the fair treatment of customers is central to the corporate culture;

(b) Ensure that Customers are: (i) not subject to unfair discriminatory practices, including unfair contract terms that significantly disadvantage Customers; or (ii) subject to applicable laws and regulations of the Sultanate of Oman, discriminate against Customers on grounds of nationality, ethnicity, religion, social background or gender, etc.

(c) Provide Customers with clear information and are kept appropriately informed before, during, and after the point of sale, including the costs, risks, and important exclusions or limitations;

(d) Ensure that the staff, representatives, and agents of the Licensee exercise due care, skill, and diligence when dealing with Customers;

(e) Ensure that the Customers do not face unreasonable post-onboarding barriers imposed by Licensees to change products, switch providers, submit a claim, or make a complaint.

8.4. Data Protection, Confidentiality

8.4.1. A Licensee must protect and maintain the confidentiality of Customer Data, including when it is held by a third party or agent of the Licensee, unless otherwise provided for in this Framework. The Customer Data may be

accessed and used only by such personnel, agents, and staff of the Licensee who need to have access to such data.

8.4.2. A Licensee must not disclose Customer Data except where:

(a) Required, pursuant to applicable laws and regulations; or

(b) The disclosure is made with the prior written consent of the Customer.

8.4.3. A Licensee shall put in place and maintain:

(a) Adequate policies, procedures, and controls, as well as employee awareness training, to protect Customer Data and to identify, act to prevent and resolve any information security breaches;

(b) Data protection controls in accordance with the requirements under Article 3; and

(c) Measures to protect cybersecurity and technology-related compliances, in accordance with Articles 4 and 5, to the extent such compliances are essential to protect the best interests of the Customer.

8.5. Marketing and Advertisement

8.5.1. A Licensee must ensure that any advertising or promotional material for Open Banking Services, comply with the requirements stipulated below:

(a) All advertising or promotional material should be fair, clear, not misleading and should not omit information that is important for a Customer to make an informed decision in relation to the Open Banking Services;

(b) All advertising or promotional material should prominently disclose the full name, regulatory status, and address details of the Licensee.

(c) All text and numbers stated in such material should be clearly visible and understandable, with a legible font size used for all text (including footnotes, endnotes, and disclaimers).

(d) The advertising and promotional material is designed and presented so that any customer can reasonably be expected to understand that it is an advertisement and that the availability of the Open Banking Services may require the Customer to meet certain criteria.

(e) All advertising and promotional material must be approved in writing by the compliance function of the Licensee, after having vetted its compliance with the Licensee's internal marketing policies and applicable laws and regulations of Open Banking Services, including but not limited to those relating to marketing, data protection, and financial consumer protection.

(f) Advertising or promotional material shall not be sent to any person under the age of 18 years, where such material presents unsuitable risk to such customers.

(g) Any targeted marketing is undertaken responsibly by suitably licensed entities and presented to the audience only appropriate products or services.

(h) All advertising or promotional material must comply with all applicable laws, regulations, guidelines, or other rules applicable across the Sultanate of Oman.

8.5.2. For the purposes of this Framework, marketing, promotion, or advertising includes, but is not limited to, any direct or indirect form of the below:

(a) Communications, publication of data, information, promotional-influenced or sponsored material across any traditional and new-age multi-media channels, etc.;

(b) Communications (whether written or spoken), including through letters, e-mails, and any other correspondence and telephone conversations, product brochures or fact sheets; press releases; magazines, journals, or newspaper advertisements; web content; correspondence, newsletter, or mailshot; or presentation by flip book or other means;

(c) Self-generated or third-party published social media posts/blogs, comments, endorsements, non-written communications, banners/billboards, videos, live streams, etc.;

(d) Events or promotional activities held in the Sultanate of Oman to encourage market participation in the sector, specifically soliciting clients or incentivising access to the Open Banking Services;

(e) Any invitation or inducement to enter into an agreement regarding the Open Banking Services provided by the Licensee or offered by another person, including a Bank, a PSP Licensee, or a Financial Institution; or

(f) Advertisements, paid or non-paid, and all forms of publicity-driving content served across any platform and channel, etc.

8.6. Contractual Agreements

8.6.1. Requirement for Written Contracts

(a) The Licensee shall, prior to the commencement of the Open Banking Services, enter into a Framework Contract with each Customer, which specifies the Licensee's duties and responsibilities when providing Open Banking Services.

(b) The Licensee shall provide warning statements, as may be necessary, to notify the Customer of any potential risks, along with the Framework Contract.

(c) A Licensee must supply the Framework Contract to each of its new Customers, at least ten (10) days prior to the commencement of the provision of Open

Banking Services so that the Customer may make an informed decision as to whether or not to proceed. The Framework Contract shall be communicated to the Customer in writing and delivered in accordance with the Customer's preference.

(d) The Licensee must obtain valid acceptance from the Customers, which must be given in a form that is compliant with all applicable laws and regulations of the Sultanate of Oman. The acceptance of the Framework Contract must be procured from the Customer prior to the start of the Open Banking Services.

(e) The Framework Contract, as approved by the Central Bank under Article 2.5.9 (k), must be drafted in Arabic and English in a simple, clear, and direct language.

(f) The Framework Contract must comply with all applicable laws, including but not limited to applicable consumer protection laws, and should ensure compliance with the general requirement to act honestly, fairly, and in the best interests of its clients and the integrity of the market.

(g) The Framework Contract must at all times be fair, transparent, accurate, and not misleading. The agreements or written terms and conditions must be sufficiently clear to the Customer, with regard to the nature of the Open Banking Services and the intended market for such services.

(h) The Licensee must send a copy of the Framework Contract to each Customer after it has been executed. Additionally, a Licensee must supply a document detailing the Framework Contract to each of the existing Customers, at their request.

(i) At the request of the Customer, the Licensee must supply the Customer with documents relating to the orders, invoices, and split of charges under the Framework Contract.

(j) The Framework Contract, and any information related to the terms and conditions in the Framework Contract, shall be communicated to the Customer in writing and delivered in accordance with the Customer's preference.

(k) The Licensee shall communicate any changes or amendments in the Framework Contract conditions at least thirty (30) calendar days in advance of any such changes being implemented. If a Customer does not agree to the revised terms and conditions, the Customer will be provided the right to terminate the contractual relationship at no charge or penalty. The Customer shall be required to communicate to the Licensee of non-acceptance of any such terms prior to the lapse of the thirty (30) day period.

(l) The Licensee must maintain a record of all versions of the written agreements with the Customer and be able to identify all changes made between versions.

(m) The Licensee may charge such fees and charges which reasonably correspond to the Licensee's costs and expenses and reasonable profit margins. Furthermore, the Framework Contract and any documents provided

thereunder, must adequately disclose all applicable charges that may be levied on a Customer, including relevant exchange rates, any reimbursable expenses, currency conversion charges, refund and credit mechanisms, floating charges, cancellation charges, etc. The Customer shall not be liable to pay for any charges of which the Customer has not received sufficient notice in writing. The Customer shall not be charged for any information that the Customer is required to share with the Licensee under law or contract.

(n) Except where the Customer has acted fraudulently or has with intent or gross negligence, failed to ensure that its personalised security credentials are not accessible to persons other than the Customer, the Customer is not liable for any losses incurred in respect of an unauthorised transaction:

i. Arising after notification to the Licensee in the agreed manner on becoming aware of the loss, theft, misappropriation, or unauthorised use of the Customer's personalised security credentials;

ii. Where the Licensee has failed at any time to provide the Customer appropriate means to enable a Customer to notify the Licensee of the loss, theft, misappropriation, or unauthorised use of the Customer's personalised security credentials; or

iii. Where the Licensee has failed to apply strong customer authentication processes.

8.7. Content of the Framework Contracts

8.7.1. The Framework Contract must provide the information set forth below:

(a) The name, address, and contact details of the Licensee;

(b) A description of the main characteristics of the Open Banking Services provided;

(c) The information or unique identifier that must be provided by the Customer in order for a transaction to be properly initiated or executed;

(d) The manner in which the Open Banking Services may be provided and details of any part of the Open Banking Services that are undertaken through a third party, including where such vendors are located outside the territory of Sultanate of Oman;

(e) Details of any transaction limits, any time period for cancelling a transaction or order, and timelines for completing a transaction or order;

(f) Schedule of fees, charges, and commissions, including currency and conversion rates, any reimbursable expenses, withdrawal charges, floating charges, where applicable;

(g) Safeguards and corrective measures adopted by the Licensee to protect the Customer's Data, including mechanisms for providing or revoking consent by the Customer;

(h) Means of communication agreed between the parties for the transmission of information or notifications under the Framework Contract;

(i) Identification of third-party service providers to whom any portion of the Open Banking Services are outsourced, along with the description of the services they perform;

(j) Clearly identify that the Licensee does not at any time have control of the Customer's funds;

(k) The secure procedures by which the Licensee will contact the Customer in the event of suspected or actual fraud or security threats;

(l) Measures adopted by the Licensee to stop or prevent unauthorised transactions;

(m) The conditions for any refunds, cancellations, or rejection of orders;

(n) Liability of the Licensee to the Customer, including any exclusions based on the Licensee's contractual arrangements with a Bank, PSP Licensee, or Financial Institution, including any relating to fraud, unauthorised transactions, etc.;

(o) Liability of the Customer under the Framework Contract;

(p) Notification to the Customer that the Customer must fulfil the necessary AML/KYC verifications, failing which the Licensee may immediately suspend or terminate the Framework Contract;

(q) Provisions relating to amendments to the Framework Contract, term of the Framework Contract, and each party's right to termination;

(r) Complaints handling procedures under the Framework Contract;

(s) Governing law of the Framework Contract and dispute resolution mechanism.

8.8. Order & Execution Process

8.8.1. Immediately after the receipt of an order for a transaction, the Licensee must provide each of its Customers with:

(a) A confirmation of the successful or unsuccessful initiation and execution of the transaction;

i. A reference number to track the status of the transaction, including the date and amount of the transaction, the amount of the transaction, the charges associated with the transaction (including any related fees or charges, including

the actual currency and conversion rates used, and withdrawal charges) and the date on which the Licensee received the order.

8.8.2. The Licensee must implement procedures to detect when any information in any transaction initiated is missing or inaccurate. If any of the information is missing or inaccurate, the Licensee must either:

(a) Reject the order;

(b) Obtain the missing or corrected information from the Customer before initiating the transaction.

8.8.3. A Licensee may refuse an order only if:

(a) The conditions for rejecting orders as set out in the Framework Contract are established;

(b) The Licensee has grounds to suspect that the transaction is fraudulent or poses a money-laundering or terrorism-financing risk; or

(c) The transaction would breach any of the Licensee's obligations under applicable regulations or laws.

8.8.4. When an order is refused, the Licensee must (to the extent permitted by applicable law) notify the Customer in a timely manner of the refusal and be provided with objectively justifiable reasons for the refusal, as well as details on how to rectify the problem.

8.8.5. A Licensee must provide each of the Customers with a statement of the transactions under a Framework Contract at least once per month free of charge, including details of the amounts, the fees, charges, and commissions, the dates and times of execution, and the reference numbers for each transaction.

8.9. Customer Complaints

8.9.1. Complaint Resolution – Core Rules

(a) The Licensee shall put in place a formal, publicly disclosed customer complaint redressal, dispute management framework and escalation matrix, including designating an officer/executive to handle the customer complaints. The complaint facility, if made available on website / mobile, shall be clear and easily accessible. The customer complaint framework shall stipulate the Licensee's timelines for addressing customer complaints and any changes to such timelines shall be communicated by the Licensee to the Customer.

(b) A Licensee must ensure that complaints raised by a Customer are handled and addressed in a fair and timely manner. Except as required under law, all Customer complaints shall be maintained confidential by the Licensee. On receiving a complaint, the Licensee must make every effort to address all points

raised in its reply to the customer making the complaint. Systems and procedure failures shall be resolved in least possible time.

(c) The Licensee shall acknowledge the receipt of all complaints within 24 hours. The Licensee shall investigate all complaints promptly and resolve complaints as soon as practicable within a reasonable period of time which shall be informed to the Customer.

(d) If the resolution takes longer, the Licensee shall inform the customer with the revised timeline, clearly mentioning the reasons of delay in resolution.

(e) Where the provision of Open Banking Services involves any third-party entities, the Licensee shall establish procedures to facilitate the handling of such complaints between their Customer and such third-party entities (including Banks, PSP Licensees and Financial Institutions). The Licensee shall remain responsible for the resolution of such complaints.

(f) The Licensee shall not impose any fees or charges for the acceptance or handling of any complaints.

(g) The Licensee shall adequately train its staff in handling Customer complaints.

(h) The Licensee must ensure that the personnel handling Customer complaints are able to act impartially and do not have any conflict of interest.

(i) The Licensee shall review its complaints handling procedures annually. Further, once a year, the Licensee shall review reports enlisting the complaints received from Customers and identify any recurring or systemic problems, including but not limited to:

(i) Analysing the causes of complaints so as to identify common causes of complaints;

(ii) Considering whether such root causes may also affect other processes, services, including those not directly complained of; and

(iii) Correcting such causes.

8.10. Internal Complaint Resolution Process

8.10.1. A Licensee must, at a minimum:

(a) Have a role or function that handles customer complaints and operates a complaints handling system that facilitates the recording, tracking, categorization, and status of complaints;

(b) Make an easy-to-use template form for filing complaints available to customers and provide accessible means, along with clear instructions, on where such complaints can be submitted. However, it shall not limit Customers to only

submitting complaints through one channel or in one form in order to be recognised as a complaint;

(c) Make other channels of complaint registration available to customers, including telephone lines, online channels, and postal communications.

(d) Provide or make available its complaint handling procedures (including how to make a complaint and the documentation required, as well as the Customer's right to make a complaint through the Licensee's available channels);

(e) Provide or make available all necessary details to be used by the Customer for following up on a complaint;

(f) Resolve the complaint within the period stipulated under the customer complaint framework (unless the Customer has confirmed that the complaint has been resolved before the end of this period);

(g) Document the channel used to communicate with a customer in relation to complaints and retain details of each complaint; and

(h) Provide the information required by a Customer who wishes to escalate its complaint to the Licensee or to the Central Bank as a result of being dissatisfied with the result of the resolution of their complaint and direct the Customer to the relevant party.

8.10.2. A Licensee must submit details of its complaints handling procedures to the Central Bank. Central Bank may review these procedures and direct it to alter or amend the complaints handling procedures in accordance with the requirements of applicable laws and regulations.

8.10.3. Escalation process

(a) When the Customer has verbally expressed dissatisfaction with any Open Banking Service and the matter cannot be resolved by the frontline staff of the Licensee, the Licensee's front-line staff must inform the Customer of his/her right to file a written complaint through the Licensee's complaint management process.

(b) When a Customer's dissatisfaction with any Open Banking Service is verbally expressed, but the Customer does not wish to pursue it as a formal complaint, the Licensee must maintain a log of the Customer's expression of dissatisfaction. The log will detail the date, issue, and outcome and should form part of the analysis of the Licensee.

(c) When a Customer wants to pursue a complaint, by submitting a formal written complaint, the Licensee must designate personnel of sufficient seniority to review the complaint and obtain a resolution.

(d) If the Customer continues to be dissatisfied with the resolution, then the Licensee and the Customer may, at its discretion, escalate the matter to:

i. Either the dispute resolution mechanism stated in the Framework Contract; or

ii. File a complaint to the customer service department at Central Bank.

8.11. Record of Complaints

8.11.1. The Licensee shall keep a record of:

(a) All complaints received from their Customers;

(b) All measures they have taken in response to complaints; and

(c) The resolution of all complaints.

8.11.2. The Licensee shall retain the records of the complaints for the period of two (2) years from the date of resolution or closure, whichever is latest.

8.12. Reporting of Complaints

8.12.1. A Licensee must report to the Central Bank on an annual basis the complaints that it has received from its Customers in such form as the Central Bank may direct.

8.12.2. The report shall include details on the complaint, the details of the Customer, the communication channel, the resolution status of the complaint, the complaint resolution process adopted, and remedial/corrective measures undertaken by the Licensee.

8.12.3. Such data may be requested by the Central Bank at its discretion.

8.13. Filing of Complaints to Central Bank

8.13.1. The Central Bank shall only receive Customer complaints in the event that a resolution process with the Licensee is unsuccessful under the provisions of the Framework Contract.

8.13.2. The Central Bank will maintain provisions to receive Customer complaints. The Central Bank will consider such complaints and may follow them up with a Licensee to determine any corrective actions to be taken. Further, where it deems it appropriate, the Central Bank may refer the Customer to other competent authorities or entities to address their complaints.

8.13.3. The Central Bank may undertake such procedures, investigations, and regulatory actions as necessary to investigate the complaint filed against the Licensee. The Licensee shall assist the Central Bank in any investigations. If so directed by the Central Bank, submit to the Central Bank with all relevant data, facilities, books, records, accounts, documents, and other information for examination.

8.13.4. The Central Bank may, after completion of its investigation, either:

(a) Reject the complaint; or

(b) Recommend any remedial and corrective actions necessary to protect the interest of the Customer.

8.13.5. While enforcing any remedial or corrective actions, the Central Bank shall act in accordance with its powers under the Banking Law and NPSL and the regulations issued thereunder.

8.13.6. If either the Customer or the Licensee are dissatisfied with the actions or decisions of the Central Bank in relation to the complaint, then either party, may seek formal dispute resolution in accordance with the dispute resolution process mentioned in the Framework Contracts.

8.13.7. The Central Bank, may, based on its findings under an investigation process, adopt other enforcement actions against the Licensee, including but not limited to the enforcement actions under the Banking Law and the NPSL. If the Licensee has any complaints against such actions of the Central Bank, it may, at its option, approach the courts of the Sultanate of Oman for redressal of its complaints.

8.14. Whistleblowing

8.14.1. A person who makes a disclosure of information specified in Article 8.14.2 to a person specified in Article 8.14.3 is, for the purposes of this Framework, referred to as a 'whistleblower.' A whistleblower is entitled to the protection in Article 8.14.4.

8.14.2. For the purposes of Article 8.14.1, the disclosure of information made by the person must:

(a) Relate to a reasonable suspicion that a Licensee or, an officer or employee of a Licensee has or may have:

i. Contravened a provision of any applicable law and regulations; or

ii. Engaged in money laundering, terrorism financing, fraud, or any other financial crime;

(b) Be made in good faith.

8.14.3. For the purposes of Article 8.14.1, the disclosure of information is made to any one or more of the following:

(a) The Senior Management or compliance officer of the Licensee;

(b) An auditor, or a member of the audit team, of the Licensee;

(c) The Central Bank; or

(d) A criminal law enforcement agency in the Sultanate of Oman.

8.14.4. Where a whistleblower makes a disclosure as referred to in Article 8.14.1:

(a) The person shall not be subject to any civil or contractual liability for making that disclosure;

(b) No contractual, civil, or other remedy or right shall be enforced against the person by another person for making that disclosure; and

(c) The person shall not be dismissed from his current employment, or otherwise subject to any action by his employer or any related party of the employer which is reasonably likely to cause detriment to that person, for making that disclosure.

8.14.5. A Licensee must have appropriate and effective policies and procedures in place to facilitate the reporting of regulatory concerns made by a whistleblower and for the assessment and, where appropriate, escalation of those concerns. The procedures/various channels available for whistleblowing should be well publicized and periodically reviewed.

8.14.6. Where a whistleblower makes a disclosure to the Central Bank, the Central Bank may investigate such disclosures, and depending on the findings of its investigation, adopt any remedial, corrective, or enforcement actions, in accordance with the provisions of the Banking Law and NPSL.

8.14.7. If the Licensee has any complaints against such actions of the Central Bank, it may, at its option, approach the courts of the Sultanate of Oman for redressal of its complaints.

9. Participant Exit

9.1. License Withdrawal Process

9.1.1. If the Licensee elects to discontinue providing Open Banking Services, the Licensee shall submit an application to the Central Bank in the form as prescribed under this Article 9.

9.1.2. The Central Bank shall take into account various factors for assessing the request for withdrawal of the License, including but not limited to the following:

(a) Relevant and adequate resources, including capital, liquidity, knowledge, and manpower to withdraw the License in an orderly and timely manner;

(b) Provide a notification to all Customers in regard to its intention to withdraw the License a minimum of sixty (60) days in advance;

(c) Publish an advertisement in an English and Arabic daily newspaper, in circulation in the Sultanate of Oman, in regards to its intention to withdraw its

license. This advertisement must be published a minimum of sixty (60) days in advance.

(d) The Licensee has discharged all obligations owed to the Customers, Central Bank, PSP Licensees, Financial Institutions, and any other parties relating to its business at the time of making application of withdrawal and/or has provided a plan for discharging its obligations owed to the Customers prior to the date of License withdrawal;

(e) Transfer or migration of the Customers to another Licensee regulated by the Central Bank;

(f) Deletion of Customer Data or obtaining of consent for retention of Customer Data for the purposes of performance of any obligations or provision of services by the Licensee outside the scope of this Framework;

(g) Unresolved, unsatisfied, or anticipated complaints, against the Licensee or its employees;

(h) Proposed processes to hold records in a secure and accessible form for as long as required by the Central Bank upon withdrawal of License;

(i) Outstanding fees payable to the Central Bank under this Framework or otherwise;

(j) Any other factors that the Central Bank would reasonably expect to be resolved before granting a request for the withdrawal of a License.

9.2. Withdrawal Plan Requirement

9.2.1. If the Licensee elects to discontinue providing Open Banking Services, the Licensee shall submit a detailed withdrawal plan to the Central Bank in addition to the application, as stipulated under Article 9.1, for its approval. The withdrawal plan must address the factors to the satisfaction of the regulator, including but not limited to the following:

(a) Evaluation of the resources that are needed to facilitate an orderly and timely withdrawal of the License;

(b) Governance processes, management information monitoring, and other control processes to support timely withdrawal of License.

(c) Personnel management and exit arrangements;

(d) Procedures in place to identify material risks or obstacles to winding down in an orderly manner;

(e) Return or destruction of Customer Data held by the Licensee unless otherwise permitted under this Framework.

(f) Communications strategy, including the provision of clear and timely disclosures to all Customers;

(g) Procedures to place to ensure effective maintenance of records;

(h) Procedures in place to identify current and contingent liabilities and the plans in place to satisfy such liabilities.

9.2.2. The Licensee shall update the withdrawal plan periodically, in particular where there are any material changes in the business/operating models.

9.2.3. The Licensee must obtain written approval from the Central Bank prior to making any material changes to the withdrawal plan.

9.2.4. The Central Bank may refuse a request for the withdrawal of a License where:

(a) The Licensee has failed to settle its debts owed to the Customers, Central Bank, PSP Licensees, Financial Institutions, and any other parties relating to its business ; or

(b) It is in the interests of a current or pending investigation by the Central Bank, or by another regulatory body or authority.

9.2.5. Insolvency based withdrawal: In the event the Licensee is deemed or established to be bankrupt under the Royal Decree 53/2019, the Central Bank may permit for the withdrawal of the License in accordance with Article 9.1.

10. Penalties

10.1. Where the Central Bank deems a Licensee is non-compliant with any applicable laws, regulations, or instructions, then after following due process, the Central Bank may decide to carry out remedial action or impose penalties as applicable under the NPSL and the Banking Law.

***