HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C
B9/67C

29 October 2019

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Consumer Protection Measures of Authorized Institutions in respect of Open Application Programming Interface Framework

I am writing to clarify the expectations of the Hong Kong Monetary Authority ("HKMA") on Authorized Institutions ("AIs") on consumer protection in respect of Open Application Programming Interface ("Open API") Framework.

Consumer Protection Measures

As set out in the HKMA publication dated 18 July 2018 on "Open API Framework for the Hong Kong Banking Sector", the adoption of technology by AIs, including Open API, could bring benefits and efficiency gains to the banking industry and its customers through the development and delivery of innovative and integrated banking services that improve customer experience. To achieve this policy objective, it is important for AIs to implement consumer protection measures when implementing the Open API Framework. This will not only protect the interests of the customers, but also enhance customer confidence in using the relevant banking services and promote the healthy development of innovative technology in the banking industry.

The HKMA would like to remind AIs that they are expected to uphold consumer protection principles set out in the Code of Banking Practice and comply with other applicable regulatory requirements, regardless of the underlying technology adopted for their banking products and services, and whether AIs provide the products and services themselves or in partnership with third-party service providers ("TSPs").

During the implementation of Open API, as the TSPs may interface with customers for providing the services under the Open API Framework, there are several consumer protection aspects (e.g. fair treatment of customers, disclosure and transparency, protection of customers against fraud, protection of customer data, complaint handling and redress mechanism, liability and settlement arrangement, potential risk of mis-representation of AIs by the TSPs, etc.). AIs should devise and adopt adequate consumer protection measures that are in line with the aforementioned existing expectation (i.e. to uphold consumer protection principles set out in the Code of Banking Practice and comply with other applicable regulatory requirements for their banking products and services). Some elements of the TSP governance process, including effective risk management and controls as well as consumer protection measures, have already been set out in the abovementioned HKMA publication dated 18 July 2018 on "Open API Framework for the Hong Kong Banking Sector". Some sound consumer protection practices for Open API Phase II and beyond are listed in the **Annex** for easy reference.

In order to strike a balance between innovation and consumer protection, AIs should adopt a risk-based approach, and implement consumer protection measures that are commensurate with the risks involved. For instance, for TSPs that would only redirect customers to the user interfaces (e.g. websites, mobile apps, etc.) of AIs without handling bank customer data ("Simple Redirection Model"), the level of due diligence in the on-boarding checks and on-going monitoring of the TSPs can be lower, compared with those Open API collaborations which involve bank customer data.

Use of Intermediaries

The HKMA would also like to take the opportunity to clarify the requirements about AIs' engagement of intermediaries, as the use of TSPs under Open API Framework (e.g. where customers' information are collected by the TSPs and then passed to AIs in respect of retail consumer financial products or services, such as personal loans, tax loans and credit cards) may constitute the use of intermediaries by AIs. For the avoidance of doubt, Simple Redirection Model is not considered as use of intermediaries by AIs.

According to the HKMA's circular of 7 August 2015 on "Engagement of Intermediaries and Sales Agents by Authorized Institutions" ("2015 Circular"), AIs should cease the use of intermediaries for the purpose of sourcing retail consumer financial products or services, such as personal loans, tax loans and credit cards. The policy intention is to protect the interests of bank customers and reduce the potential risks to the reputation of the banking industry arising from possible malpractices by fraudulent lending intermediaries.

Given that AIs and TSPs providing the collaborated services under Open API Phase II and beyond operate under a partnership arrangement and there will be a formal TSP governance process under the Open API Framework to ensure there will be effective risk management and controls as well as consumer protection measures, such collaboration is different from the other lending intermediaries the use of which has been ceased by virtue of the 2015 Circular. In other words, AIs are allowed to engage TSPs to provide collaborated services, including retail consumer financial products or services such as personal loans, tax loans and credit cards, under Open API Framework as lending intermediaries. For the avoidance of doubt, in respect of such engagement, AIs should still comply with the applicable requirements related to engagement of intermediaries issued by the HKMA, including, among others, those set out in Annex 1 to the HKMA's circular issued on 30 November 2016 on "Engagement of Intermediaries by Authorized Institutions (AIs)". For instance, it is generally expected that such TSPs should not charge loan-related fees on prospective borrowers.

Should you have any questions regarding this circular, please feel free to contact Ms Stella Ma on 2878-8601 or Ms Teresa Chu on 2878-1563.

Yours faithfully,

Alan Au
Executive Director (Banking Conduct)

Encl.

Annex

Sound Consumer Protection Practices by AIs for Open API Phase II and Beyond

AIs should adopt sound consumer protection practices, including, among others:

1. **Conduct proper on-boarding checks and on-going monitoring on the TSPs** as well as the **collaborated products and services**, having regard to the expectation that AIs should uphold consumer protection principles set out in the Code of Banking Practice for providing banking services to customers, and commensurate with the risks involved.

   The assessments involved in the on-boarding checks and the ongoing monitoring should include risk-based reviews of the TSPs and the collaborated services as to whether the consumer protection measures have been properly implemented in practice (in addition to reviewing the policies, procedures and/or undertakings by the TSPs), and be conducted by an appropriate assessor which could be an external party or the AIs' internal department (i.e. second or third line of defence) that is independent of the design and implementation of the relevant controls and measures;

2. **Publish a list of partnering TSPs** (to help the public distinguish which TSPs are partnering with the AI and which are not) and the **corresponding specific products and services** provided in partnership with the respective TSPs (to help the public distinguish which particular products and services are offered in partnership with a particular TSP and which are not), as well as **provide timely updates to such list and the relevant central register**;

3. **Carry out monitoring regularly** as far as practicable to see if there are third party websites, apps or similar scams purporting to be operated by the AI's partnering TSPs[1] or claiming to be partnering with the AI when they are not; and **notify promptly customers and the public** through issuing press release (or similarly effective means) whenever the AI becomes aware of the irregularities;

[1] Alternatively, AI may also adopt an arrangement where its partnering TSP performs the regular monitoring and notification to the public and customers for scams purporting to be operated by the partnering TSP as far as reasonably practicable. If an AI adopts such an arrangement, the AI should include in its on-boarding checks and on-going monitoring the reviews of whether the TSP has put in place proper procedures and measures to implement the arrangement, and whether the arrangement has been properly implemented in practice.

4. **Enhance education** to help customers, among others:

   (a) better manage any potential risks, and understand the respective responsibilities of the AI and the TSPs;

   (b) know the possible ways of differentiating between the TSPs which are partners of the AI and those which are not, and which particular products and services are offered in partnership with a particular TSP and which are not (e.g. educating the customers to refer to the AI's list of partnering TSPs and their relevant partnering products and services); and

   (c) be vigilant to bogus calls or other similar scams (e.g. alerting them of the scams and educating the customers to first authenticate the identity of the callers or senders who purport to be the AI's representatives, using the relevant AI's hotlines for this purpose which could be found at the AI's official website or the HKMA's website), etc.

5. **Establish clear liability and settlement arrangement** with the partnering TSPs for compensating customers' loss arising from unauthorised transactions, with clear communication to customers upfront; and **adhere to the principle that a bank customer should not be responsible for any direct loss** suffered by him/her as a result of unauthorised transactions conducted through his/her account attributable to the services offered by the TSPs using AIs' Open API **unless the customer acts fraudulently or with gross negligence**;

6. **Put in place proper complaint handling and redress mechanism**, including providing customers with reasonable channels to make complaints, submit claims and seek redress that are accessible, fair, accountable, timely and efficient; and

7. **Put in place policies and procedures** to ensure that the collaborated services comply with the relevant consumer protection requirements and other conduct-related requirements issued by the HKMA from time to time.