

EXPLANATORY NOTE

1. Since its adoption in advanced economies in 2018, open banking has begun to spark transformative changes in the digital finance marketplace by breaking down data silos and opening up access to data to a wider range of users. Middle- and low-income countries are now starting to explore the promise of open banking.¹ Open banking has further led to the launch of new products and services that extend to other services beyond bank accounts, revolutionizing the way consumers and businesses use financial services.
2. The Bangko Sentral ng Pilipinas (BSP) is cognizant of the benefits of moving towards inclusive fintech ecosystems that espouses consent-driven data portability, interoperability and collaborative partnerships among incumbent financial institutions and fintech players. The BSP also recognizes the transformative benefits that can be derived from “open finance”, which refers to the extension of permissioned data sharing and third-party access to a wider range of financial sectors and products.
3. The BSP conducted a survey with BSP-supervised financial institutions (BSFIs) in April to June 2020 and completed a comparative study of regulatory landscape in other jurisdictions to better understand how open banking / open finance has been implemented and identify what needs to be considered when developing a framework for an open finance regime. Respondents were generally supportive of the idea signaling the need for BSP to draft the circular with due consideration to feedbacks and learnings gathered.
4. The BSP has released for public consultation this first version of the draft Circular on Open Finance to help inform our regulatory strategy and collaborate with the industry players to support the development and improved access to new financial products towards fostering broad-based and inclusive economic development. Consultation shall be conducted without prejudice to the statutory powers and regulatory frameworks of the National Privacy Commission (NPC) and other financial regulatory agencies.
5. In seeking to establish an open finance ecosystem, the BSP hopes to involve industry players and engage them in an active dialogue to facilitate mutual learning and optimal determination of an industry-led self-governing body/authority, which is expected to promulgate membership and participation rules and formulate standards and procedures for the industry.
6. **Tiered Approach to Implementation.** The BSP foresees a tiered implementation by data sensitivity, data type, and data holder type. The tiers are not necessarily sequential, and multiple implementations may occur simultaneously. The first tier involves sharing of product and service information and other details of financial products/services that is readily accessible online and can be freely used, reused, and redistributed by any entity. The second tier involves sharing of subscription and new account applications

¹ Plaitakis, Ariadne, and Stefan Staschen. 2020. “Open Banking: How to Design for Financial Inclusion.” Working Paper. Washington, D.C.: CGAP.

information. The third tier involves sharing of account information or personal and financial information provided by a customer. The fourth tier covers transactions data, such as payments and other financial transactions data. The fifth tier covers those not covered by tiers 1-4 and other more complex financial products or use cases.

7. **Open Finance Governance Framework.** The BSP sees the value of placing the governance of the industry into a single body with explicit formalized self-governance structure where the industry standards and inter-participant business rules are housed. Under the draft Open Finance Circular, sound governance shall be performed by the Open Finance Oversight Committee (OFOC), an industry-led self-governing body that is duly recognized and overseen by the BSP. The OFOC shall promulgate its own membership and participation rules and formulate its own standards and procedures. It shall promote non-discriminatory membership by ensuring 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. The open finance participants shall recognize the authority of the OFOC as the governing body that is duly recognized by the BSP and shall subscribe to its prescribed conventions. OFOC will have direct responsibilities in its area of competency, to the extent appropriate to the size and complexity of the market and to assist BSP and other government agencies in meeting their respective regulatory objectives. OFOC and its members are expected to be involved in rule development discussions affecting their industry. OFOC shall adopt, update, and enforce its own procedural rules and rules of conduct.
8. The consultation period closes on 23 December 2020. Responses to this consultation will help inform/enhance the Open Finance Framework processes and guide the development process in setting up, recognizing, and capacitating the governing body.



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. _____
Series of 2020

Subject: Guidelines for Adoption of Open Finance Framework

The Monetary Board, in its Resolution No. ____ dated _____, approved the adoption of the Open Finance Framework, which shall be incorporated as Section ____ of the Manual of Regulations for Banks (MORB) and Section _____ of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Section 1. Section ____ of the MORB and its Subsections are hereby created to read as follows:

“Section ____ . GUIDELINES FOR ADOPTION OF OPEN FINANCE FRAMEWORK

SubSec. 1. Policy Statement. The Bangko Sentral recognizes the significance of an environment that encourages competition, financial inclusion and product innovation while safeguarding the integrity and stability of the financial system. This involves fostering the development of innovative financial solutions that aim for greater financial transparency options and consumer protection by empowering customers with better control over their personal and financial data and alternative access to financial services even beyond financial institution-owned channels. Thus, the BSP is cognizant of the benefits of moving towards an Open Finance ecosystem which espouses consent-driven data portability, interoperability and collaborative partnerships among incumbent financial institutions and third-party players. Through Open Finance, incumbent financial institutions and third parties can utilize permissioned-access to financial information needed to develop and offer innovative products/services that are responsive to customers’ needs. The underlying idea of Open Finance is that customers are the owner of personal and transaction data, thus, such information shall be shared if the customers wish to do so. Towards this end, the Bangko Sentral recognizes the potential complexities of business models and arrangements that will surface from the implementation of the Open Finance Framework. Accordingly, the applicability of the guidelines stated herein shall be guided by the principle of proportionality taking into account materiality factors such as, but not limited to, size complexity of operations, and risks posed by the relevant stakeholder to itself and the financial system.

Subsec. 2. Coverage. The Open Finance Framework covers technology, products and policies that enable customers to securely compare and use financial services from qualified third-party service providers. It applies to all BSP-supervised financial institutions (BSFIs) and third-party service providers, classified as either Account Information Service Providers and/or Payment Initiation Service Providers.

SubSec. 3. Definition of Terms. The terms as used in this Section, shall be defined, as follows:

- a. *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;
- b. *Customer-permissioned data* refer to data held by Participants (e.g., customer transactions, personal identification data, and customer financial history) that is 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);
- c. *Open Finance* refers to the sharing and leveraging of customer-permissioned data among banks, other financial institutions and third-parties to build innovative financial solutions, such as those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities;
- d. *Open Finance Standards* refer to the recommended standards in implementing the Open Finance that takes into consideration various factors, including the financial industry's level of readiness to adopt such standards and the overall benefits arising from such standardization;
- e. *Open API*, also known as external or public API, is a software technology interface that provides a means of accessing data based on a public standard;
- f. *Open Data* refers to publicly obtainable data that is published by Participants, including, but not limited to financial product, service information, and other public information;
- g. *Open Access* means allowing authorized third parties to access consented data without needing to establish a business relationship with the Open API publisher;
- h. *Account Information Service Provider (AISP)* is 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;
- i. *Payment Initiation Service Provider (PISP)* is a registered operator of payment systems (OPS), as defined under R.A. No. 11127 and clarified in BSP Circular No. 1049, 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* refers to any external legal entity who is not a part of the supervised financial institution. Third-parties can also be supervised financial institutions in instances when they access customer permissioned data residing in another participant;
- k. *Fourth party* is an outsourcing partner or a service provider of a third party;

- l. *Participant* is the collective term used to describe the entities covered by the Open Finance Framework such as the BSFIs and third-party service providers like the AISPs and PISPs;
- m. *Reverse engineering* is a process of analyzing the compiled application to extract information about its source code in order to determine which information is exchanged between an application and a server;
- n. *Screen scraping* refers to the use of automated scripts to collect displayed data elements from one application so that the collected data can be used by another application.

Subsec. 4. Governance Framework. Under the Open Finance Framework, sound governance shall be performed by an Open Finance Oversight Committee (OFOC), an industry-led self-governing body that is duly recognized and overseen by the BSP. The OFOC shall promulgate its own membership and participation rules and formulate its own standards and procedures (collectively “Conventions”). It shall promote non-discriminatory membership by ensuring 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. The Participants shall recognize the authority of the OFOC as the governing body that is duly recognized by the BSP and shall subscribe to its prescribed Conventions.

The OFOC shall adopt agreements, policies, and guidelines governing Open Finance Framework which shall be consistent with relevant laws, rules and regulations and subject to concurrence by the BSP. At the minimum, these shall cover the following:

- a. OFOC functions, limitations, and member qualifications;
- b. Participants’ roles and responsibilities;
- c. Development of API standards reference or other equivalent documentation;
- d. Authorization, authentication and encryption requirements for each product/service tier;
- e. Standard forms to operationalize consent acquisition including waiver of bank secrecy on deposits;
- f. Consent management;
- g. Registration guidelines for AISPs;
- h. Guidelines on tie-up partnership and outsourcing of AISPs;
- i. Mechanism for monitoring Participants’ continuing compliance;
- j. Responsible use of data;
- k. Reciprocity arrangement among participants;
- l. Economic model;
- m. Liabilities, problem and complaints management (e.g., procedures for handling and resolving disputes); and
- n. Data privacy and data protection.

Subsec. 5. Registration Standards. Existing BSFIs are automatically eligible to become participants of the Open Finance Framework. Conversely, applicant AISPs which are not yet

covered by existing BSP licensing and registration frameworks but intending to participate in Open Finance activity shall obtain applicable registration from the Open Finance Oversight Committee, pursuant to and upon compliance with the registration requirements of relevant regulatory authority. Further, in any circumstance as determined by the Monetary Board, the BSP may impose that such entities obtain a clearance from the BSP before becoming participants. Both existing BSFIs and registered AISPs shall also be responsible for ensuring compliance by fourth parties with applicable BSP regulations.

Subsec. 6. Open Finance Standards. Participants should adhere to the standards in implementing the Open Finance Framework, which will form part of an API standards reference or other equivalent documentation and will be developed separately by the OFOC in line with the recommended technical standards, to facilitate industry-wide adoption. At a minimum, these shall cover the following:

- a. *API Architecture Standards* shall comprise, among others, reference for Open API specifications, including communication protocols, and architecture types. Participants are encouraged to adopt the recognized industry-wide architectural styles such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP);
- b. *Data Standards* shall include data formats, data structures, and related data protection and privacy rules that provide a reference point to enable parties to share data and information in a way that ensures understanding is preserved and the meaning can be conveyed. While OFOC may adopt other data specifications, it is encouraged to adopt data formats which are recognized by the industry such as JavaScript Object Notation (JSON), Extensible Markup Language (XML), Comma Separated Values (CSV) and Structured Query Language (SQL). In addition, such definition (often called “data dictionary”) should be published online, with sufficient level of detail to facilitate third-party understanding and adoption;
- c. *Security Standards* shall cover minimum security compliance requirements that must be met by participants, including authentication, authorization, and encryption. Participants should always make reference to sound industry practices, relevant regulatory and internal requirements, and apply holistic controls on information and cybersecurity based on a risk- and principle-based approach to protect their systems as well as financial and consumer data. At the minimum, Participants shall adopt the latest and robust authorization and authentication protocols that are adequate for the risks presented by Open Access, such as two-factor authentication, TLS/AES/HMAC encryption standards and OAuth 2.0 authentication standard. Participants are required to use more secure methods for sharing data, such as tokenized authentication through APIs, as opposed to screen scraping or reverse engineering. The API must be designed in such a way that is able to restrict access whereby end-users may only access data that they are permissioned 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;

- d. *Outsourcing Standards* shall manage risks arising from outsourcing particularly those involving data disclosure and confidentiality, data privacy and protection, data management such as procedures for accessing and processing data, contract management, security, performance monitoring and business continuity, among other things. Participants should adhere to the pertinent BSP regulations on Outsourcing and IT Outsourcing/Vendor Management Program.

Subsec. 7. Adoption of Open Finance Standards and Publication of Open APIs. All Participants that intend to provide Open Access should adopt the Open Finance Standards and shall comply with pertinent BSP regulations on Outsourcing, Operational Risk Management, IT Risk Management, Internal Control, Anti-Money Laundering, Financial Consumer Protection, and sound corporate governance principles, among others.

To facilitate third-party adoption, participants should publish detailed API documentation online to accompany the published Open APIs. Open Finance Standards may be revised periodically to address emerging issues or to enrich the Open API functionalities. Participants should also ensure that the published Open APIs are consistent with the latest version of Open Finance Standards, within a specific period to be determined by OFOC.

Subsec. 8. Tiered Approach towards Open Finance Standards Adoption. 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 and financial information provided by a customer at any given time or other details pertaining to the account (balance, transaction history, limits, payment schedules, etc.) of authenticated customers for stand-alone or aggregated views. This consists 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 transfer initiated by customers.
- e. *Tier 5 – Others.* Refers to other data and processes not covered by tiers 1-4.

Subsec. 9. Other Provisions

Consumer Protection. Participants shall adopt customer awareness measures to, at the minimum, educate its 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; and (iv) problem resolution procedures. Participants shall disclose, prior to entering into an initial transaction and on an ongoing basis, all material risks to their clients in a manner that is clear, fair and not misleading.

Data Privacy and Data Protection. Each contract relating to the implementation or use of Open API will 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 Philippine data privacy laws, otherwise known as Republic Act 10173 – Data Privacy Act of 2012. This views that while customer and transaction data are in the custody of the BSFIs and third parties, their rights to control the use of such data is limited to the boundaries of the consent the customer provided.

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

User Consent and access to opt-in and opt-out mechanisms. Proper mechanisms should 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 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 actually utilized their permissioned data within a given period.

Subsec. 10. Regulatory Sandbox. The BSP seeks to provide a regulatory environment that is conducive for the deployment of innovative financial services, including developing standards for Open Finance. This includes adopting new and reviewing existing regulatory requirements or procedures that may unintentionally inhibit innovation or render them non-viable.

As part of this process, the BSP will permit innovation in Open APIs to be deployed and tested in a live environment, within specified parameters and timeframes. Corresponding guidelines on Open APIs that have been tested and can be implemented shall be issued by the OFOC and approved by the BSP for guidance of all participants.

The guidelines shall ensure that:

- access to and participation in standard-setting, including any planning and consultation process, is non-discriminatory;
- the procedure for adopting the standard is transparent; and
- the Open Finance Standard will be accessible by all qualified parties.

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 BSP encourages the designated 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 central sandbox shall ensure that:

- it implements all levels of security for APIs;
- it contains a set of executable tests that API developers can use to validate compliance; and
- it will be provided free of cost to developers so barriers to entry are avoided.

The OFOC shall maintain a list of approved Use Case API Services with defined technical and security standards. This list will include clear mechanisms and guidelines for providing these 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 constantly updated based on new API innovations from the industry that have been accordingly reviewed by the BSP or other relevant governing body.

Subsec. 11. Transitory provisions. All existing Open API arrangements prior to the issuance of this Circular shall comply with the applicable requirements prescribed herein within one (1) year from the date on which this Circular came into force.

The BSP reserves the right to suspend, modify, downgrade, limit or revoke any authority of the OFOC (including any or all of those generally authorized activities) for prudential reasons and for purposes of meeting the objectives of this circular.

Subsec. 12. Effectivity. 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