BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1122
Series of 2021

Subject: Open Finance Framework

The Monetary Board, in its Resolution No. 730 dated 10 June 2021, approved the adoption of the Open Finance Framework, which shall be incorporated as Section 154 of the Manual of Regulations for Banks (MORB) and Sections 152-Q/149-S/146-P/130-N/129-T/123-CC of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Section 1. Section 154 of the MORB and Sections 152-Q/149-S/146-P/130-N/129-T/123-CC of the MORNBFI is hereby created, to read as follows:

"Section 154/152-Q/149-S/146-P/130-N/129-T/123-CC. GUIDELINES FOR THE ADOPTION OF OPEN FINANCE FRAMEWORK

Policy Statement. It is the thrust of the Bangko Sentral to promote an enabling environment that fosters innovation, encourages coopetition, and advances financial inclusion while safeguarding the integrity and stability of the financial system. In line with this, the Bangko Sentral is introducing the Open Finance Framework that aims to empower customers by giving them better control over their personal and financial data catalyzing the development of products and services that are responsive to their needs.

The Open Finance Framework espouses consent-driven data portability, interoperability, and collaborative partnerships among financial institutions and third-party providers (TPPs). Under the framework, financial institutions and TPPs can leverage on permissioned-access customer financial information to develop bespoke financial products and services for customers. The Open Finance Framework subscribes to the principle that "customers are the owners of personal and transaction data" hence, information shall only be shared with the consent of the customers.

Coverage. The Open Finance Framework covers technology, products, services, information, and policies that enable customers to securely share their financial data with qualified parties, either BSP-supervised financial institutions (BSFIs) or TPPs.

Definition of Terms. The terms used in this Section shall be defined as follows:

a. *Account Information Service Provider (AISP)* refers to an information technology service and/or software solution provider that processes data and provides an alternative access point to multiple sources of data other than payment transactions;

b. *Application Programming Interfaces (APIs)* refer to a set of rules and specifications for software programs to communicate with each other, forming an interface between different programs to facilitate interaction;

c. *Customer-permissioned data* refers to data held by Participants (e.g., customer transactions, personal identification data, and customer financial history) that are permissioned by the Participants' customer to be accessed by a third party (and possibly shared onwards with fourth parties if covered by the customer's consent);

d. *Open Finance* refers to leveraging on and sharing of customer-permissioned data among banks, other financial institutions, and TPPs to develop innovative financial solutions, such as among others, those that provide real-time payments, promote greater transparency to account holders, and provide marketing and cross-selling opportunities to banks, other financial institutions, and TPPs;

e. *Open Finance Standards* refer to the recommended standards in implementing the Open Finance Framework that takes into account various factors, including the financial industry's level of readiness to adopt such standards and the overall benefits arising from such standardization;

f. *Open API*, also known as external or public API, refers to a software technology interface that provides a means of accessing data based on a public standard;

g. *Open Data* refers to publicly obtainable data that is published by Participants, including, but not limited to financial products, service information, and other public information;

h. *Open Access* refers to allowing authorized third parties to access consented data without needing to establish a business relationship with the Open API publisher;

i. *Payment Initiation Service Provider (PISP)* refers to a registered operator of payment systems (OPS), as defined under Republic Act (R.A.) No. 11127 - The National Payments Systems Act and clarified in Part I, Section 101 of the Manual of Regulations for Payment Systems (MORPS), that carries out payment orders at the request of payment service users in connection with payment accounts held at other payment service providers;

j. *Third party providers* or TPPs refers to any external legal entity such as service providers, integrators, solutions vendors, and/or infrastructure support that interact with BSFIs to provide services to customers. They are classified as either AISP and/or PISP, however, other TPP classification may be created by the Open Finance Oversight Committee (OFOC), as deemed applicable;

k. *Participant* refers to the entities covered by the Open Finance Framework such as the BSFIs and TPPs;

l. *Open API publisher* refers to the Participant that keeps/is the custodian of customer data;

m. *Third party* refers to the Participant who has open access to customer-permissioned data residing in another Participant (publisher) through the Open API; and

n. *Fourth party* refers to an outsourcing partner or a service provider of a third party.

Governance Framework. The Bangko Sentral shall recognize an Open Finance Oversight Committee (OFOC), an industry-led self-governing body, that shall exercise governance over the activities and Participants of the Open Finance Ecosystem. The OFOC shall be subject to the regulation and supervision of the Bangko Sentral.

The Bangko Sentral shall facilitate the establishment of the OFOC in coordination with industry stakeholders. For this purpose, the initial set of members of the OFOC shall be comprised of representatives from each bank classification, non-bank financial institutions, electronic money issuers, operators of payment systems, TPPs, and other relevant sectors, as may be determined by the Bangko Sentral. The OFOC shall:

a. Adopt membership and participation rules that are non-discriminatory to ensure that key areas of interest of the financial industry are adequately represented and that all members and applicants for membership are treated fairly and consistently.

b. Define the functions, roles, and responsibilities of the Committee and the Participants. It shall adopt policies in monitoring Participants' compliance with the established policies and in handling non-compliance thereto including the corresponding sanctions or penalties for non-compliance.

c. Adopt standards, agreements, policies, and guidelines (Conventions) governing the Open Finance Framework which shall be consistent with relevant laws, rules and regulations and regional/global standards. At the minimum, these shall cover the following:

   (1) Registration/On-boarding of non-BSFI Participants;
   (2) API standards reference or other equivalent documentation;
   (3) Authorization, authentication, and encryption requirements for each product/service tier;
   (4) Disclosure and transparency requirements as prescribed under Section 1002 of the MORB and Sections 1002-Q/702-S/702-N/115-CC of the MORNBFI;
   (5) Consent management;
   (6) Protection of client information including responsible data handling as well as data privacy and protection;
   (7) Reciprocity arrangement among Participants;
   (8) Economic model; and
   (9) Consumer protection and effective recourse as prescribed under Part Ten of the MORB, Parts Ten of the Q-Regulations/Seven of the S-Regulations/Six of the P-Regulations/Seven of the N-Regulations, and Section 117-CC of the MORNBFI.

d. Cooperate with and extend fullest assistance permissible to the Bangko Sentral and other regulators in enforcing applicable laws and regulations, in promoting adherence to this Framework.

Consistent with the provisions of Section 002 of the MORB and Sections 002-Q/002-S/002-P/001-N/002-T/121-CC of MORNBFI, the Bangko Sentral reserves the right to deploy its range of supervisory tools to promote adherence to the requirements and expectation set forth in this Framework. In this regard, the Bangko Sentral may issue directives to or impose sanctions against the OFOC, such as suspension or revocation of any authority of the OFOC (including any or all of its generally authorized activities), without prior notice, to promote the safety and soundness of the financial system and/or to protect Participants, its customers, or the general public.

Registration Standards. BSFIs with a composite rating of at least "3" under the Supervisory Assessment Framework (SAFr), or its equivalent, are automatically eligible to become Participants of the Open Finance Ecosystem. On the other hand, those that do not meet the minimum rating must secure prior Bangko Sentral approval to participate in the Open Finance Ecosystem. Participants which are not under the regulation and supervision of the Bangko Sentral shall comply with the applicable registration requirements set by the OFOC, pursuant to pertinent laws, rules and regulations of the Bangko Sentral and other relevant authorities. Participants shall be responsible for ensuring fourth party compliance with applicable laws, rules and regulations.

Open Finance Standards. The OFOC shall issue guidelines aimed at ensuring that:

a. access to and participation in the standard-setting process, including any planning and consultation activities, is non-discriminatory;
b. the standards development process is transparent; and
c. the Open Finance Standards will be accessible to all qualified parties.

The API standards reference or other equivalent documentation that shall be developed by the OFOC shall meet the recommended technical standards to facilitate industry-wide adoption, and shall cover, at a minimum, the following:

(1) *API Architecture Standards.* These shall comprise, among others, reference for Open API specifications, including communication protocols, and architecture types. Participants are encouraged to adopt recognized industry-wide architectural styles such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP);

Data Standards. These shall include data formats, data structures, and related data protection and privacy rules to enable Participants to share data and information accurately and efficiently. Participants shall adopt data formats which are recognized by the industry such as, but not limited to, JavaScript Object Notation (JSON), Extensible Markup Language (XML), Comma Separated Values (CSV), and Structured Query Language (SQL). The "data dictionary" shall be published online, with sufficient level of detail to facilitate third party understanding and adoption;

(2) *Security Standards.* These shall cover minimum security compliance requirements, guidelines, and specifications that must be met by Participants, including authentication, authorization, and encryption. Participants should always refer to industry sound practices, relevant regulatory, and internal requirements, and apply holistic controls on

information and cybersecurity based on a risk- and principles-based approach to protect their systems as well as financial and consumer data. At a minimum, Participants shall adopt the latest and robust authorization and authentication protocols that are adequate for the risks presented by Open Access, such as, but not limited to, multi-factor authentication, Transport Layer Security (TLS)/Advanced Encryption Standard (AES)/Hashed Message Authentication Code (HMAC) encryption standards and OAuth 2.0 authentication standard. Participants should use more secure methods for sharing data, such as token-based authentication through APIs. The API must be designed in such a way that the end-user access shall be limited to data that the end-user has permission to see or process. These access rights must be appropriately recorded, verified, measured, and audited. In terms of secure hosting, PCI DSS and ISO 27001 are most desired; and

(3) *Outsourcing Standards.* These shall refer to the management of risks arising from outsourcing activities particularly those involving data disclosure and confidentiality, data privacy and protection, data management such as procedures for accessing and processing data, obtaining consent, contract management, security, performance monitoring and business continuity, among others.

Adoption of Open Finance Standards and Publication of Open APIs. All Participants that intend to provide Open Access shall adopt the Open Finance Standards and shall comply with relevant laws and pertinent Bangko Sentral regulations particularly on Outsourcing, Operational Risk Management, IT Risk Management, Internal Control, Anti-Money Laundering/Countering the Financing of Terrorism, Financial Consumer Protection, and sound corporate governance principles, among others.

Open Finance Standards may be revised periodically to address emerging issues or to improve the Open API functionalities. To facilitate third party adoption, Participants shall publish detailed Open API documentation and ensure consistency with the latest version of Open Finance Standards.

Tiered Approach towards Open Finance Standards Adoption. Open Finance Standards shall be classified into five (5) tiers based on data sensitivity, data type, and data holder type. The tiers are not necessarily sequential, and multiple implementations may occur simultaneously.

a. *Tier 1* - Product and Service Information. Refers to "read-only" information on financial data and other details of financial products/services that is readily accessible online and can be freely used, reused, and redistributed by any entity such as deposit/lending rates, credit card offerings, service charges and other public data.

b. *Tier 2* - Subscription and New Account Applications. Includes customer acquisition and account opening processes, along with facilitating digital application and submission of supporting documents. Applications for deposits, loans, debit/credit cards, and other financial products are covered under this category.

c. *Tier 3* - Account Information. Refers to personal (e.g., name, registered address, phone numbers, etc.) and financial information provided by a customer at any given time or other details pertaining to the account of authenticated customers for stand-alone or aggregated views. This consists of, but are not limited to, data types such as account balance, credit card outstanding balance, transaction records, credit limit change, and credit score.

d. *Tier 4* - Transactions. Covers payments and other financial transactions such as scheduled payments and transfers initiated by customers.

e. *Tier 5* - Others. Covers other more complex financial products or use cases and those that are not covered by tiers 1-4.

Cooperative Regulatory Oversight. The Bangko Sentral duly recognizes that other regulatory/supervisory authorities may be involved in the Open Finance Framework as this would involve other Participants that are not under the supervisory ambit of the Bangko Sentral. In this regard, the Bangko Sentral shall coordinate with the concerned regulatory authority with respect to the implementation of the Open Finance Framework.

Regulatory Sandbox

The Bangko Sentral seeks to provide a regulatory environment that is conducive for the deployment of innovative financial services, including the development of standards for Open Finance. In line with this, the Bangko Sentral will permit innovation in Open Finance, such as, but not limited to, the development of an industry API sandbox, in which Open APIs can be deployed and tested in a live environment and within specified parameters and timeframes.

Recommendation to Build a Central API Sandbox. While API providers will be encouraged to develop local sandboxes, it is recognized that costs may present a barrier and further incentives may be required. Thus, the Bangko Sentral encourages the OFOC to establish a central sandbox for testing developers and for other purposes related to local sandbox development (e.g., outsourcing sandbox development to trusted parties). The OFOC shall ensure that the central sandbox (i) implements all levels of security for APIs and (ii) contains a set of executable tests that API developers can use to validate compliance. The OFOC shall provide the executable tests to developers free of charge so that barriers to entry are avoided.

The OFOC shall maintain a list of approved Use Case API Services[1] with defined technical and security standards. This list shall include clear mechanisms and guidelines for providing the API services (e.g., basic APIs such as Authentication, Account Information, Transfers, etc.). The Use Case list per API service is a list that will be regularly updated based on new API innovations that have been reviewed by the Bangko Sentral or other relevant governing body.

Consumer Protection

Consumer Protection. Participants shall adopt customer awareness measures to, at the minimum, educate their customers on the following: (i) safeguarding of information; (ii) use of the Open API; (iii) actual fees and charges related to the access of information and performance of transactions; (iv) fair and equitable terms and conditions; (v) products and services appropriate to the capacity and risk appetite of the consumer; and (vi) problem resolution procedures. Participants shall disclose, prior to entering an initial transaction and on an ongoing basis, all material risks to their clients in a manner that is clear, fair and not misleading. Participants shall carry out initiatives to give consumers the knowledge, skills, and confidence to understand and evaluate the information they receive and empower them to make informed financial decisions.

Data Privacy and Data Protection. Each contract relating to the implementation or use of Open API shall contain a clause for the recognition by each party that the customers have ownership over their data being collected and processed through the transaction, and that they have all the rights enumerated under R.A. No. 10173 (Data Privacy Act of 2012). This views that while customer and transaction data are in the custody of the Open API publisher, their rights to control the use of such data

[1] All existing API arrangements prior to the issuance of this Circular shall comply with the applicable requirements prescribed herein within one (1) year from effectivity of this Circular. In cases awaiting policy-setting or further clarifications, compliance timetable shall be further determined by the OFOC.

is limited to the boundaries of the consent the customer provided. All Participants shall comply with relevant requirements of the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other National Privacy Commission issuances.

Dispute Mechanism. Participants shall have an adequate, prompt, and effective mechanism or procedure for handling and resolving disputes covering Open Finance issues aligned with agreed Conventions, as applicable.

User Consent and access to opt-in and opt-out mechanisms. Proper mechanisms shall be in place to ensure customers' private information is not used for purposes that are against their interests. The customers should, at all times, not only be educated and informed but they must also consent to how their data is being used and be provided with opt-in and opt-out mechanisms if and when they want to withdraw or modify the scope of their consent. Customers must be periodically informed as to how the Participants have utilized their permissioned data within a given period. Proper mechanisms based on industry standards shall be in place in providing a consent management portal/service that is interoperable, open, and has extensible information structure for recording obtained consents, consent duration, timestamp and opted-in/opted-out services, among others.

Section 2. Transitory Provision. The following transitory provision shall be incorporated as a footnote in Section 1:

All existing API arrangements prior to the issuance of this Circular shall comply with the applicable requirements prescribed herein within one (1) year from effectivity of this Circular. In cases awaiting policy-setting or further clarifications, compliance timetable shall be further determined by the OFOC.

Section 3. This Circular shall take effect fifteen (15) calendar days following its publication in the Official Gazette or any newspaper of general circulation.

FOR THE MONETARY BOARD:

BENJAMIN E. DIOKNO
Governor

17 June 2021