Hong Kong's open era begins: your Open API Survival Guide

July 2018

Hogan Lovells

Hong Kong's open era begins: your Open API Survival Guide

On 18 July, 2018, the Hong Kong Monetary Authority (the "**HKMA**") published its Open Application Programming Interface ("**API**") Framework for the Hong Kong retail banking sector (the "**Open API Framework**"). The much-anticipated Open API Framework is one of the key planks in the HKMA's "New Era of Smart Banking" initiative launched in September 2017.

Why Open API?

The HKMA's vision for the Open API Framework is a more competitive, innovative and technologically advanced retail banking environment for Hong Kong, to be achieved through financial institutions opening up their data through new digital interfaces, including those intermediated by fintechs and other third party service providers ("**TSPs**") who are not licensed under the banking regulatory regime. The increased flow of bank product and customer data is expected to encourage greater flexibility for consumers to make informed choices amongst competing products and ultimately encourage innovation in the design and delivery of financial services in Hong Kong.

The Open API Framework is a bold move for the retail banking environment in Hong Kong. There are synergies and important touch points with the reboot of the HKMA's virtual banking licensing regime, the expected launch of the faster payments system in the autumn of this year and the introduction of the stored value facility ("**SVF**") licensing regime in 2016, which introduced a separate authorization regime for non-bank payment accounts to Hong Kong.

How to comply?

The Open API Framework does not actually represent regulatory change for financial institutions – it calls for the application of existing regulations to new data-driven business models. A number of leading financial institutions in Hong Kong have already opened APIs to TSPs, and the introduction of licensed SVFs to the Hong Kong ecosystem precipitated a flurry of similar commercial collaboration and data exchanges through digital wallets in recent years. The Open API Framework formalizes regulatory expectations around changes to banking business that are already well underway.

The core compliance requirements for financial institutions triggered by the Open API Framework are largely prescribed by the HKMA's current risk management framework under the Banking Ordinance (the "**BO**"), the Code of Banking Practice (the "**HKAB Code**"), the Personal Data (Privacy) Ordinance (the "**PDPO**") and existing anti-money laundering and counter-terrorist finance ("**AML-CTF**") regulations: all which apply with increased importance to retail banking business in the data-driven "open environment".

Critically for financial institutions, the Open API Framework leaves it entirely to individual banks to judge the risk of engaging TSPs in specific circumstances. Financial institutions are the compliance gatekeepers.

Our "Open API Survival Guide" set out below is intended to help financial institutions and fintechs alike navigate Hong Kong's open environment.

Key features of the Open API Framework

As anticipated in our briefing on the framework consultation, the HKMA has come out in favour of a phased introduction of the Open API Framework and has chosen not to impose a mandatory requirement for institutions to make data available to TSPs.

In a fundamental divergence from the example set by the UK Competition and Market Authority's "Open Banking" initiative, the Open API Framework is not a "forced opening" of bank data, and it does bring about a fully regulated ecosystem in which TSPs are also subject to licensing. Hong Kong financial institutions releasing data through API will remain fully responsible for this data. TSPs will not be vetted or licensed by the HKMA. This role is allocated to the institutions.

Of course TSPs misusing personal data obtained through APIs may be held to account under the PDPO, and it continues to be the case that TSPs cannot carry on regulated business in Hong Kong without a licence. However, it is equally clear that Hong Kong's licensed banks will be the gatekeepers responsible for judging that TSPs are suitable for handling their customer data, and for ensuring that contracting arrangements with TSPs are effective in "flowing down" banking regulatory requirements in key areas such as technology risk management ("**TRM**"), the handing of customer payment instructions and AML-CTF. Banks are required to ensure TSPs operate as if they were part of the bank.

Phased approach to Open API

The Open API Framework retains the phased approach to implementation outlined in the HKMA's consultation papers:

Phase	Category of API	Description and Examples	Timeframe for Implementation of APIs
1	Product and Service Information	– "Read only" bank product information – API are opened, for example, to aggregators and comparison sites and other TSPs providing consumers with tools to compare and evaluate products – TSPs in this space may currently be "scraping" product information from bank sites: open API promises more accurate, real time product information providing consumers with more granular and effective "like for like" product comparisons	6 months
2	Subscriptions and New Applications	– Customer acquisition interfaces allowing for online submission of loan and credit card applications through TSP platforms – These APIs support a wide range of TSPs who may wish to support consumer credit options: e-	12 – 15 months

Phase	Category of API	Description and Examples	Timeframe for Implementation of APIs
		commerce platforms, payment gateways and TSPs offering better or more integrated UX	
3	Account Information	– Retrieval and alteration of account balances, transaction histories, payment limits and schedules – API to support stand-alone and aggregated views of account information – TSPs include a wide range of non-transactional applications, including accounting and personal finance application providers, multi-banking interfaces and proof of income providers	HKMA to fix in next 12 months
4	Transactions	– TSPs communicate customers' payment instructions to the bank, allowing customers to pay directly from their bank accounts through the TSP's digital interface – TSPs would include payment gateways integrated with e-commerce platforms or merchant point of sale systems	HKMA to fix in next 12 months

The phasing above reflects increasing risk for API implementation at each stage.

The release of static product information to TSPs in Phase 1 obviously entails much lower risk than an institution's reliance on a customer's payment instruction intermediated by a TSP, as envisaged in Phase 4. Recognizing the increasing complexity and risk, the HKMA has indicated that it will closely monitor the progress of the implementation of the Open API Framework and take into consideration local and international developments in coming to a decision on the Phase 3 and 4 implementation dates in the coming 12 months.

No API standardization

Another key issue discussed as part of the Open API consultation is the matter of standards. Imposing standard API datasets and universal technical standards could mean greater interoperability between institutions, and could also set a clearer course for TSPs and others taking risk investing in infrastructure that functions in the open environment.

As foreshadowed in the consultation papers, however, the HKMA has concluded that it would be cumbersome to reach agreement in these areas in advance. The HKMA has recommended certain APIs that should be opened in each phase (as outlined in Annex A to the framework). Each institution is responsible for providing the HKMA with a road map of the APIs it proposes to open, including justification for any gaps against the recommendations. Annex C to the framework supplements the approach with illustrative examples of product and service information data fields which institutions may wish to include in their APIs.

In the same vein, Annex B of the framework sets out the HKMA's recommendations for architecture, security and data standards.

No regulatory vetting of TSPs

As noted above, the Open API Framework places institutions in charge of regulating the TSPs they interact with in the open environment.

The Open API Framework requires banks to establish a formal TSP governance process for managing risk. In relation to Phase 1 Product and Service Information APIs, banks are required to establish a simple TSP registration process that allows the institution to keep track of its dataflows primarily for general consumer protection purposes, but also to support capacity planning for the volumes of bank data being drawn through the APIs. The HKMA also expects banks to have terms and conditions in place with TSPs that address a number of risks arising in Phase 1: (i) the TSP uses the API information to misrepresent the bank's products; (ii) the TSP separately collects personal data from bank customers in a manner that breaches the PDPO; and (iii) the TSP does not fully disclose the risks involved in their own products. Even in Phase 1, then, there are important risks for banks to manage.

In relation to Phase 2 Subscriptions and New Application APIs (and beyond into Phases 3 and 4), the HKMA expects that institutions will mobilize (through the Hong Kong Association of Banks ("**HKAB**") or otherwise) to develop a common baseline set of criteria for TSP governance, with the objective of streamlining banks' engagement with TSPs.

The Open API Framework sets out a number of areas for due diligence into TSPs for Phases 2 through 4, including financial soundness and various operational risk areas, with examples being data protection, cybersecurity and business continuity.

The HKMA is clearly motivated to ensure that TSP assessments do not become a bottleneck for the Open API Framework. The HKMA is encouraging a common approach, potentially with banks recognizing each others' assessments so as to avoid duplication or even structuring TSP assessments through a centralized assessor working to the banks' common principles of assessment.

As with the Phase 1 APIs, there is significant focus by the HKMA on banks' approach to contracting with TSPs as part of Phase 2 and beyond (see "**The Open API Survival Guide**" below for more details).

Further, the HKMA expects each institution to publish a list of partnering TSPs and their relevant products, with the regulator encouraging the industry to centralize this aspect of the open environment in a public registry. The HKMA has also cautioned banks that they must now be vigilant in this new open environment, keeping watch for those who may trade on the guise of being API collaborators, when in fact they are not.

Finally, the HKMA has suggested that API facilitation should take place through a centralized repository or "dashboard" of APIs, recommending that the Data Studio of the Hong Kong Science and Technology Parks be used for this purpose.

Open API Survival Guide

The Open API Framework is ultimately about data-driven collaboration between banks and fintechs.

The key hurdle is in meeting the banks' risk management and customer data regulations, with primary considerations being the onboarding of TSPs and settling contract terms that are flexible but sufficiently protective of each side and the consumers that they serve.

TSP Due Diligence

The HKMA has recommended that banks seek a common set of standards for vetting TSPs in respect of Phases 2 through 4, perhaps even establishing a centralized assessment body that would certify TSP suitability for API collaboration on an industry-wide basis. This is clearly a worthy objective as it will ease the path to opening APIs and help ensure a critical mass of attractive TSP offerings. Certification would not eliminate the need for banks to evaluate the specific risk factors raised by a particular collaboration model, but it would streamline matters to certify a TSP against basic eligibility criteria.

The HKMA's list of considerations for TSP vetting is, however, rather long. The list is consistent with (but in some respects goes beyond) the considerations for selecting an outsourced service provider found in the HKMA's "Outsourcing" Supervisory Policy Module SA-2 ("**SA-2**").
The HKMA's vetting criteria for TSPs takes the SA-2 criteria and supplements these with additional TRM and data protection topics. The focus on TRM and data protection is appropriate to the context, but it can be foreseen that the basic eligibility criteria for TSPs could in themselves become a bottleneck to TSP onboarding. A risk-based scaling of criteria would be appropriate. Not all API collaborations will be in the nature of an "outsourcing" where the TSP is literally carrying on regulated banking business on behalf of the bank. It is clear that TSPs bringing payment instructions to banks as part of the Phase 4 Open APIs need to be very carefully vetted against a wide range of risk factors. However, there may well be implementations of Phase 2 APIs, in particular, that do not involve the same degree of intermediation between bank and consumer and so do not raise all of the same risk factors. The onboarding criteria should naturally be fewer in number and set at a lower baseline in lower risk categories of API collaboration.

Taking another example where risk profiles may vary significantly, customer data varies in its sensitivity, with, for example, customer email contact details generally being less sensitive than detailed listings of transaction data. A proportionate, risk-based approach to TSP vetting is consistent with the requirements of Data Protection Principle 4 of the PDPO and would ensure that the right risk factors are looked at in the context of the specific collaboration model.

Contracting with TSPs

In many cases, the open environment will call for new contract forms that reflect new types of collaboration. The topics that these contracts should address will depend on the specific form of collaboration, but we have set out a number of issues below that we believe both sides of the collaboration will likely need to address in order to satisfy the bank's regulatory requirements and at the same time introduce a flexible collaboration model with a sensible allocation of risk each way.

Getting the basics right: As with any contract, being clear on "which party does what" is key. From a banking regulatory perspective, the boundary between regulated banking business and unregulated activity is fundamental. API collaborations can blur this boundary and so care is needed to ensure that the bank is exercising the control it needs to exercise in order to ensure the collaboration is compliant.

A practical oversight model: The project governance applied to Open API collaborations will appear, from a tech perspective, to be more intensive and rigorous than data-driven collaborations in other sectors. From the bank's perspective, the seemingly heavy-handed approach is necessary in order to ensure that the bank can meet regulatory requirements to ensure that it remains fully on top of how its customers are being treated, how the integrity of its systems is being maintained, and how customer data is being handled. That said, the bank's standard material outsourcing agreement will certainly not be the right solution in every case, and in many cases it won't get signed. Finding practical accommodations that reflect a proportionate, risk-based approach to project governance will be the key.

Data protected: The success of Open API will depend on there being adequate consumer confidence in the handling of customer data outside of the four walls of the bank. Contracts between banks and TSPs must have clear direction as to the specific customer data being licensed and released through the APIs, for what purposes this data will be processed and how it will be kept secure. Data processing clauses have moved on in Hong Kong in recent years, with increasing technical rigor and an eye to facilitating a rapid response should there be a cyber incident. The focus here is not entirely down to the data management practices of the bank and the TSP: many of the cyber points of failure rest in the hands of the consumer using their smartphone to take advantage of an innovative service delivery model. The arrangements need to turn an eye to how consumers will be in a position to do their part to manage risk.

Change is here to stay: Contracts governing novel forms of commercial collaboration must be crafted to reflect the fact that there will be business change and regulatory change to come. A carefully calibrated risk-based assessment can come unstuck if the underlying risk of the collaboration changes. A good collaboration agreement is flexible (where it can be) and sets out clear parameters for managing change.

The Commercials: Many of the considerations for drafting effective contracts in the open environment relate to regulatory considerations. However, as with any other business collaboration, the opening of APIs represents significant commercial value and risk for the parties concerned and so the contract must be reflective of these considerations. Key topics include:

- fees, royalties and other financial remuneration reflecting the investment and risk on each side;
- clear provisions governing each party's performance standards (and the consequences of not meeting those, in terms of impact on remuneration, termination rights and otherwise);
- clear limitations and exclusions of liability that fairly allocate the risks of collaboration;
- ownership and licensing of intellectual property rights, including those brought to the table as "background IP" and those developed or co-developed as part of the collaboration; and
- planning for the exit, ensuring that there is an orderly wind-down upon expiry or termination of the collaboration, ensuring that business is not disrupted and customer data is securely managed.

Contacts

Mark Parsons

Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Tommy Liu

Senior Associate, Hong Kong
T +852 2840 5072
tommy.liu@hoganlovells.com

George Willis

Registered Foreign Lawyer, Hong Kong
T +852 2840 5915
george.willis@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com