HONG KONG MONETARY AUTHORITY
香港金融管理局

accenture

The Next Phase of the Banking Open API Journey

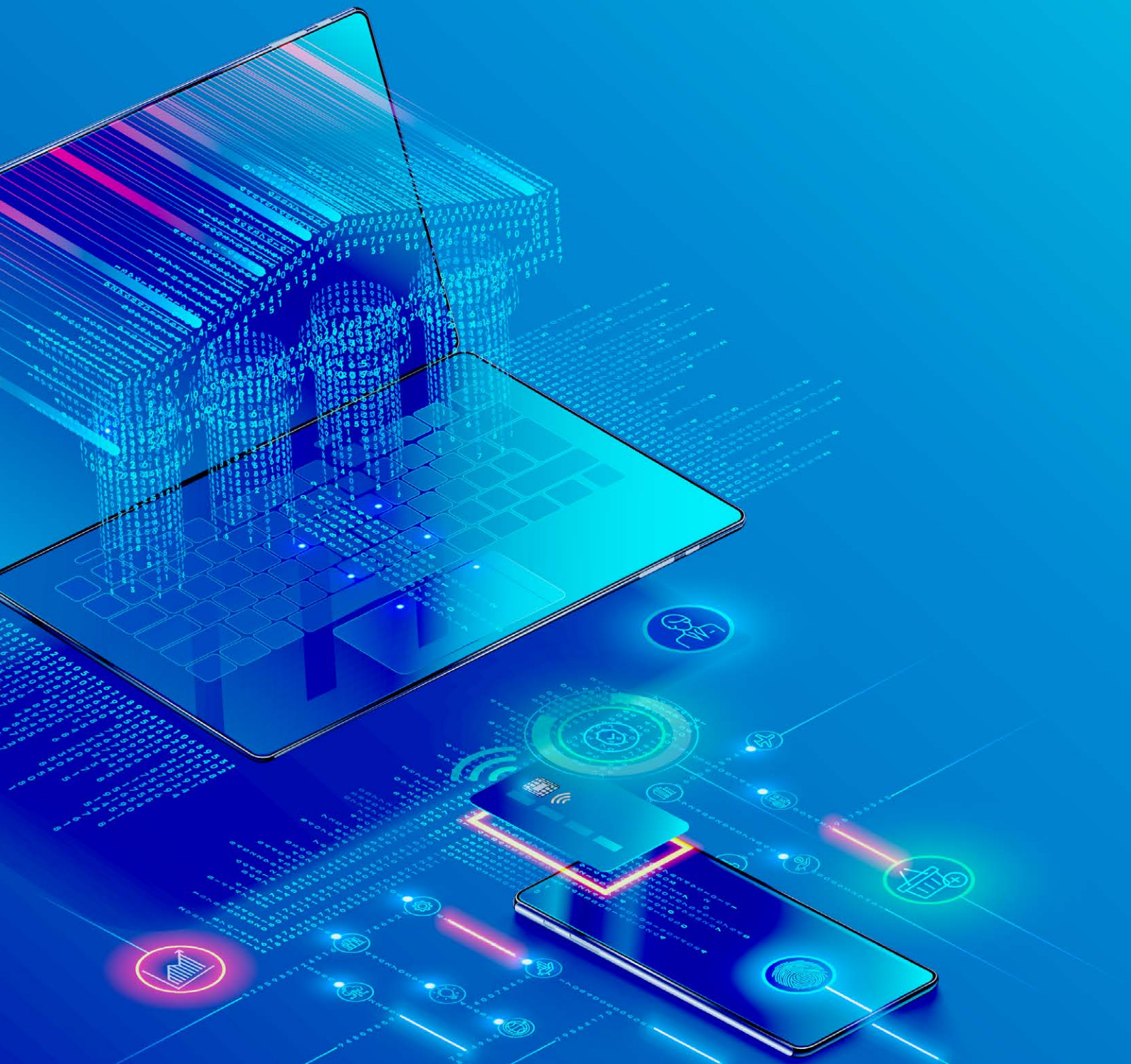


Table of Contents

Foreword

In recent years, there has been significant change in the competitive landscape of banking in Hong Kong brought about by the rapid adoption of digital technologies.

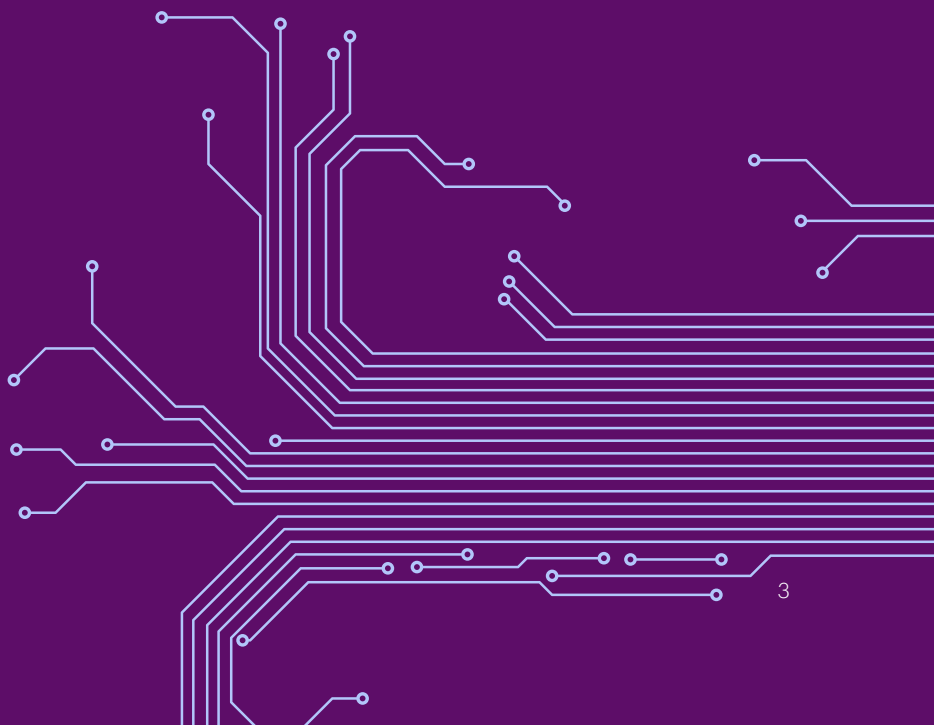
The widespread move to digitalisation has been further accelerated in the context of the current COVID-19 crisis, with financial players moving swiftly to provide more online services and reinvent their product offerings over the past year. Open Application Programming Interface (API) technology has opened up opportunities for banks in Hong Kong to co-create innovative digital products with non-financial companies, as well as to attract and engage customers through new digital channels.

Following the introduction of the Hong Kong Monetary Authority (HKMA) Open API Framework in July 2018, and the subsequent implementation of Phases I and II of banking Open API in January and October 2019 respectively, the HKMA has seen encouraging progress being made towards the adoption of banking Open APIs in Hong Kong. To date, more than 20 participating banks have launched over 800 Open APIs covering a diverse range of banking products and services. Customer receptiveness for banking Open APIs has also risen sharply, with the number of API calls in Q3 2020 exceeding the recorded number of calls for Q4 2019 almost 70-fold.

As we prepare to implement the next phases of the banking Open API journey, we recognise the importance of ensuring robust cybersecurity and proper risk management and fully addressing the customer protection and data privacy challenges brought about by their implementation. We hope that this study will provide useful insights into the current and evolving banking Open API landscape in Hong Kong, and will encourage banks to apply our recommendations as practical steps in facilitating the next phases of implementation.

This report would not have been possible without the great support of the banks and institutions that participated in our research. The HKMA greatly appreciates their contribution and extends our gratitude to them.

Howard Lee
Deputy Chief Executive
Hong Kong Monetary Authority



01

Executive Summary

Fast-moving digital and technological development is compelling banks worldwide to rethink how they operate and how they serve their customers. Open Banking, which promotes the secure sharing of customer financial data with third-party service providers (TSPs) through Open APIs, has emerged as a key technology enabler that is allowing banks to deliver improved banking services in collaboration with third parties.

Since their introduction in the European Union and the United Kingdom, Open Banking initiatives have expanded globally into jurisdictions such as Australia, Switzerland and Singapore. In Hong Kong, the launch of the HKMA banking Open API Framework, along with connected initiatives such as virtual banks and the Faster Payment System, are similarly paving the way for a new smart banking playing field where Open APIs are at the forefront.

The HKMA plans to move towards Phases III and IV of the Open API Framework, fostering an innovative digital development environment that prioritises information security and customer interests. To this end, the HKMA commissioned Accenture to carry out a study to analyse and recommend ways forward for the implementation of Phases III and IV, taking into consideration international practices and the local market situation. This study has been organised as follows:

- Research into and review of international developments in banking Open APIs, with the aim of formulating the most appropriate strategy for the next phases of the implementation of banking Open APIs in Hong Kong.
- Exploration of the current status of banking Open API implementation in Hong Kong, and examination of any barriers to adoption.
- Identification of common practices for the next phases of banking Open API implementation in Hong Kong, based on international practices and taking the local situation into consideration.
- Analysis of and recommendations for ways to proceed in the next steps of Hong Kong's banking Open API journey.

In developing this research, Accenture utilised a number of resources to help gain a holistic understanding of the current adoption status of (and challenges faced by) each key stakeholder, namely banks as data providers, TSPs as data consumers, and customers as end-users of banking Open API products and services. These included:

- An industry survey of 28 banks, including major retail banks and all virtual banks in Hong Kong, and 31 TSP respondents that included a mix of non-bank third parties in Hong Kong, conducted between September and October 2020.
- Interviews with 53 entities conducted in October 2020, including banks, financial technology (fintech) companies operating in both the retail and commercial sectors, non-financial third-party providers across technology, telecommunications, payments, e-commerce, insurance, and transportation sectors, professional bodies including the Hong Kong Fintech Association and the Hong Kong Association of Banks, and customer focus groups involving retail customers and small and medium-sized enterprises (SMEs).
- A customer survey of more than 2,000 Hong Kong respondents conducted in 2019, and a business survey of over 50 small businesses and large corporations in Hong Kong conducted at the end of 2018.

Structure of report

02 Introduction

Open APIs allow financial institutions to open up their internal IT systems and data for programmatic access by third-party service providers (TSPs) in an open and secure manner. One example of an Open API use case is a digital application enabling banking customers to easily compare various bank products and offerings by aggregating service information from different banks into a single website.

In 2018, the HKMA published the Open API Framework to encourage the broad market adoption of Open APIs in the Hong Kong banking sector. In this section we describe the purpose of the framework, its four-phased approach, and the scope of its implementation.

03 Implementation status of banking Open APIs in Hong Kong

Since the publication of the Open API Framework in July 2018, retail banks in Hong Kong have made encouraging progress in adopting banking Open APIs in areas such as defining strategy, building business and technical API infrastructure, and adopting use cases. This study's key findings on the current implementation status of banking Open APIs are as follows:

- Both banks and TSPs have shown high readiness for adopting banking Open APIs in terms of their strategy development, investment, and organisational change. The pace of adoption has also been accelerated due to regulatory support.
- There has been a high adoption rate of Phase I and II Open API use cases within retail banking, with over 20 participating banks having made more than 800 Open APIs available to the market. The encouraging progress made by the industry thus far bodes well for the success of Phase III and IV implementation.
- Prior to formal implementation timetables being put in place for Phases III and IV, early adopters have already been moving to implement banking Open API functionality and take advantage of market opportunities.
- There has also been a noticeable shift beyond retail banking, with increased activity in the commercial (SME) banking sector. The industry has recognised the benefits of banking Open APIs for enhancing SMEs' access to financial services and meeting fast-changing business demands.
- Increased technical complexity, fraud-related threats, wider cybersecurity risks and the need for data protection represent the main challenges facing implementing parties as they handle the more complex functions of Phases III and IV of banking Open API.

04 Essential practices for implementing Phases III and IV of banking Open API

With reference to international experience in the implementation of banking Open APIs, this section describes seven essential practices for Phases III and IV that will facilitate a secure and efficient implementation for industry participants, including banks, TSPs and regulators.

Adopt appropriate risk management strategies: Monitoring and reviews of risk management frameworks need to be regularly conducted to protect against risks associated with cybersecurity, system resilience, data privacy, liability, fraud and money laundering.

Introduce appropriate protection mechanisms: Appropriate protection mechanisms are of the utmost priority and must be enabled by measures addressing data protection and retention, customer consent, protection against fraud, disclosure and transparency, and liability and redress management.

Design compelling banking Open API propositions for customers: Designing customer-centric use cases, fostering trust towards TSPs, and educating customers are essential for driving adoption of banking Open APIs.

Understand the range of bank capabilities required: To facilitate Open API implementation, banks need a defined strategy, a robust operating model and infrastructure, and technical readiness (e.g. API portals).

Understand the range of TSP capabilities required: Establishing the appropriate operating model, data management, and information security capabilities, are fundamental considerations for TSPs engaging in banking Open APIs.

Select one or more appropriate business/finance models: In designing banking Open API use cases, banks and TSPs should develop a suitable monetisation strategy, based on one of a range of direct monetisation models (e.g. freemium model, third-party pays, third-party gets paid, end user pays) and indirect monetisation models (e.g. increased reach and awareness, improved personalisation, efficiency gains).

Monitor the banking Open API ecosystem: Mechanisms for monitoring fraud, API availability and API performance are crucial to building trust and transparency among ecosystem participants and ensuring reliable banking Open API operations.

05 Proposed measures for the robust and effective implementation of Phases III and IV

Based on international practices, local industry insights and the HKMA's strategic considerations, this section sets out four key recommendations for the implementation of Phases III and IV of banking Open API:

Adopt a progressive implementation approach for selected API functions in Phases III and IV, based on viable use cases and target customer segments, having regard to the most viable use cases identified, namely (i) Personal/Business financial management, (ii) Know Your Customer (KYC)/Authentication as-a-Service, (iii) Enhanced credit profiles, and (iv) E-commerce payments.

Develop industry API technical standards for API functions selected based on the identified viable use cases, and continuously maintain these standards as additional API functions are progressively launched thereafter.

Revise the Phase II Common Baseline[1] for TSP onboarding to facilitate the implementation of Phases III and IV, enhancing the requirements where necessary.

Develop additional customer protection measures in the areas of consent management and customer education to facilitate trust across banking Open API participants.

02

Introduction

2.1 What are Open APIs?

Over recent years, Open APIs have been applied by companies in different industry sectors to expand their core businesses and develop ecosystems that enable relevant, interconnected and intelligent customer experiences. For example, travel agency websites have leveraged Open APIs to access data from hotels and airlines in order to provide real-time booking and ticketing services.

From a technical perspective, APIs are computer programming tools that facilitate the exchange of information and executing instructions between different computer systems. Open APIs refer to APIs that allow applications developed by third parties to integrate seamlessly with the overall enterprise system of an organisation. In the banking sector, Open APIs allow banks to open up their internal systems and data for programmatic access by third-party service providers (TSPs) or their counterparts in a secure and controlled manner. By providing data access to TSPs such as fintechs or players in other industries, banks can leverage the capabilities of these potential partners to innovate and offer better products and services to their customers.

2.2 Background of the HKMA's Open API Framework

The Open API Framework for the Hong Kong Banking Sector ("Open API Framework") is one of the seven Smart Banking initiatives[2] announced by the HKMA in September 2017. Following the announcement, in early 2018 the HKMA conducted an industry consultation on a draft framework with participants from banks, industry associations and other ecosystem stakeholders. With respondents proving supportive of the HKMA's policy direction, the final Open API Framework was published in July 2018. It aims to help ensure the continued competitiveness and relevance of the banking sector by enabling collaboration between banks and TSPs in developing innovative banking services that can improve customer experience.

The Open API Framework adopts a risk-based principle and has a four-phased implementation approach (Figure 1). Banks were expected to implement Open APIs according to the timeline set out in the framework starting in 2019.

In response to the framework, the local banking sector launched Phase I in January 2019 and Phase II in October 2019. Information on Phase I and II Open APIs can be found on the Data Studio website of the Hong Kong Science and Technology Parks Corporation,[3] which acts as a central repository for all the Open APIs offered by Hong Kong banks. After an industry consultation with ecosystem stakeholders including technology firms/fintech and industry bodies, the Hong Kong Association of Banks released the Common Baseline in November 2019, which is intended to facilitate and streamline banks' onboarding of TSPs to encourage adoption of Banking Open API. The Common Baseline represents a comprehensive set of business and risk management considerations that should apply to a bank's involvement in a Phase II Banking Open API collaboration, subject to an independent bilateral negotiation between a bank and a TSP.

Figure 1: Summary of the four-phased approach of the Open API Framework

Open API functions	Description and examples
I. **Product and service information**	"Read-only" information offered by banks, providing details of their products and services.
II. **Subscriptions and new applications for products/services**	Customer acquisition processes, such as online submissions/applications for credit cards, loans, or other bank products.
III. **Account information**	Retrieval and alteration (where applicable) of the account information of authenticated customers, e.g. account balances, transactions (balances, transaction history, etc.), for stand-alone or aggregated viewing.
IV. **Transactions**	Banking transactions and payments or scheduled payments/transfers initiated by authenticated customers.

03

Implementation Status of Banking Open APIs in Hong Kong

3.1 Adoption readiness

Since the issuance of the Open API Framework in July 2018, retail banks in Hong Kong have made encouraging progress in building capabilities to adopt banking Open APIs in the areas of strategy, organisation structure and API infrastructure.

Strategy

Under Phases I and II of the banking Open API Framework, banks have made good progress in formulating strategies for banking Open API adoption. According to the survey conducted by Accenture, 93% of banks have already defined, or are planning to define, a banking Open API strategy (Figure 2).

Organisation structure

Many banks are transforming their internal organisational structure in response to banking Open APIs. Of the surveyed banks, 50% indicated that they have set up, or plan to set up a central team to develop a bank-wide strategy for banking Open API development. Over two-thirds of the surveyed banks (68%) indicated that they now have, or will have, a business unit to drive banking Open API initiatives. Similarly, 68% have set up, or plan to set up, an IT team to execute banking Open API technical development (Figure 3).

Figure 2: Progress in defining a banking Open API strategy

Q: Has your bank defined, or is your bank planning to define, a banking Open API strategy?

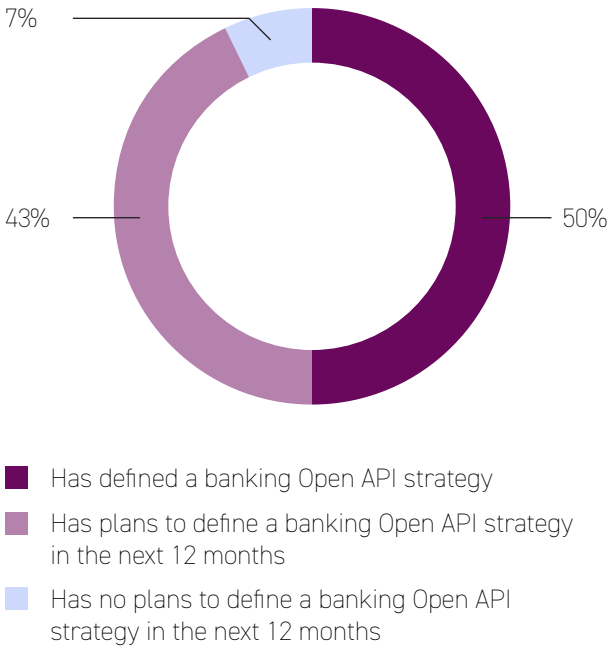
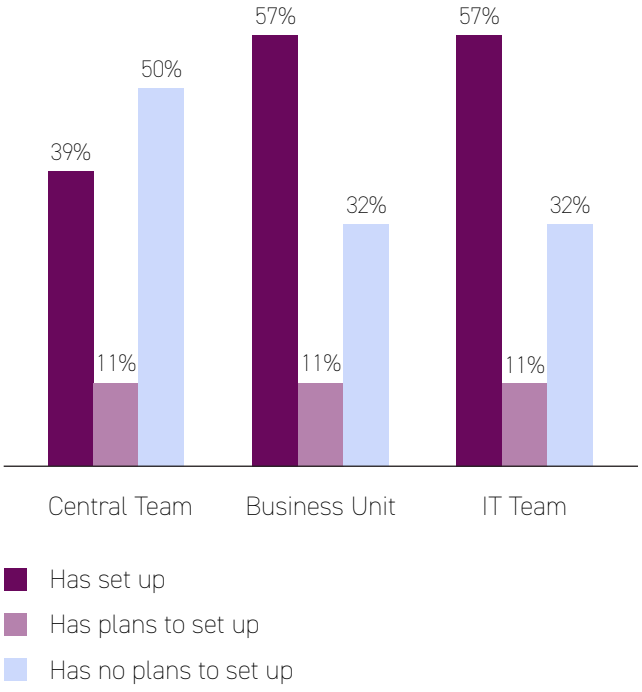


Figure 3: Organisational structures of banks for implementing banking Open APIs

Q1. Has your bank set up, or is it planning to set up, a central team for banking Open API development?

Q2. Has your bank set up, or is it planning to set up, a business unit for banking Open API development?

Q3. Has your bank set up, or is it planning to set up, an IT team for banking Open API development?



Technical readiness

In terms of technical readiness, 86% of surveyed banks have developed a banking Open API infrastructure. TSPs are relatively less mature in their technical capabilities but are gaining traction in this area, with 61% of surveyed TSPs having set up, or having plans to set up, an infrastructure to enable banking Open APIs (Figure 4).

Capital investment

To enable the capabilities mentioned above, most banks and TSPs have developed investment plans for banking Open API initiatives. A large majority (89%) of the surveyed banks have allocated a budget for banking Open API development or have already invested in various Open API initiatives (Figure 5); 56% of these have committed an investment amount of US$500,000 or above.

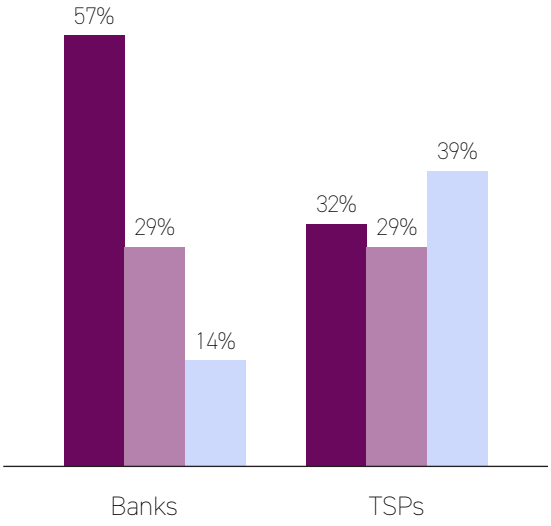
TSPs have also taken action—68% of surveyed TSPs revealed that they have invested, or plan to invest, in banking Open API initiatives. A total of 52% of these have committed an investment amount of US$500,000 or above.

Supported by the launch of the Open API Framework, most of the surveyed banks have begun their banking Open API journey. Well-defined strategies, coupled with investment in business and technical infrastructure, will be fundamental in driving and sustaining banking Open API adoption.

TSPs, meanwhile, have also shown increased interest in pursuing banking Open APIs. Their experiences in developing Open API solutions for other industries and sectors (e.g. warehouse data enquiries for suppliers or location sharing for logistics companies) can be leveraged by banks as they explore opportunities to develop new customer propositions.

Figure 4: Technical readiness of banks and TSPs for implementing banking Open APIs

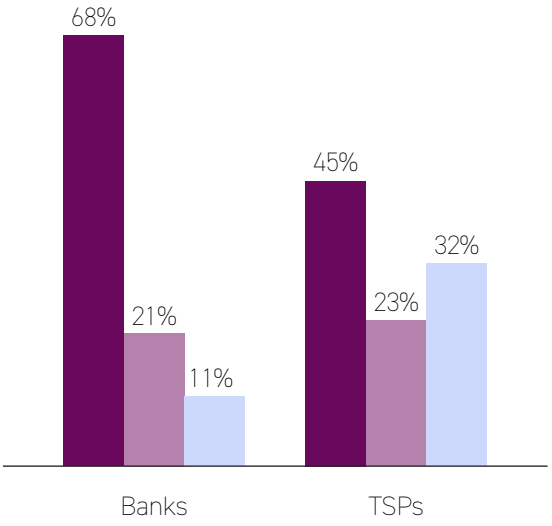
Q: Has your organisation set up, or is it planning to set up, a banking Open API infrastructure (e.g. API gateway, API developer portal) for banking Open API development?



- Has set up a banking Open API infrastructure
- Has plans to set up a banking Open API infrastructure in the next 12 months
- Has no plans to set up a banking Open API infrastructure in the next 12 months

Figure 5: Investment in banking Open APIs by banks and TSPs

Q: Has your organisation invested in, or is it planning to invest in, a banking Open API initiative?



- Has invested in a banking Open API initiative
- Has plans to invest in a banking Open API initiative in the next 12 months
- Has no plans to invest in a banking Open API initiative in the next 12 months

3.2 Phase I and II adoption status

Hong Kong's banking industry successfully launched Phases I and II of banking Open API in January 2019 and October 2019 respectively. More than 20 retail banks participated in the banking Open API initiative by offering third parties access to their product and service data, and a high adoption rate of Phase I and II use cases can be seen to date (Figure 6). Over 800 Open APIs covering a wide range of banking products and services were launched in Phases I and II.

Aside from participation by banks, the high adoption rate of banking Open APIs can also be attributed to the active participation of TSPs from various industries, including telecommunications, real estate and fintech amongst others. There were over 900 registrations by TSPs wishing to access Phase I and II Open APIs as of Q3 2020, representing growth of 240% from Q1 2019 (Figure 7).

Figure 6: Adoption status of Phase I and II retail banking use cases

Q: Has your bank launched, or is it planning to launch, any Phase I and II retail banking Open API use cases?

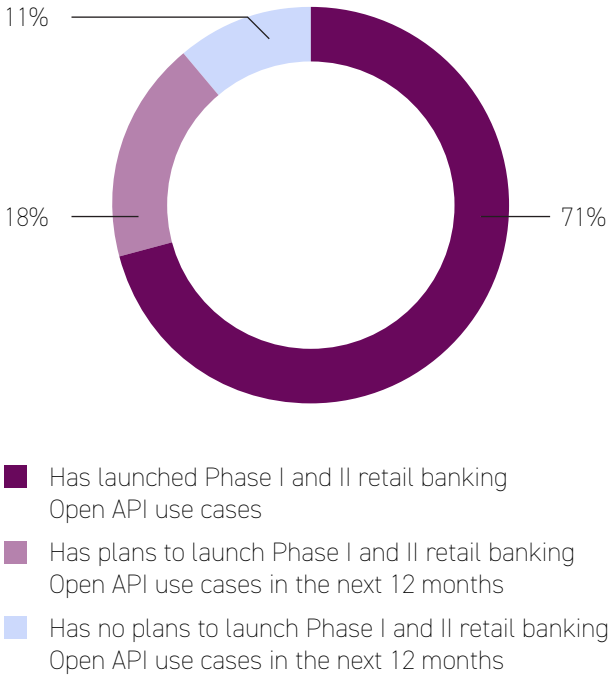
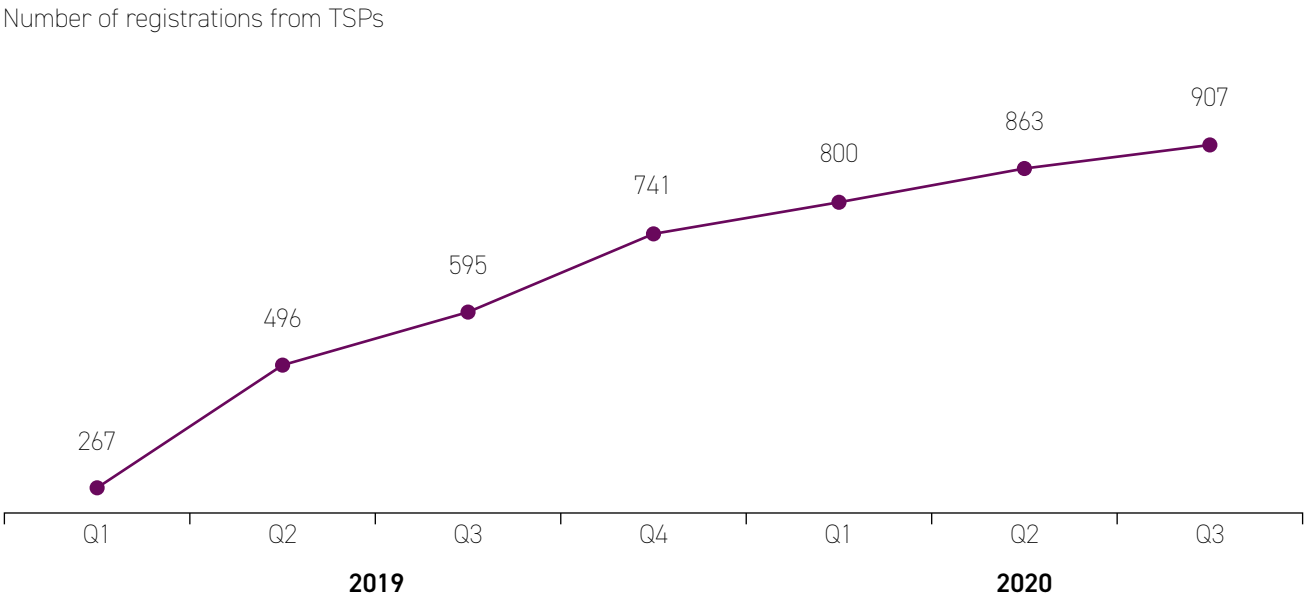


Figure 7: Number of registrations by TSPs with access to Phase I and II banking Open APIs



The most adopted categories of Phase I and II retail banking use cases include (Figure 8):

- Product and service information enquiries from third-party websites (80%), e.g. enquiries about branch locations, mortgage rates or foreign exchange rates
- Real-time product and service comparisons (52%), e.g. comparisons of time deposit interest rates, foreign exchange rates or travel insurance products
- Streamlining of product and service subscriptions (40%), e.g. applications for mortgages, credit cards or loans

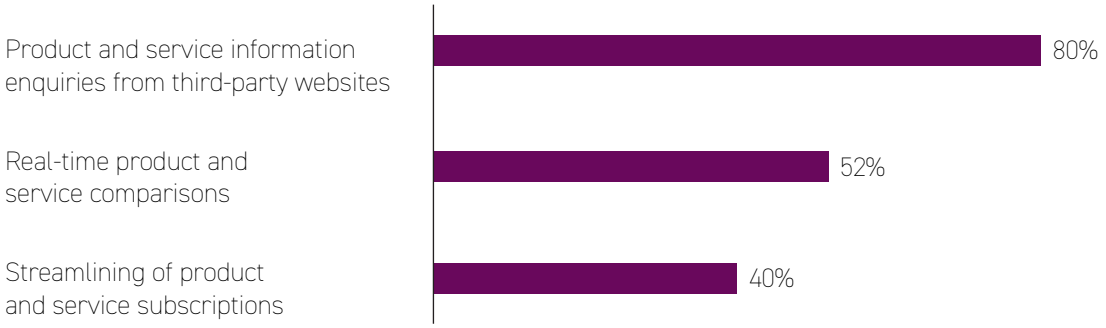
These use cases have led to increased market activities, especially for Phase II use cases.

The 68-fold increase in Phase II banking Open API quarterly calls between November 2019 and August 2020 indicates widespread uptake and a positive reception by the market (Figure 9).

On the other hand, a number of the surveyed banks stated that the banking Open API functions and data points available in Phases I and II only enabled a narrow range of use cases, with limited business benefits. These use cases are mostly related to simple product and service information enquiries and applications for products, bringing limited opportunities for TSPs to collaborate with banks. Nevertheless, Phases I and II have been recognised as building blocks that will eventually transform the banking Open API customer experience.

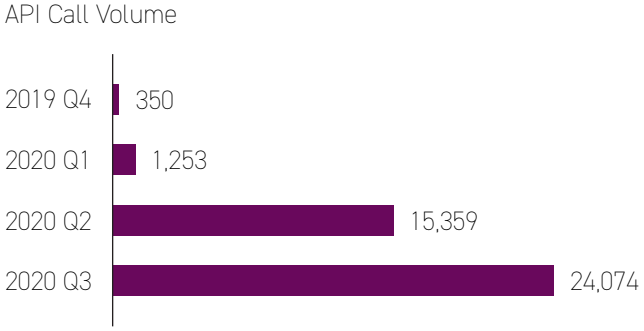
Figure 8: Most widely-adopted Phase I and II retail banking use cases

Q: If your bank has launched/planned to launch Phase I and II use cases, what are these use cases?*



* Respondents were able to submit more than one answer

Figure 9: Number of Phase II banking Open API calls from Q4 2019 to Q3 2020



3.3 Phase III and IV adoption status

Prior to the announcement of the implementation timeline for Phases III and IV, a number of banks have been proactively advancing banking Open API development to support their digital propositions. Of the surveyed banks, 36% have launched, or are planning to launch, Phase III and IV retail banking use cases (Figure 10).

The most popular Phase III and IV retail use cases launched by these banks are (Figure 11):

- Account information aggregation services (50%), e.g. consolidation of data from different bank accounts to enable a one-stop view for better financial management.
- Transaction initiation services (50%), e.g. pay-with-points/loyalty points redemption on merchant sites.

Figure 10: Adoption status of Phase III and IV retail banking use cases

Q: Has your bank launched, or is it planning to launch, any Phase III and IV retail banking Open API use cases?

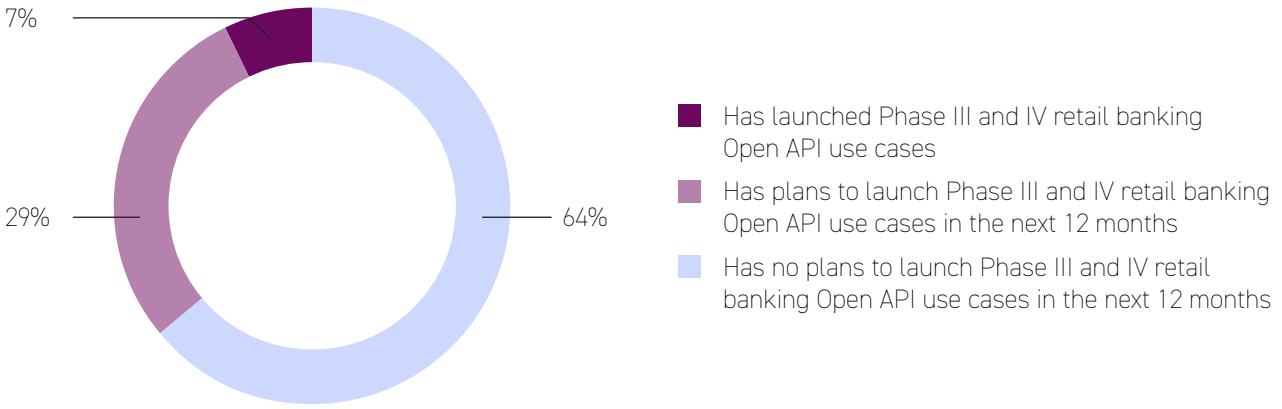
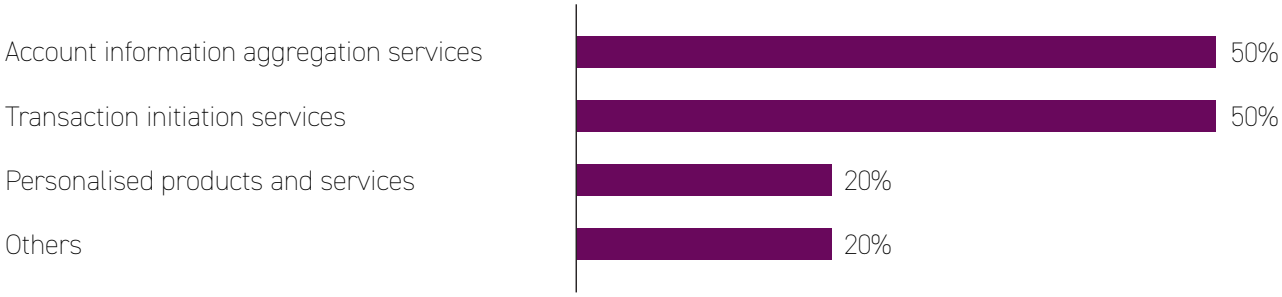


Figure 11: Most widely-adopted Phase III and IV retail banking use cases

Q: If your bank has launched or plans to launch Phase III and IV use cases as indicated in the previous question, what are these use cases?*



* Respondents were able to submit more than one answer

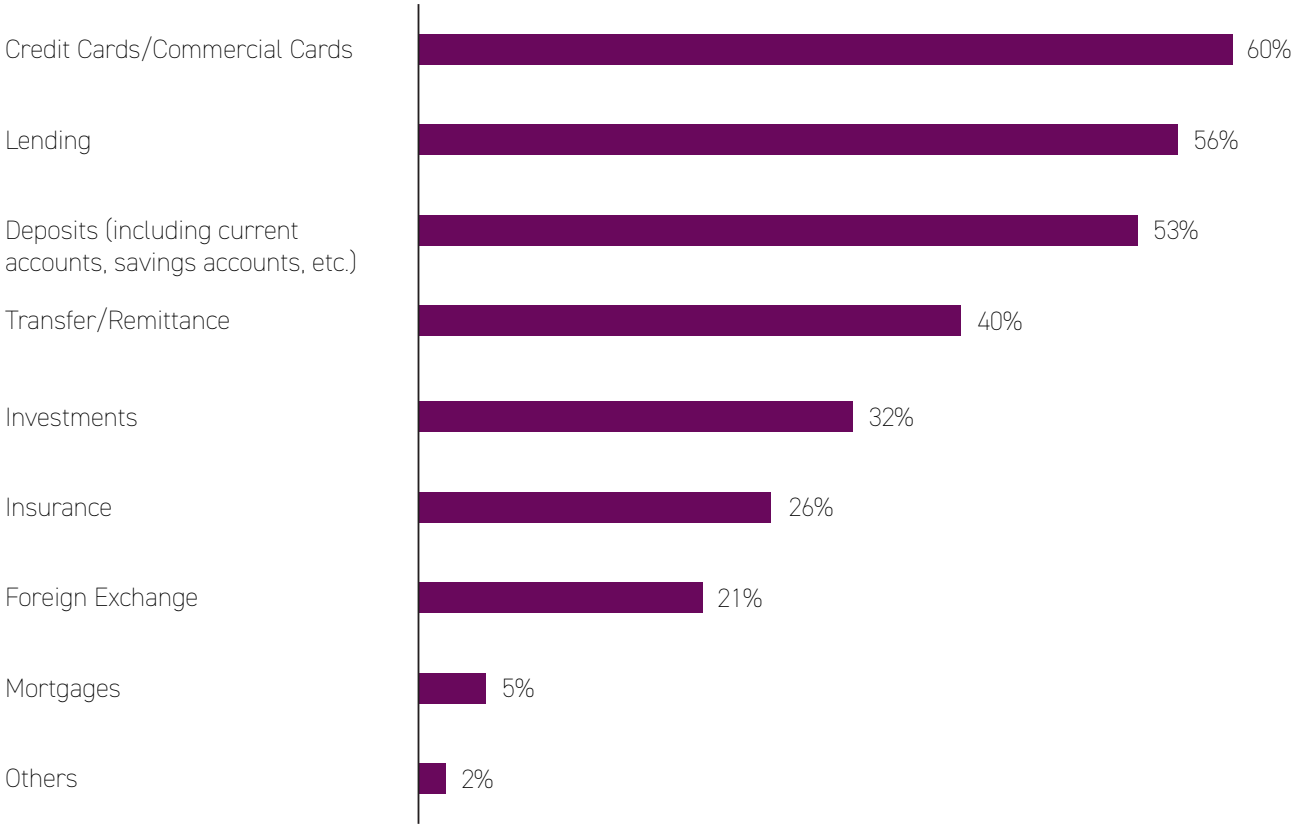
In terms of their focus on banking products in Phases III and IV, both banks and TSPs selected credit cards/commercial cards (60%), lending (56%) and deposits (53%) products as those with the highest potential value to their businesses (Figure 12).

Industry participants anticipate that the rollout of Phases III and IV will create a more complete customer journey with better value-adding services and a wider range of use cases, ranging from information enquiries and applications to personalisation and transaction initiation.

In light of the experience gained by the local banking industry in implementing Phases I and II of banking Open API, there is a high degree of confidence that subsequent phases will bring new business opportunities to banks and TSPs.

Figure 12: Commercially viable banking products available through Phase III and IV banking Open APIs

Q: Which three product categories does your organisation see as the most commercially viable through Phase III and IV banking Open APIs?



3.4 Commercial & SME banking adoption status

Although the Open API Framework focuses primarily on retail banking, banks are encouraged to extend the framework to other banking businesses as they deem appropriate. Internationally, there is a growing trend for commercial and SME banking to leverage banking Open APIs for new business opportunities.

Based on the survey findings, both banks and TSPs plan to focus on banking Open API development for retail banking in the next two years. In total, 93% and 68% of the surveyed banks and TSPs respectively consider the retail banking segment to hold the most business potential for banking Open API development.

Although the primary focus of banking Open APIs is on retail banking, some banks have started to explore extending banking Open APIs to commercial and SME banking customers—with 45% of the surveyed banks having launched, or planning to launch, commercial and SME banking use cases related to banking Open APIs (Figure 13). The use cases include:

- Prefilling of information for loan applications on third-party websites.
- Enquiries on loan interest rates or foreign exchange rates.
- Foreign exchange transfers or account payable settlements from third-party websites.
- Account information aggregation from different bank accounts.

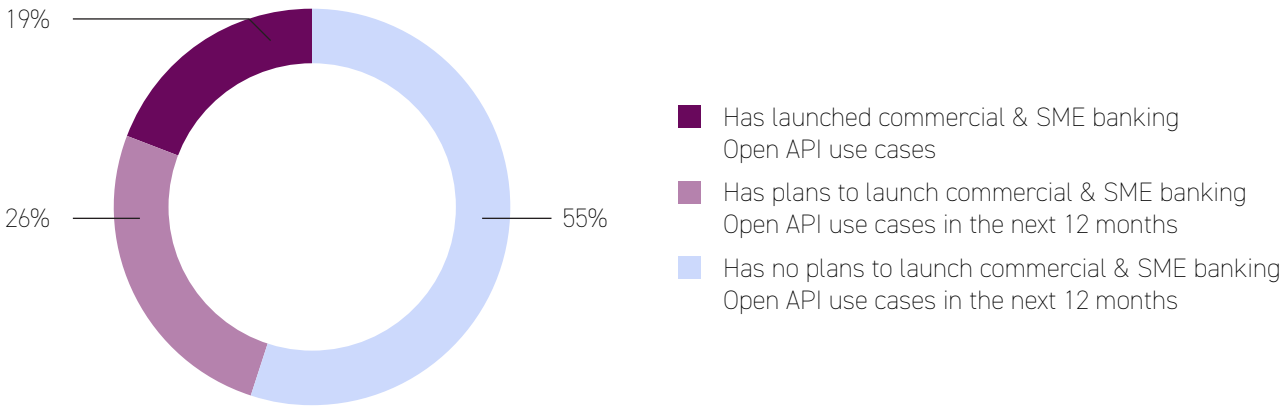
The industry interview results also show that commercial and SME banking can take advantage of banking Open APIs if the following activities are undertaken:

- The benefits of commercial and SME banking use cases are promoted.
- TSPs are actively encouraged to develop commercial and SME banking use cases.
- There is greater digitalisation of commercial and SME banking journeys and processes.

Findings from the industry interview indicate that more can be done to drive greater adoption of banking Open APIs within the commercial and SME banking sector. As gathered from respondents, the local banking sector recognises the benefits of applying banking Open APIs in commercial and SME banking. Banks are well positioned to take best practices from retail banking Open API offerings and apply them to commercial and SME banking use cases.

Figure 13: Adoption status of commercial & SME banking use cases

Q: Has your bank launched, or is it planning to launch, any commercial & SME banking Open API use cases?



3.5 Benefits of implementing banking Open APIs

Benefits to Hong Kong

The implementation of banking Open APIs will enable Hong Kong to:

Maintain its status as a leading international financial centre

Banking Open APIs are an emerging trend that have generated significant interest across major global economies. As customers shift from physical to digital banking, and as organisations fast-track digitalisation as a result of the COVID-19 pandemic, banking Open API products and services are helping to meet customers' changing expectations. Banks are encouraged to adopt banking Open APIs as a way of further advancing their delivery of innovative digital banking services in the region, and upholding Hong Kong's role as a leading international financial centre.

Drive greater innovation in the banking industry

The implementation of banking Open APIs supports the adoption of new technologies and stimulates innovation in banking services. By facilitating an ecosystem partnership environment where banks, fintechs and other non-bank TSPs can collaborate closely, banking Open APIs inject competitiveness into the banking industry and fuel the development of new product and service offerings.

Benefits to Banks and TSPs

Banking Open APIs give TSPs the opportunity to innovate and design solutions to meet customers' digital needs, while banks can leverage TSPs' capabilities to improve customer experiences. According to the survey, 98% of banks and TSPs see benefits in participating in the banking Open API ecosystem. The top three benefits of Open APIs, according to respondents, are (Figure 14):

New revenue streams

Banking Open APIs enable banks to partner with TSPs in offering new products and services to their customers, thus creating new revenue streams. To further capture banking Open API opportunities, banks can explore offering Banking-as-a-Service to TSPs, by which they provide banking capabilities to TSPs for a fee. On the other hand, TSPs can earn income from referral fees by distributing banks' products through their platforms.

Customer satisfaction and retention

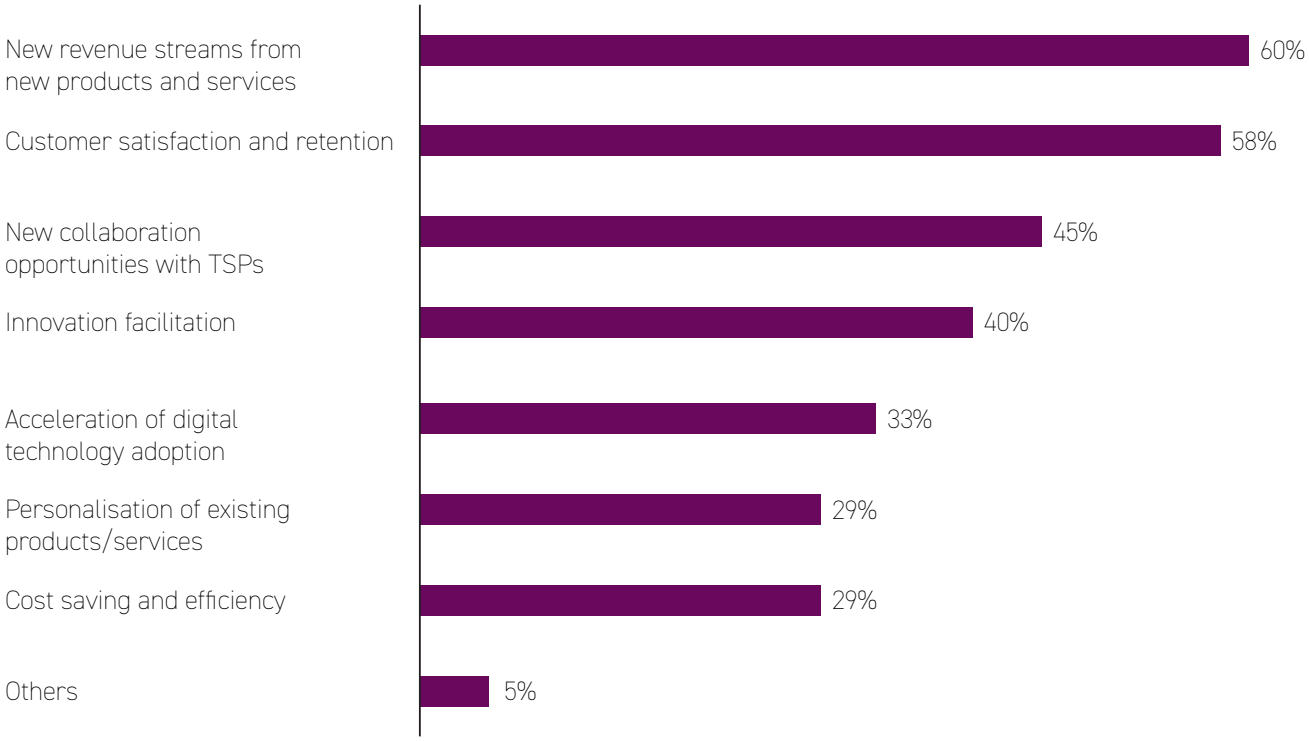
Banking Open APIs enable banks and TSPs to generate better customer insights, facilitating the design of personalised products and services that provide better customer engagement and that result in improved satisfaction and customer retention.

New collaboration opportunities with TSPs

Banking Open API partnerships enable banks and TSPs to leverage their complementary strengths and offer a wider set of products and services across each other's channels to meet customers' financial and non-financial needs.

Figure 14: Ranked benefits of banking Open APIs according to banks and TSPs

Q: Which of the following does your organisation see as the most significant benefits of banking Open API?*



* Respondents were able to submit more than one answer

Benefits to Customers

Retail Banking

According to Accenture's 2019 Hong Kong Open Banking Survey[4] (Figure 15), most surveyed retail banking customers saw "tailored offers" and "personalised services" as the top two benefits of providing data access to TSPs.

Tailored offers

Banking Open APIs allow banks and TSPs to better understand customers' behaviour and recommend financial and non-financial offers tailored to their needs. These include better mortgage rates, higher returns on deposit products, and better merchant discounts (e.g. with e-commerce platforms).

Personalised services

Banking Open APIs enable banks and TSPs to provide customers with personalised experiences that help guide their decision-making.

For example, through a personal financial management application, banks and TSPs could analyse customers' spending patterns and offer personalised advice to help them achieve their financial goals.

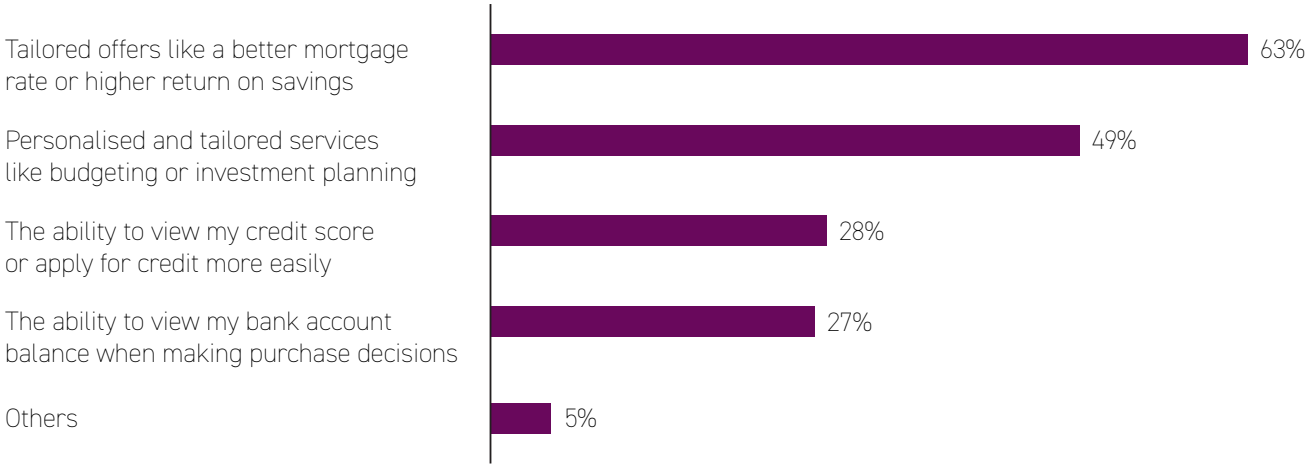
Additionally, the industry interviews suggested the following benefit for retail customers:

Improved security

The practice of "screen scraping" requires a third party to log on to applications on behalf of customers by using their credentials to access data. However, sharing of customer digital banking credentials with third parties presents a high security risk (e.g. risk of data breach or unauthorised transactions). Banking Open APIs make the process of sharing customers' data more secure by removing the need for customers to share their credentials with third parties.

Figure 15: Incentives/Benefits that would motivate retail customers to share their banking data

Q: What incentives/benefits would convince you to trust a third party or provide one with access to your banking data?*



* Respondents were able to submit more than one answer

Sample size = 2,010 Hong Kong consumers

Commercial and SME Banking

According to Accenture's 2018 Open Banking for Businesses Survey,[5] most commercial and SME banking customers see the following as the top benefits of using banking Open API services (Figure 16):

Convenient access to banking services

SMEs are perceived to be underserved as they have limited access to financing.[6] With banking Open APIs, banks and TSPs can gain a better understanding of an SME's financial position through the sharing of business transaction data, and offer the SME pre-approved lines of credit based on its business needs.

Greater reach to clients and partners

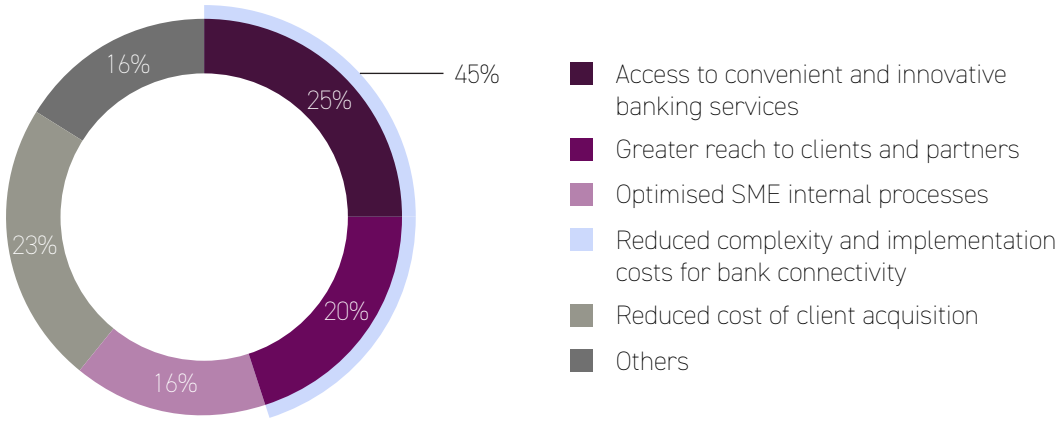
To achieve business growth, SMEs need to expand their supply chains by engaging new clients and partners. Banking Open APIs can be leveraged to create marketplace offerings where SMEs can connect with new business partners. This will lead to increased commercial opportunities among ecosystem participants, resulting in business growth.

Optimised operational efficiency

SMEs often use third-party packaged software to support their business administration activities, such as accounting, invoicing and reconciliation. Banking Open APIs can enable SMEs to connect their software to their bank accounts, allowing them to synchronise payment cycles, better manage their cashflow, and generally improve their operational efficiency.

Figure 16: Incentives/Benefits that would motivate commercial & SME customers to share their banking data

Q: What incentives/benefits would convince you to trust a third party or provide one with access to your banking data?



3.6 Challenges of implementing banking Open APIs

Challenges for Banks and TSPs

While most banks and TSPs acknowledge that banking Open APIs bring benefits and efficiency gains to the industry and to customers, both parties see risks and challenges associated with its implementation. More than half of the survey respondents indicated "fraud and cybersecurity risks", "complexity of technical development", "difficulty in identifying use cases" and "concerns around being solely liable for any faults made by partners" as major challenges in implementing banking Open APIs (Figure 17).

Threats from fraud and cybersecurity risks

Since Phases III and IV will open customer data to third parties and involve transaction processing, fraud and cybersecurity risks should be mitigated to protect customers. Interviews with banks and TSPs revealed that the maturity levels of their cybersecurity and internal risk mitigation policies varied. The lack of experience in sharing sensitive customer data between banks and TSPs is another key consideration. Established banking practices involving the secure handling of data are currently designed for internal purposes. The introduction of banking Open APIs involving the sharing of sensitive data outside bank systems presents an additional security risk that needs to be mitigated.

Figure 17: Ranked challenges of participating in banking Open APIs according to banks and TSPs

Q. What are the challenges encountered by your organisation in participating in banking Open APIs?*

* Respondents were able to submit more than one answer

Complexity of technical development

Several of the surveyed banks said they intended to undertake their own development of Phases III and IV due to data sensitivity and the associated commercial sensitivity of use cases. These banks foresee difficulties in ramping up the skills and resources needed to meet complex technical requirements.

Some bank respondents also face challenges around integrating their existing legacy infrastructure with new Open API technology, leading to the need for a longer development period. Additionally, some TSPs have noted that technical standards vary across banks, leading to higher implementation costs as they expand their partnerships with banks.

Difficulty in identifying use cases

Interviews with respondents revealed that smaller organisations and especially TSPs from non-financial sectors have encountered difficulties in identifying commercially viable use cases. Non-financial TSPs may lack experience in collaborating with banks, and this means that additional time and effort is needed to identify viable banking Open API use cases.

Concerns around being solely liable for any faults made by partners

Some of the surveyed banks and TSPs have concerns about being the sole liable party for any faults due to their partners, especially in the areas of unauthorised payments, fraudulent payment behaviour and data breaches.

Other challenges

Banks and TSPs in general face challenges around TSP onboarding. Some banks have indicated that they have limited resources and capabilities to perform the necessary TSP onboarding checks, with Phase III and IV implementation expected to result in more stringent onboarding requirements. Respondents believed that detailed onboarding requirements (e.g. specific required documentation to support TSP applications) would help streamline the Phase III and IV onboarding process.

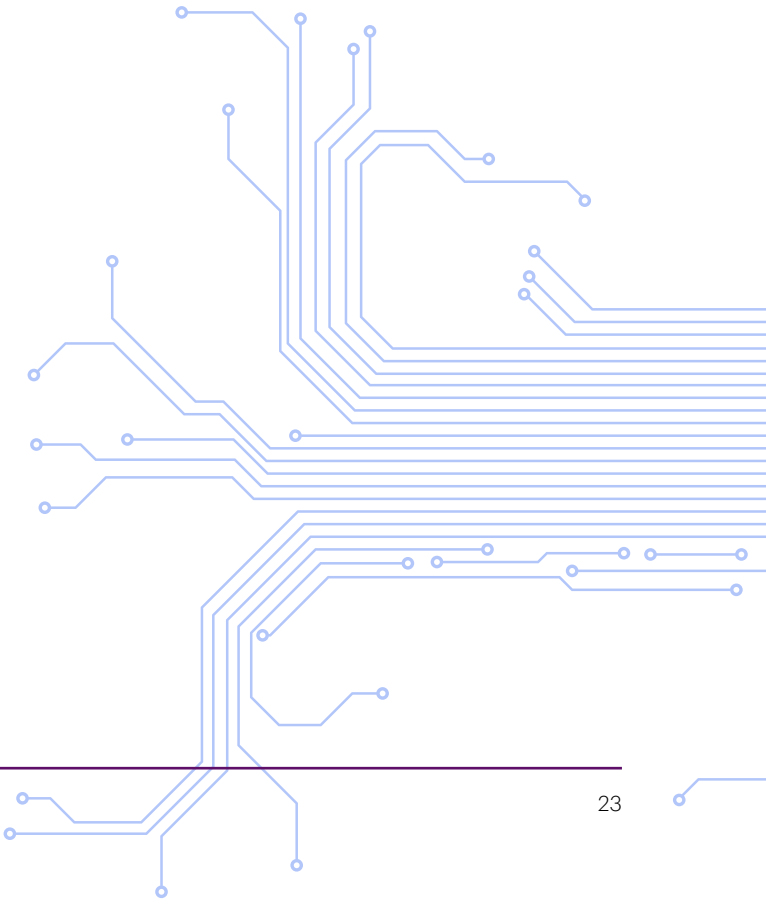
Challenges for Customers

Retail perspective

Accenture's 2019 Hong Kong Open Banking Survey shows that 71% of Hong Kong customers are concerned about data privacy. Interviewees from the customer focus groups expressed concerns about their data being shared beyond the agreed scope and purpose of their consent. Other concerns included TSPs' data protection capabilities, procedures relating to customer complaints, and liability in the event of incidents resulting in financial loss.

Commercial and SME perspectives

Data privacy and security are also key concerns for SMEs. Interviewees from the customer focus group noted that SMEs are typically cautious about giving TSPs access to their data, as data breach incidents could adversely impact their business performance. On the other hand, banks play a key role in encouraging SMEs to adopt banking Open APIs. According to Accenture's 2018 Open Banking for Businesses Survey, most SMEs (63%) were receptive to participating in banking Open APIs with their banks, compared to only 29% who were receptive to participating in banking Open APIs with non-bank TSPs.



04

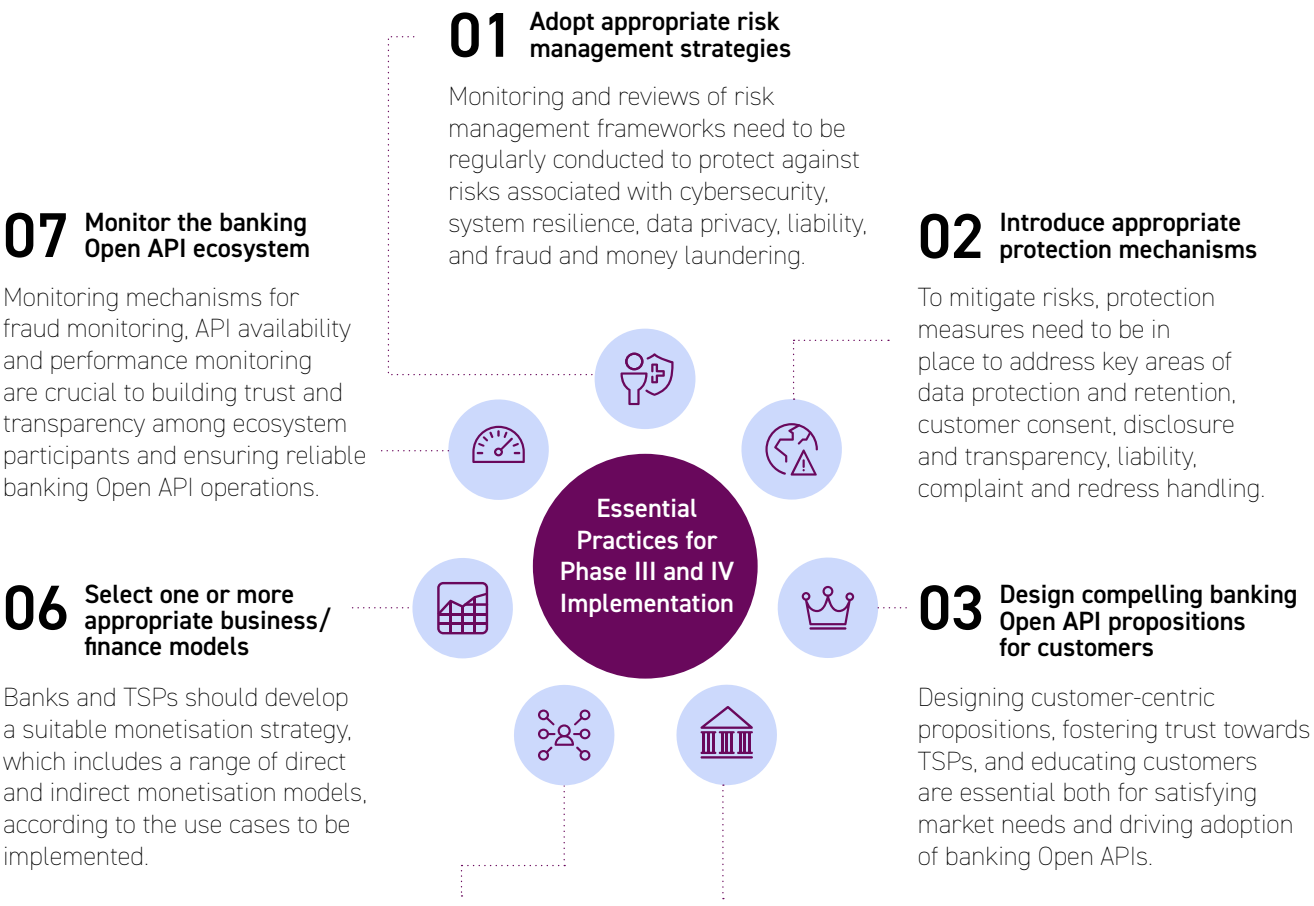
Essential Practices for Implementing Phases III and IV of Banking Open API

The potential benefits of banking Open APIs, as presented in Section 3.5, represent real opportunities for banks and non-financial organisations in Hong Kong.

Open API technology can be used to address many aspects of these organisations' internal operations and customer needs, ranging from customer services to sales and back-office operations.

However, the adoption barriers discussed in Section 3.6 need to be overcome. With reference to common practices adopted in leading international jurisdictions, this study has identified seven essential practices for addressing the challenges connected with implementing Phases III and IV. Building upon the foundations that have been laid in Phases I and II, these practices aim to help ecosystem participants, including banks and TSPs, to better navigate the banking Open API journey.

Figure 18: Essential practices for Phase III and IV implementation



4.1 Adopt appropriate risk management strategies

A risk-based approach is essential for effectively managing the risks arising from banking Open API implementation. Conducting regular risk assessments, with reviews of frameworks and processes, allows organisations to identify, assess and take appropriate mitigation measures in accordance with their level of risk. Risks that are potentially associated with banking Open API implementation are summarised below.

Cybersecurity risks

The introduction of new external interfaces enabling customer data sharing will make customer information accessible to multiple parties, bringing the risk of unauthorised intrusion into internal systems. The increased number of access points and data transmissions resulting from banking Open APIs creates potentially greater vulnerability to external hackers, who will look to exploit these for crimes such as identity theft or unauthorised transactions. In addition, cyber security vulnerabilities could lead to data integrity issues, such as the provision of inaccurate or inconsistent data for processing.

System resilience risks

Banking Open API-driven partnerships will continue to grow as more customers adopt banking Open API products and services. As ecosystem participants become more technologically interdependent in delivering new banking Open API-enabled innovations to customers, system outages caused by infrastructure or application failures in one party's system could have a significant operational impact on its partners if they are unable to provide a business-as-usual service to customers.

Data privacy risks

Unauthorised data access occurs when customer data is shared with third parties without explicit customer consent, or when it is used for purposes outside of the consent provided for account information and transaction purposes. Additionally, data privacy risks can stem from an organisation's inexperience in or lack of sensitive data handling practices. Lack of proactive data protection capabilities to prevent malware attacks also makes organisations more susceptible to a data breach.

Liability risks

In cases of disputed transactions (e.g. payment errors or unauthorised access resulting in customer financial loss), it may be unclear whether banks or TSPs have liability. Lack of proper liability handling may lead to significant financial and reputational impact for the parties involved.

Fraud and money laundering risks

As transactions involving multiple parties increase with the implementation of banking Open APIs, challenges relating to monitoring transactions to detect fraud and money laundering risks are expected to arise. Existing detection systems may not be adequate to effectively manage these risks in this new environment.

4.2 Introduce appropriate protection mechanisms

Proper protection measures are an important part of any comprehensive risk management strategy. Common protection measures have been adopted in other jurisdictions when implementing banking Open APIs. These measures are outlined below.

Data protection and retention

As Phases III and IV involve the handling of sensitive customer data, implementing proper data protection and retention practices will help safeguard customer interests. In line with the Personal Data (Privacy) Ordinance, as well as any other relevant codes of practice issued by the Privacy Commissioner of Personal Data (PCPD), organisations need to establish a clear data protection and retention policy with protocols for safeguarding information. Data that is no longer in use should be securely disposed of once customer consent is withdrawn or has expired within the data retention period required by law.

The use, access or storage of customer data for any purpose is not permitted except for the provision of the account information or payment initiation service explicitly requested by the customer. Third parties storing customer data need to be equipped with well-defined capabilities to manage data acquired through banking Open APIs. These include capabilities to handle token-based authentication, consent management and data privacy.

Customer consent

To ensure customer data is only used for the purposes of account information and transaction, customers should provide explicit consent for the use of their data. An appropriate period for the consent to remain effective increases data sharing security, with customers performing re-authentication with their banks to continue their consent. Due to the sensitivity of the data, appropriate customer authentication methods such as two-factor authentication should be established to reduce the chance of identity theft or fraud by making it harder for attackers to access data. Customers should always have control over their data and be able to access, manage or withdraw their consent at any point in time.

To support consent management practices, banks and TSPs will need to develop and agree on a consent management mechanism which includes a clear set of policies and processes. For example, when requesting customers' consent for data sharing, consent details need to be clearly communicated. These include the reason for accessing the data, the scope of the data being shared, and how long the data will be used. Additionally, consent withdrawal handling needs to be transparent to customers at the point of requesting data access, with functionality available when customers wish to withdraw their consent. When consents have been withdrawn or have expired, the data that a customer has provided should be deleted in adherence to the Personal Data (Privacy) Ordinance, as well as any other relevant codes of practice issued by the Privacy Commissioner of Personal Data (PCPD). The proper documentation and maintenance of consent records (e.g. data consented by customer, duration of consent, withdrawal of consent) also facilitates the handling of potential disputes.

Protection against fraud

To protect customers' data from fraud, an authentication process whereby customers confirm the third party's data sharing request with their bank needs to be in place. Two authentication processes are commonly adopted in other jurisdictions, namely the 'redirection' model and the 'decoupled' model.

The redirection model requires customers to be redirected to their bank's app from the third-party app. Once redirected to their bank's app, the customer can authenticate and consent to the data sharing request, and then return to the third-party app to continue their journey. The redirection model eliminates the need for customers to manually provide their banking credentials to third parties in order to receive the service provided by them.

The decoupled model separates the bank and TSP interactions. The TSP sends a customer's consent request to the bank. The bank then sends a notification to the customer for authentication and approval. The customer authenticates and approves the consent request in the bank's channel at their own convenience, and the TSP is notified by the banks accordingly.

When considering the implementation of authentication models, the following guiding principles should be considered:

1. Two-factor authentication

Banks should apply two-factor authentication to verify a customer's identity prior to executing a TSP's request for consent.

2. Authentication method

Customers should be able to use the normal two-factor authentication methods (e.g. user name, password, one-time passcode) when they are authenticating with their banks. However, TSPs should not collect or store customers' login credentials when providing any products and services, to prevent fraud due to the leakage of the credentials. This method of handling credentials should be stated clearly on customer-facing interfaces.

3. Customer experience

The authentication journey involving TSP applications should not involve additional steps or greater friction than in equivalent bank authentication journeys for other banking transactions.

Effective authentication methods to verify the identity of customers trying to log in to their account help mitigate the risk of unauthorised access. The use of two-factor authentication, in which customers are required to present two different sets of credentials (e.g. a login password and a fingerprint scan), adds an additional layer of security in preventing unauthorised access to customers' TSP accounts. Adequate security controls also need to be in place, such as increasing the strength of customers' login passwords by including a Personal Identification Number (PIN), disallowing repeated login attempts using invalid passwords, and sending periodic reminders to customers whose passwords have remained unchanged for a long period of time to change them.

As the adoption of Open Banking APIs increases, phishing attacks will become common security challenges faced by both consumers and businesses in keeping their information secure. Common practices in other jurisdictions to address this risk include regularly assessing the associated risks and implementing relevant mitigating control measures to minimise potential impact on their customers. These may include:

a. Educating customers proactively about phishing scams and adopting effective methods to enable customers to distinguish phishing messages from genuine messages.

b. Ensuring customer-facing interfaces (web/mobile) are up to date, and have the latest security patches.

c. Arranging regular cyber security and awareness training for employees on phishing techniques, and deploying appropriate defences against them.

d. Ensuring security of information, and using certificates for secure data transmission.

e. Implementing additional authentication methods (e.g. device binding/trusted browser) to safeguard against phishing risks.

Disclosure and transparency

Customer transparency sits at the centre of banking Open API product and service design. To enable customers to make informed data sharing decisions, banks and TSPs need to help them to understand the implications of data sharing before they approve and agree to the terms and conditions of consent.

Besides, the common international practice is for banks to make a list of their TSPs accessible to their customers, including listing the category of products and services offered by each of their partners and providing timely updates to that list and the relevant central register, like the one currently maintained by the Data Studio of the Hong Kong Science and Technology Parks Corporation.

Liability management, customer complaint and redress management

As customers will interact with both banks and TSPs in banking Open APIs, appropriate liability models and redress mechanisms should be established for handling customer complaints and resolving disputes. These details should be set out in the bilateral agreements between banks and TSPs.

Ideally, a liability model should describe the primary responsible party for immediate liability in case of incidents such as payment errors or unauthorised payments. Customers should not be responsible for any direct loss as a result of unauthorised transactions conducted through their accounts due to services offered under banking Open APIs, except in cases of customer fraudulence or gross negligence. To mitigate some potential risks arising from services delivered collaboratively by banks and TSPs (e.g. customers not being properly compensated for loss arising from unauthorised transactions), one option might be for banks and TSPs to have insurance coverage where appropriate or necessary, taking into consideration the risk associated with the services (i.e. on a risk basis).

International practice indicates that it is important for banks and TSPs to develop customer complaint resolution mechanisms with clearly defined roles and responsibilities, and have sufficient channels available to customers for lodging complaints, including both physical and digital channels. Once a customer files a complaint, it needs to be assigned to a designated handler, resolved within a defined period, and properly documented and stored for dispute-handling and audit purposes.

4.3 Design compelling banking Open API propositions for customers

Banking Open API offerings are at an early stage of evolution and customer uptake is gradual, but many expect this trend to accelerate and reshape the banking industry in the near future. Key factors in the success of banking Open API adoption will be the receptiveness of consumers to potential offerings, and the ability of banks and TSPs to create value by using shared data to meet customers' emerging needs while also addressing any security concerns.

Based on insights from customer focus groups and international observations, this report puts forward the following principles for developing customer propositions in relation to banking Open APIs:

Provide the right motivation for change

Industry participants shared two key factors that they felt would draw in customers if incorporated into the design of Open API use cases. The first is a frictionless sign-up process that would result in a streamlined registration experience, with minimal data input requirements. Secondly, offering rewards is likely to attract customers to try out new digital propositions. The scope and type of the rewards would need to be carefully designed to ensure they deliver value to end customers.

Nevertheless, customers may remain reluctant to adopt banking Open APIs due to concerns about data privacy. They may also lack motivation to shift from existing services and offerings. A key to driving adoption will be for banks and TSPs to identify the appropriate target customer segment and provide a compelling value proposition that necessitates the safe and secure adoption of banking Open API-related functionality, products or services.

Unlock the full potential of use cases

Partially enabled use cases (e.g. those having no straight-through processing, resulting in incomplete data sets and inaccurate advice) will only discourage users from adopting banking Open APIs. To overcome these, the design of use cases should involve thorough research and prototyping, close collaboration with partners and customers, and continuous process improvements based on customer feedback.

Give customers a sense of ownership

Data ownership should be retained by customers. Providing customers with control over their financial data and information on how their data will be used fosters their trust in using banking Open API services. Banks and TSPs should implement consent management journeys in which customer data is only shared to TSPs for the purpose of account information and transaction, upon the provision of explicit consent by customers.

Other considerations

Some additional considerations for improving customer receptiveness are outlined below:

Fostering trust towards TSPs

Customers are generally hesitant about sharing their banking data with non-bank TSPs due to concerns around data security. To address these customer concerns, appropriate internal controls and processes need to be in place for the handling of customer financial data, including an effective mechanism with banks to resolve incidents, supported by audit records and reporting.

Industry alliances between banks and TSPs can also play a role in increasing customer confidence. For example, having a common guideline on complaint and financial loss compensation handling to address incidents would build customers' trust in using banking Open API services.

Educating customers

Customer education is crucial to improving customer confidence in Open API initiatives. Being trusted partners to their customers, banks play a leading role in educating customers on what banking Open APIs are, the importance of customer authentication, as well as on the risk mitigation measures in place to protect and support customers. Banks can enhance customer education on the importance of referring to the bank's list and the central register of partnering TSPs and their relevant partnering products and services, and of being vigilant for fake websites, bogus calls or other similar scams (e.g. alerting customers of scams and educating them to authenticate the identity of callers or senders who purport to be bank representatives by using the relevant bank hotlines for this purpose, details of which can be found on the banks' official websites).

4.4 Understand the range of bank capabilities required

Having their banking Open API vision, strategy and role within the ecosystem (e.g. as data provider, data consumer or both) clearly defined enables banks to identify potential partners and capture new market opportunities early on. Examples of banking Open API strategies include:

- Expanding bank product reach by creating new distribution channels via third-party offerings/platforms
- Extending product/service offerings beyond financial services to other non-banking products/services
- Creating a financial marketplace for personalised financial/non-financial products

Operationally, it is important for banks to develop the capabilities outlined below when implementing their banking Open API strategies.

Federated operating model

A "federated" operating model for designing, implementing and managing banking Open API initiatives could be considered for effective and efficient banking Open API implementation. Under a federated model, a central team provides overall strategy and direction in key areas such as TSP partner management, governance and technology, while lines of business teams collaborate closely with the central team to execute banking Open API initiatives based on their respective business priorities.

Robust core system

Banking systems running on legacy technology are potentially limited in their ability to support banking Open API data sharing. To support banking Open API data sharing and reduce the interaction time between core processing systems, a decoupled architecture which enables system components or layers to execute independently could be considered.

Customer authentication

Customer data protection is of the utmost priority in the delivery of banking Open API products and services. Industry standards for authentication and authorisation, including OAuth 2.0 Authorisation[7] and OpenID Connect[8] frameworks, can be leveraged for the secure sharing of customer data.

Developer portal

An API developer portal enables third-party developers to access banking Open APIs in an open and secure manner. As the number of third parties involved in Phases III and IV increases, banks equipped with an API developer portal with comprehensive capabilities can more effectively collaborate with TSPs in developing new banking Open API services.

Key features for banks to consider when developing or advancing their API developer portals are:

- **Enabling ease of access** through a streamlined registration process for developers
- **Offering a sandbox environment** for testing new propositions
- **Providing developer support** such as API technical documentation, including security requirements

Information security and cyber resilience

The number of third-party connections is expected to increase significantly as banking Open APIs become more mature and more widely adopted. Proactive measures in the areas of cyber resilience, data transmission and data storage can protect banks and customers from the associated information security risks. Examples of these measures include:

- Adopting security measures and requirements such as access control, data loss prevention, vulnerability management and application patching.
- Implementing an authentication capability to verify partners' and customers' identities.
- Applying strong data encryption with sound encryption key practices to protect the confidentiality of customers' information when stored and transmitted over networks.
- Performing transaction risk analysis and fraud monitoring, especially for payment-related transactions.
- Undertaking regular monitoring of the latest cyber threat landscape and implementing appropriate measures to mitigate those threats.
- Verifying and testing the system resilience to ensure there is no single point of failure in systems or infrastructure, and no dependency on less critical systems.

4.5 Understand the range of TSP capabilities required

TSPs wishing to participate in the banking Open API ecosystem are advised to formulate an appropriate business strategy. With reference to the available use cases, three broad roles are available for TSPs. The first is that of an "Account Information Aggregator", where TSPs leverage customer data to provide services such as personal or business financial management. The second is that of a "Payment Initiation Service Provider", where TSPs enable customers to make payments on a third-party platform. Thirdly, TSPs can consider operating as a "Technical Service Provider" where they provide services to other TSPs by exposing unified APIs, which are common API endpoints that enable TSPs to connect with different banks through a single connection instead of multiple individual API connections.

From an operational perspective, operating models, data management and information security capabilities need to be considered when engaging in banking Open APIs.

Operating model

A robust operating model enables TSPs to effectively partner and engage with banks in banking Open API collaboration. For large corporations or non-bank TSPs, banking Open API programmes and partnerships can be managed by existing relationship management or product development teams. Fintechs or start-up TSPs without an established engagement structure can leverage their existing management or leadership teams to initiate discussions and manage banking Open API execution.

Data management

TSPs need to be able to manage the customer data that they collect in an efficient and cost-effective manner, while complying with the Personal Data (Privacy) Ordinance (PDPO), any other relevant codes of practice issued by the PCPD, and other industry best practices.

Additionally, TSPs engaging in the roles of Account Information Aggregation or Technical Service Provider can consider enhancing their data management capabilities in the following respects:

- **Data aggregation** – Ability to ingest and aggregate raw data from various banks
- **Data enrichment** – Ability to enrich the aggregated raw data with additional context information (geo location, time, device, etc.)
- **Data segmentation** – Ability to segment the enriched data and create data sets for additional analysis (affordability, credit scoring, etc.)
- **Data analytics and insights** – Ability to create data models for capturing additional insights to satisfy use case or customer journey requirements

Information security

By having comprehensive policies, procedures and governance in place, TSPs demonstrate their ability to protect banking Open API data and mitigate security risks. Examples of such security measures include:

- Developing and regularly reviewing information security policies and procedures, e.g. protocols for dealing with stolen or lost customer data.
- Establishing an information security organisation and governance structure, with adequate resources, processes and technology to implement and maintain effective security controls.
- Ensuring strong IT systems controls covering infrastructure and applications throughout the development life cycle.
- Defining adequate controls for personnel with access to sensitive information, e.g. conducting mandatory background checks, restricting access to authorised persons only.
- Developing strong security awareness within the organisation by conducting and regularly refreshing security training for employees.

4.6 Select one or more appropriate business/ finance models

Banking Open APIs offer banks and TSPs new revenue and process optimisation opportunities in an increasingly disrupted and competitive financial services landscape. Figure 19 shows sample business and financial models for monetising banking Open API offerings, which can be considered based on the types of use cases to be adopted.

4.7 Monitor the banking Open API ecosystem

To promote trust in the reliability of banking Open APIs, a monitoring mechanism for fraud, API availability and performance is desirable. Reference can be made to established practices in leading jurisdictions such as the UK and the EU. The purpose and implementation of each monitoring component is as follows.

Fraud monitoring

A transaction monitoring mechanism could be developed that involves the regular review of statistical reports on fraudulent transactions (e.g. number of fraud incidents, total value of fraud, description of fraud or payment type). Evaluation of the compiled data enables any systemic risks or gaps to be identified, and resolutions developed to address these.

API availability and performance monitoring

To deliver reliable services to their customers, TSPs need to rely on well-functioning banking Open APIs from banks. Any degradation in banking Open API services for customers will have a negative business impact. By establishing proactive banking Open API availability and API performance monitoring with regular reviews of key performance indicators (e.g. API availability, response times, successful call rates), banks and TSPs can improve customer experience.

Figure 19: Business and finance model summary

Direct monetisation	1 **Freemium model**	Banks/TSPs provide access to an API product/service by offering it for free up to a predefined limit, and charging for the use of features beyond this limit.
	2 **Third-party pays**	TSPs pay the bank for using Open APIs through different monetisation models (e.g. tiered, pay-as-you-go or monthly subscription).
	3 **Third-party gets paid**	Banks pay the TSP for using their APIs, especially if these APIs generate new product or service revenues for the bank (e.g. pay-per-click, pay-per-customer acquisition or pay-per-referral).
	4 **End user pays**	End users (consumers or businesses) pay the product/service provider directly for the use of products/services enabled by banking Open APIs (e.g. subscription or pay-per-transaction).
Indirect monetisation	5 **Increased reach and awareness**	Banks leverage third-party platforms as additional distribution channels for banking products/services to enable cross-selling to existing or new customers.
	6 **Improved personalisation**	Banks/TSPs leverage Open APIs to deliver a personalised experience to customers.
	7 **Efficiency gains**	Banks/TSPs optimise internal processes and reduce costs by using Open APIs: • Fraud monitoring and risk management cost reduction by introducing risk mitigation use cases. • KYC/authentication cost reduction by streamlining processes through sharing of customers' profiles. • Servicing cost reduction by digitalising manual processes.

05

Proposed Measures for the Robust and Effective Implementation of Phases III and IV

The four recommendations in this section aim to facilitate the implementation of Phases III and IV of banking Open API, and support the wider adoption of the associated products and services in Hong Kong. These recommendations have been formulated based on an analysis of benefits to the Hong Kong economy, local industry receptiveness, and an evaluation of implementation approaches across leading international banking Open API jurisdictions.

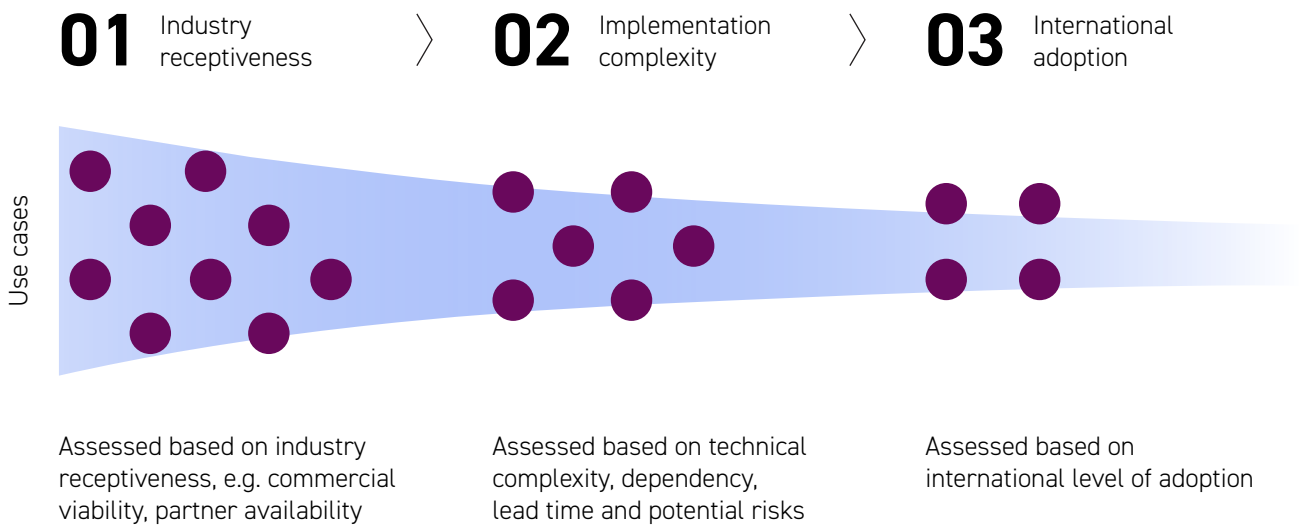
5.1 Progressive implementation

A progressive implementation is recommended for Phases III and IV of banking Open API, with selected "high-value" API functions prioritised. The participating banks and TSPs will be positioned to incrementally adopt API functions, lowering overall implementation costs and risks while also incrementally increasing customer confidence in the banking Open API ecosystem.

Use-case-driven approach: In order to determine the scope of API functions for initial phase implementation, a use-case-driven approach can be adopted. For example, an account information aggregation use case would require API functions such as retrieval of deposit account balance and transaction details, while a transaction initiation use case would require an API function like process fund transfer request.

This report has used a stage-gated framework, where each stage depends on the outcome of the previous one, to identify and prioritise the most viable use cases for Phase III and IV implementation based on industry receptiveness, implementation complexity and international adoption (Figure 20).

Figure 20: Use case viability evaluation framework



Use cases that were shortlisted on the basis of industry receptiveness were then evaluated for implementation and technical complexity, and finally assessed against their respective adoption in international markets. In the end, four use cases—applicable to both the retail and SME segments—were identified as most viable and promising (Figure 21):

i. Personal/Business financial management

ii. KYC/Authentication as-a-Service

iii. Enhanced credit profiles

iv. E-commerce payments

Implementing parties are encouraged to review the value proposition of these use cases and consider the following implementation criteria:

- **Industry receptiveness:** Prioritise use cases with higher industry receptiveness, taking into consideration their commercial viability and the availability of TSP partners in the market.
- **Technical complexity:** Select use cases with less complex technology, lower levels of external dependency and shorter development times, and develop these incrementally to reduce technology risk.
- **Risk:** Assess potential risks of use cases (e.g. fraud, data breach).
- **International adoption:** Consider use cases with high adoption rates in overseas markets so that local industry players can draw on the experiences of these markets to lower the overall risks of implementation.

In addition to the above criteria, banks can target a specific banking segment for initial implementation and thus conduct a more focused implementation with lower risk, delivering incremental value to the Hong Kong economy in a safe and secure manner.

Figure 21: Descriptions of the most viable use cases identified

Proposition	Viable use case	Target customers	Description
Financial aggregation services	Personal/ Business finance management	Retail, SME	Enables retail customers/businesses to view and manage their finances across different bank accounts in one place. Common value-adding services include providing customers with financial insights, e.g. spending pattern analysis for retail customers or cashflow optimisation for businesses
	Enhanced credit profiles	Retail, SME	Improves the credit risk profiles of retail customers/ businesses by aggregating data sources to facilitate digital lending
Process streamlining and efficiency optimisation	KYC/Authentication as-a-service	Retail, SME	Enables banks to share retail customer/business profiles for the purposes of KYC/authentication services—supporting quick verification of an identity on a third-party platform
	E-commerce payments	Retail, SME	Enables third parties to initiate payments on behalf of retail customers/businesses, instead of using payment gateways with higher costs

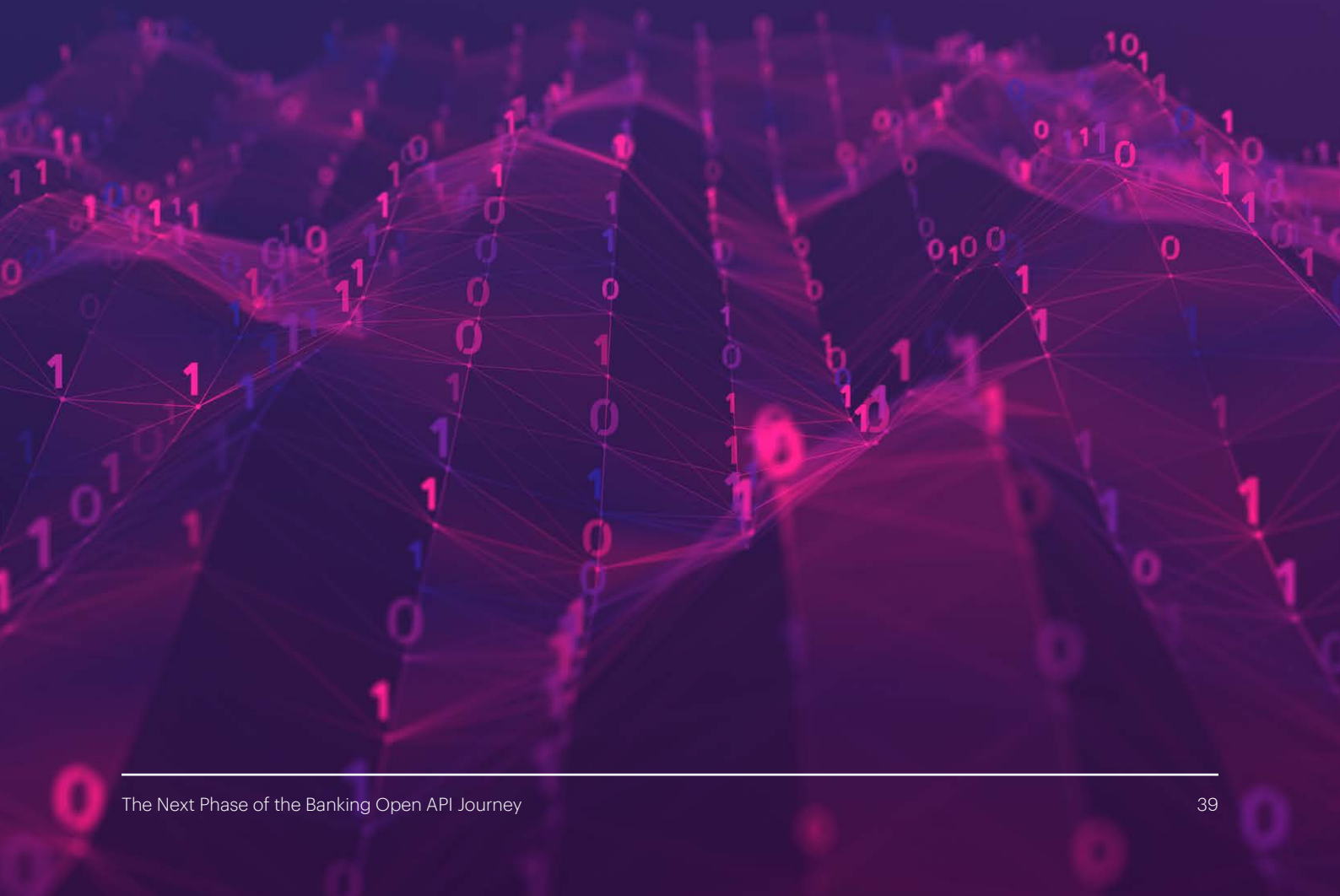
Banking segment identification

Retail banking has been the early focus of banking Open APIs across many international jurisdictions. This has led to greater investment in and a high uptake of API utilisation in the sector. Banks in Hong Kong are expected to follow this trend, driven by a large retail customer base.

The early success of banking Open APIs in the retail sector has meant that there is now increased interest in the commercial and SME banking sector, due to increasing SME needs and the potential value in delivering products and services to this market. Accenture's research shows clear opportunities to create value from commercial open banking services, if banks can deliver what their clients want – particularly given the trust those clients place in their banking partners. Banking Open APIs offer an opportunity to better serve SME needs (including those relating to cash flow management, accounting services or taxation support) by removing manual administrative processes and freeing up internal SME capacity to focus on additional value-adding activity.

During the economic recovery from COVID-19, banking Open APIs could potentially increase financial inclusion for SMEs by making lending processes faster and more reliable, by providing a more comprehensive view of SMEs' financial positions.[9] SME financing is also expected to be facilitated by other HKMA's SME-focused initiatives (e.g. the Commercial Data Interchange or alternative credit assessment technology), bringing further economic benefits.

To conclude, a progressive implementation approach involves firstly assessing the viability of different use cases, secondly identifying the associated API functions in scope for implementation, and in parallel identifying a distinct banking segment to further lower the implementation risk. Although this approach is recommended for Phase III and IV implementation, individual banks are welcome to move forward at their own pace in implementing API functions beyond the initial scope to be set out for Phases III and IV.



5.2 Open API technical standardisation

The experience of international jurisdictions in banking Open API development indicates that common API technical standards play an important role in safe and secure Open API implementation. Having common Open API technical standards brings a wide range of benefits:

Security: Standardised data policies, such as two-factor authentication and consent requirements, help mitigate the risks associated with data sharing and protect customer data at all times. The widespread adoption of such protocols strengthens security and smooths collaboration amongst ecosystem participants.

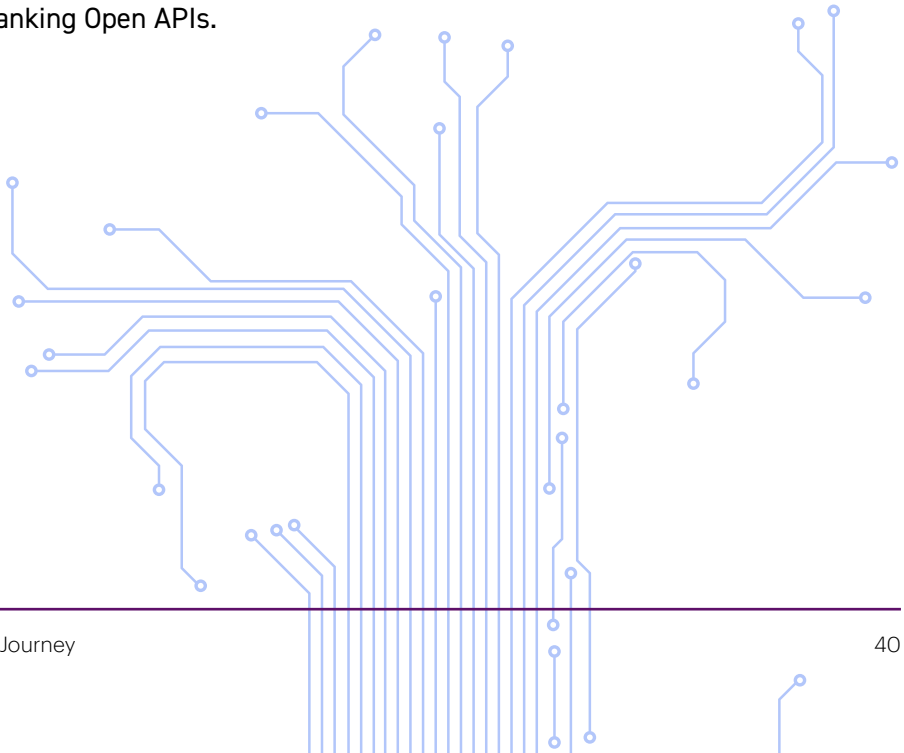
Faster rollout of new products and services with lower implementation costs: The adoption of common technical standards enables developers to easily create new products and services and deliver them more quickly across banks and TSPs, minimising the development costs associated with having to modify and integrate solutions across different parties.

Accelerated pace of innovation and adoption: Once implementing parties become familiar with the common technical standards, they can place greater focus on developing innovative product propositions. As more use cases are launched and greater value is realised from their applications, the groundswell of initiatives is expected to lead to increased industry adoption of banking Open APIs.

The importance of standardisation is also well recognised by the local banking industry. According to the survey of this study, all industry participants believe that developing Open API technical standards would be beneficial in facilitating the implementation of Phases III and IV.

Based on the consultation and exchanges with the industry, this report recommends the following approach to be taken in the development of technical API standards in Hong Kong:

- The HKMA could facilitate an industry-led API technical standardisation approach that builds on the high-level API standards defined in the Open API Framework published in 2018. That framework's API technical requirements could form the basis for industry participants to develop detailed API technical standards.
- Industry participants could work collaboratively to develop and maintain detailed API technical standards based on the principles outlined in the framework for implementing Phases III and IV of banking Open API.
- Development of API technical standards could begin for API functions selected based on the most viable use cases identified; standards for additional API functions progressively launched thereafter could be continuously maintained.



It is important for local banking industry participants to develop and maintain detailed API technical standards. A technical standardisation document covering the areas below could be prepared (Figure 22).

In line with the progressive implementation approach described in Section 5.1, the initial release of technical standards is intended to facilitate data sharing within a limited range of API functions, with banks and TSPs having the flexibility to define detailed data requirements. These initial standards will be continuously developed, reviewed and updated over time, with reference to other jurisdictions, to ensure that they remain in line with global trends and the latest industry practices as well as business needs.

Figure 22: Summary of API standards for banking Open API implementation

Technical standards	Technical design guidelines to standardise a banking Open API development approach for banks and TSPs covering development principles, API architecture, taxonomy, API security, and conventions for data sharing.
Customer experience standards	Customer experience guidelines that describe the principles, user journey, and user interface design, to enable simple, informed and secure data sharing for customers.
Customer authentication standards	Technical development guidelines covering API integration, endpoints and specifications to enable banks and TSPs to manage customer consent securely and efficiently.
Data standards	Data specifications guidelines for API functions, to enable banks and TSPs to share customer data in standardised data fields and formats.
Information security standards	Information security guidelines consisting of security measures for banks and TSPs, to ensure the confidentiality and integrity of customer data shared through banking Open APIs
Operation standards	Support process guidelines to facilitate banking Open API implementation by banks and TSPs covering API availability, performance, testing, change, incident management and business continuity planning.

5.3 Refinements to the Common Baseline

An analysis of practices in relevant international jurisdictions suggests that centralised TSP governance will only be desirable when there are relevant legal mechanisms in place. It is nevertheless recommended to continue with the bilateral approach of the Common Baseline for implementing Phases III and IV of banking Open API in the near term.

Industry participants are aware of the benefits brought by the Common Baseline. In the industry survey, approximately 70% of bank respondents said that they found the baseline useful for onboarding and monitoring TSPs. However, there is a need to refine the Common Baseline as a result of Phases III and IV to ensure that comprehensive risk mitigation measures are defined. These risk mitigation measures will need to address the increased risks in Phases III and IV, including fraud, money laundering risks and data privacy in customer data access and transaction processing. The survey respondents also indicated that they anticipate improved documentation to facilitate decision-making in the due diligence process.

In summary, refining the Common Baseline is recommended so that banks can address the increased risks associated with Phase III and Phase IV implementation. Based on common international practices, a number of key areas need to be considered when refining the Common Baseline, such as TSP governance, information security, authentication and consent management. These areas are outlined in Figure 23 below.

The banking industry in Hong Kong could work closely together to revise the Common Baseline with reference to these key considerations and the essential practices outlined in Section 4.

During the development of the Common Baseline for Phases III and IV, it will also be important to strike a balance between mitigating risks and facilitating entry for TSPs wishing to participate in the banking Open API ecosystem. Refinements to the Common Baseline enable banks to better assess TSPs during onboarding and ensure that the necessary protections are included in their respective bilateral agreements, ultimately increasing confidence amongst banking Open API participants.

Figure 23: Summary of key refinement areas for the Phase II Common Baseline

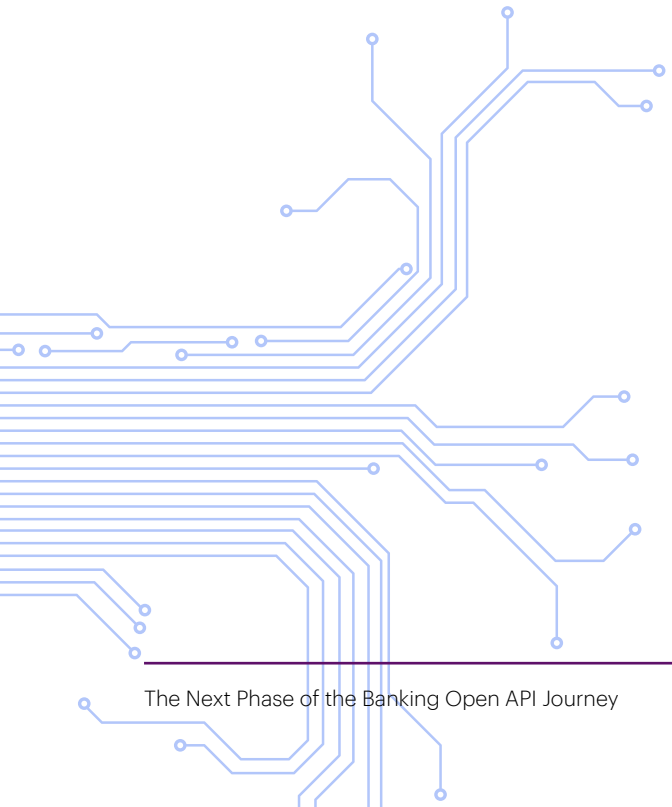
TSP governance and general risk management policies and procedures	• The industry may consider requiring TSPs to demonstrate that they have in place specific policies and procedures relevant to the risks associated with their business, if necessary, taking into account international best practices (e.g. a risk management plan to mitigate money laundering risks for TSPs offering banking Open API transaction services).
Technology risk management and cybersecurity	• The industry may consider requiring TSPs to demonstrate that they have in place policies and procedures that adhere to the security measures of the industry's banking Open API Standards, if necessary (e.g. a security incident response plan). • The industry may consider requiring TSPs to demonstrate that they have in place adequate security controls for personnel with access to sensitive customer data, if necessary, taking into account international best practices (e.g. background checks, information security training, etc.).
Data protection	• The industry may consider requiring TSPs to demonstrate that they have in place appropriate authentication methods (e.g. two-factor authentication) to protect the identity of customers against unauthorised access when using their banking Open API services, if necessary. • The industry may consider requiring TSPs to demonstrate that they have in place consent management capabilities (e.g. for obtaining and withdrawing consent) to protect customers against the sharing of data without their explicit consent when using banking Open API services.
Customer care and business practices	• Regarding complaint management mechanisms, the industry may consider developing further worked examples and/or principles (e.g. relating to the scope of complaint handling by TSPs, the channels by which customers can submit complaints, time limits for acknowledging, investigating and responding to complaints, the accessibility of TSPs' complaint handling procedures to users, etc.) • Regarding the definition of clear liability and compensation arrangements and dispute resolution procedures, the industry may consider developing further worked examples and/or principles that take into account international best practices.

5.4 Other protection measures

In formulating measures for Phases III and IV, including measures for consent management, it is recommended that the banking industry consults relevant statutory bodies, including the Office of the Privacy Commissioner for Personal Data, to ensure that any proposed measures comply with the relevant ordinances or guidelines, including the PDPO. The following customer consent and education measures are proposed for consideration to foster customer trust:

Consent management

It is important to set out common standards for both banks and TSPs regarding consent management. They ensure that information is only shared with the customer's permission, and that the customer is always in control of who can access their data, how it is being accessed, and how long it is being accessed (i.e. the customer should have the ability to revoke consent at any time). Key risk management and customer protection elements could be incorporated into the design of the consent management journey for this purpose. Implementation details will be captured in the API technical standards to be developed with industry participation as described in Section 5.2 of this report, with the guiding principles for consent outlined below according to international practice.



Explicit and clear consent

When obtaining customer consents for account information and transaction purposes, banks and TSPs should provide clear, sufficient and transparent information to aid customers in making informed data access and permission decisions. There should be minimum requirements regarding the information to be displayed in the consent form, including a description of the data to be collected, the purpose and duration for which it will be used, and the provision of explicit agreement to the consent.

Authentication and authorisation

The bank should perform customer identity authentication when redirecting a customer and obtaining their consent. As a key element of data protection, this step verifies the identity of the customer before sensitive data is shared. It also potentially reduces the risk of fraud through unauthorised access. Only upon successful authentication and consent approval should banks authorise TSPs to access the customer data.

Ongoing consent management

To ensure that customers are always in control of their data, banks and TSPs should provide customers with the ability to view, modify and withdraw their consent using easily accessible channels on consent management dashboards. These dashboards should be present on both the bank's and the TSP's platforms. For example, customers should be able to view a list of accounts that they have granted TSP access to on their banking application, and be able to modify or revoke their consent at any time. Banks should also ensure that no further account information from the customer is shared after consent is either revoked or has expired.

Customer education

To foster public participation in banking Open APIs, ecosystem participants including banks, TSPs, regulator and industry alliances could collaboratively drive customer education initiatives. These initiatives will help customers better understand what Open APIs are, and what measures have been put in place to protect their data.

Customers can be made more confident about adopting Open API-enabled products and services in the following ways:

Education by banks and TSPs

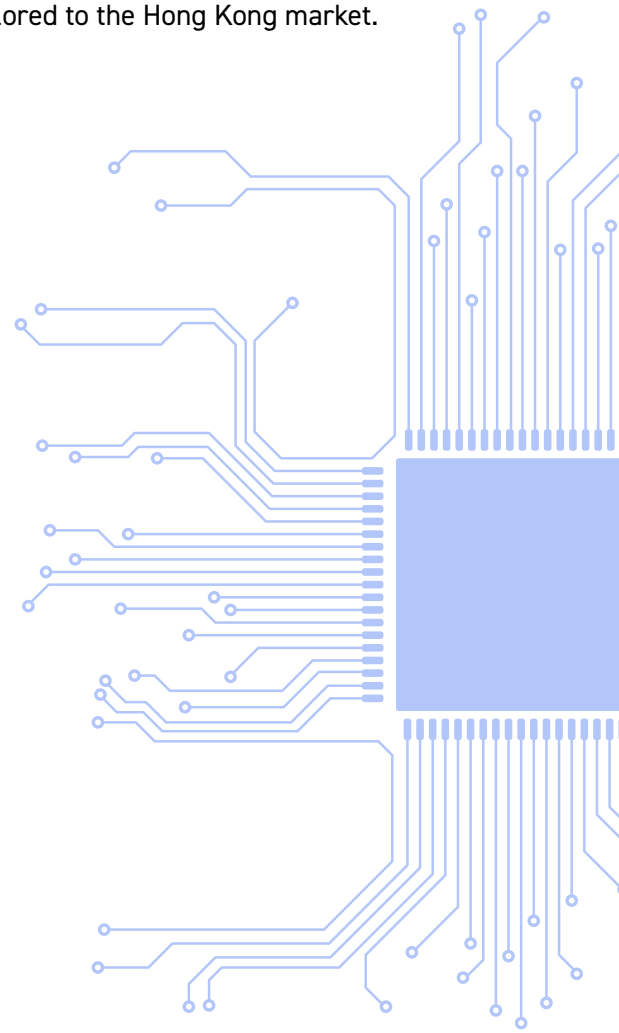
Devise customer education programmes to educate customers on the safe use of Open APIs, which could include, among other things:

- Alerting customers of third-party websites, apps or similar scams purporting to be operated by banks' partnering TSPs or claiming to be partnering with banks when they are not.
- Educating customers to refer to the central register on the Data Studio of the Hong Kong Science and Technology Parks Corporation or banks' websites for the list of partnering TSPs (to distinguish which TSPs are partnering with banks and which are not), and their relevant partnering products and services.
- Promoting awareness of the consent management process and of complaint handling procedures.

Banks and TSPs may consider sending communications containing the above educational messages to their customers, and also promote awareness about their consent management dashboards, consent withdrawal process and complaint handling procedures. In these communications, banks and TSPs can also inform customers of the new Open API offerings and their associated benefits subject to the availability of relevant consents provided by customers.^

Education by other ecosystem participants

Other ecosystem participants, such as industry alliances and members of the technology community, could proactively promote the safe use of banking Open APIs by, for example, gathering feedback on customer receptiveness, and developing communications to increase customer awareness of data protection. Apart from educating customers, these measures can also help banks and TSPs adjust their banking Open API strategy and develop appropriate offerings tailored to the Hong Kong market.



^ All such communications should only be sent to customers who have given their consent for any direct marketing activities, as stipulated in the Personal Data (Privacy) Ordinance.

Conclusion

Our industry consultation and the current use case adoption rates indicate that the implementation of banking Open APIs in Hong Kong has been successful to date. As the industry moves to implement Phases III and IV, a progressive implementation approach is recommended. The progressive implementation model will allow the highest value solutions to be deployed in the market in a sequential, stable and sustainable manner.

The importance of technical standardisation is also recognised by the banking industry. Having common Open API technical standards brings a wide range of benefits in terms of enhanced security management, faster rollout of new products and services, and lower implementation costs. This study also shows that local industry participants are highly receptive to developing and adopting a set of API technical standards for Phases III and IV.

A market-driven bilateral Common Baseline approach for Phases III and IV is recommended, given its successful implementation in Phases I and II. As Phases III and IV cover sensitive data including customer account information, the industry may consider developing further worked examples and/or principles (if necessary) on the scope of the Common Baseline around risk management, including guidance on consent management, liability and dispute handling.

Whilst a bilateral Common Baseline approach is the most appropriate TSP governance arrangement for implementing Phases III and IV for the time being, it will also be desirable to assess other governance models in future in order to keep pace with global developments and further maximise the benefits of banking Open APIs.

Finally, ongoing customer education as well as the building of customer trust in banking Open APIs are important if use cases are to be successfully implemented. This is a shared responsibility of all ecosystem partners.

Acknowledgements

This report was made possible by the active participation of the following participants in the industry consultation of this study.

No.	Organisation
1	2GoTrade Limited
2	Airstar Bank Limited
3	Alibaba Group
4	Amazon Web Services Hong Kong Limited
5	Ant Bank (Hong Kong) Limited
6	Bank of China (Hong Kong) Limited
7	Bank of Communications (Hong Kong) Limited
8	BCT Group
9	beNovelty Limited
10	Bicai365
11	Cathay Pacific Airways Limited
12	Centaline Mortgage Broker Limited
13	China CITIC Bank International Limited
14	China Construction Bank (Asia) Corporation Limited
15	Chiyu Banking Corporation Limited
16	Chong Hing Bank Limited
17	Citibank (Hong Kong) Limited
18	CMB Wing Lung Bank Limited
19	Dah Sing Bank, Limited
20	DBS Bank (Hong Kong) Limited
21	ET Net Limited
22	FiberAPI Technologies Limited
23	HKT Financial Services
24	Fubon Bank (Hong Kong) Limited
25	Fusion Bank Limited
26	Gini (More Champ Limited)
27	Gobear Hong Kong Limited
28	Google Hong Kong Limited
29	Hang Seng Bank, Limited
30	Hong Kong Broadband Network Limited
31	Hong Kong Television Network Limited
32	Industrial and Commercial Bank of China (Asia) Limited
33	Joint Electronic Teller Services Limited
34	Key Points Exchange Limited
35	Livi Bank Limited
36	Microsoft Hong Kong Limited
37	MoneyHero Global Limited
38	Mox Bank Limited
39	mReferral Corporation (HK) Limited
40	Nanyang Commercial Bank, Limited
41	New World Development Company Limited
42	NOVA Business Services Limited
43	OCBC Wing Hang Bank Limited
44	Octopus Cards Limited
45	Openrice Limited
46	Pecutus Technologies Limited
47	Ping An OneConnect Bank (Hong Kong) Limited
48	Planto Limited
49	Public Bank (Hong Kong) Limited
50	QFPay Haojin Fintech Limited
51	Shanghai Commercial Bank Limited
52	SIMNECTZ Technology Services Limited
53	SmarTone Mobile Communications Limited
54	Standard Chartered Bank (Hong Kong) Limited
55	SuperChoice Services Pty Limited
56	The Bank of East Asia, Limited
57	The FinTech Association of Hong Kong
58	The Hong Kong Association of Banks
59	The Hong Kong Federation of Insurers
60	The Hongkong and Shanghai Banking Corporation Limited
61	TransferWise Singapore PTE Limited
62	Visa Inc. Hong Kong & Macau
63	WeChat Pay Hong Kong Limited
64	WeLab Bank Limited
65	ZA Bank Limited

Appendix

8.1 Overview of project approach

To bring this study to life, the project team adopted a research-led approach involving various consultations with industry participants in Hong Kong. We then evaluated the best practices in Open API development from select leading international jurisdictions and analysed their implementation practices on Phase III and IV development. Finally, we assessed viable Open API use cases, identified potential gaps and proposed measures for the secure and efficient implementation of banking Open API in the region.

Figure 24: Detailed project approach

Approach	Description
Industry Questionnaire (September 2020 – October 2020	Solicited preliminary responses from industry participants including retail banks, virtual banks and TSPs (fintechs and participants from non-banking industries such as telecommunications, transportation, insurance, payments or technology providers) on their views on the current banking Open API adoption status, potential implementation measures and viable use cases for Phases III and IV.
Industry Interviews and Focus Groups (October 2020 – November 2020)	Conducted interviews and focus groups with end retail and SME banking customers, retail banks and TSPs; performed a deep dive on questionnaire responses and collected respondents' insights.
International Study	Evaluated the global development status and direction of Open Banking initiatives practised in select international jurisdictions, to serve as a key reference for proposed implementation measures for Phases III and IV.
Essential Practice Analysis	Analysed the essential practices for launching Phases III and IV based on common practices in leading international jurisdictions and with respect to risk management, protection mechanism, customer proposition design, TSP and banking capabilities and business and finance models.
Viable Use Case Assessment	Performed viable use case analysis for Phases III and IV and evaluated these according to industry receptiveness, business and technical feasibility, risk and international adoption considerations.
Gap Identification & Measure Design	Identified the key challenges for implementing Phases III and IV, analysed the common implementation measures of international jurisdictions and proposed measures for Phase III and IV development while addressing key risks and customer protection concerns.

8.2 Industry consultation details

As part of the approach taken, the project team conducted several industry consultations with banks and potential third-party service providers from Hong Kong between September and November 2020.

Two sets of survey questionnaires were distributed to bank and TSP participants respectively. Overall, we received responses from 59 participants, including 20 banks, 8 virtual banks and 31 TSPs.

The HKMA distributed the questionnaire for the 28 bank and virtual bank respondents, receiving a 100% response rate. For the targeted potential TSPs, questionnaire distribution was performed by members of the FinTech Association of Hong Kong, Hong Kong Cyberport, Hong Kong Science Park, and business partners from Joint Electronic Teller Services Limited (Jetco).

53 banks and potential TSPs also took part in industry interviews conducted from October to November 2020.

8.3 About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialised skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centres. Our 537,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

8.4 List of figures

8.5 Sources

1 **Open API Phase II Common Baseline**, The Hong Kong Association of Banks (2019)

2 **Smart Banking**, HKMA

3 **Data Studio of the Hong Kong Science and Technology Parks Corporation**

4 **The Time is Now**, Accenture (2019)

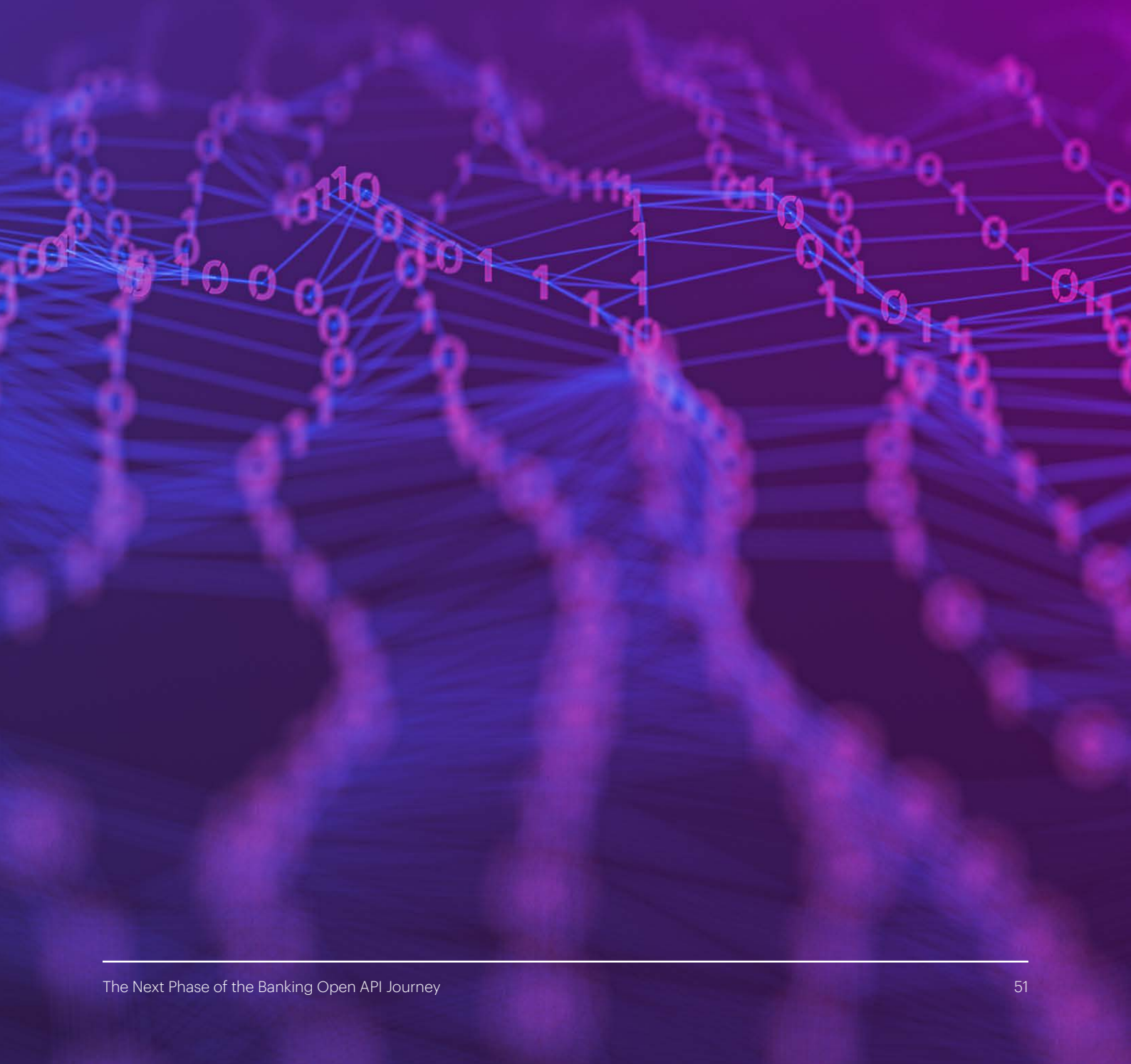
5 **Opening up Commercial Banking – The Brave New World of Open Banking in APAC**, Accenture (2018)

6 **How fintech ideas can solve big credit woes of small companies**, Hong Kong Applied Science and Technology Research Institute (July 2020)

7 **OAuth 2.0**

8 **OpenID Connect**

9 **Adapting to survive: UK's small businesses leverage open banking as part of their COVID-19 crisis recovery**, Open Banking Implementation Entity (December 2020)



Legal Notice

This report is prepared by Accenture under the instructions of the HKMA. All intellectual property rights in or associated with this report remain vested in the HKMA. This report and its contents are not intended as legal, regulatory, financial, investment, business, or tax advice, and should not be acted on as such. Whilst care and attention has been exercised in the preparation of this report, the HKMA and Accenture do not accept responsibility for any inaccuracy or error in, or any inaction or action taken in reliance on, the information contained or referenced in this report. This report is provided as is without representation or warranty of any kind. All representations or warranties whether express or implied by statute, law or otherwise are hereby disclaimed.