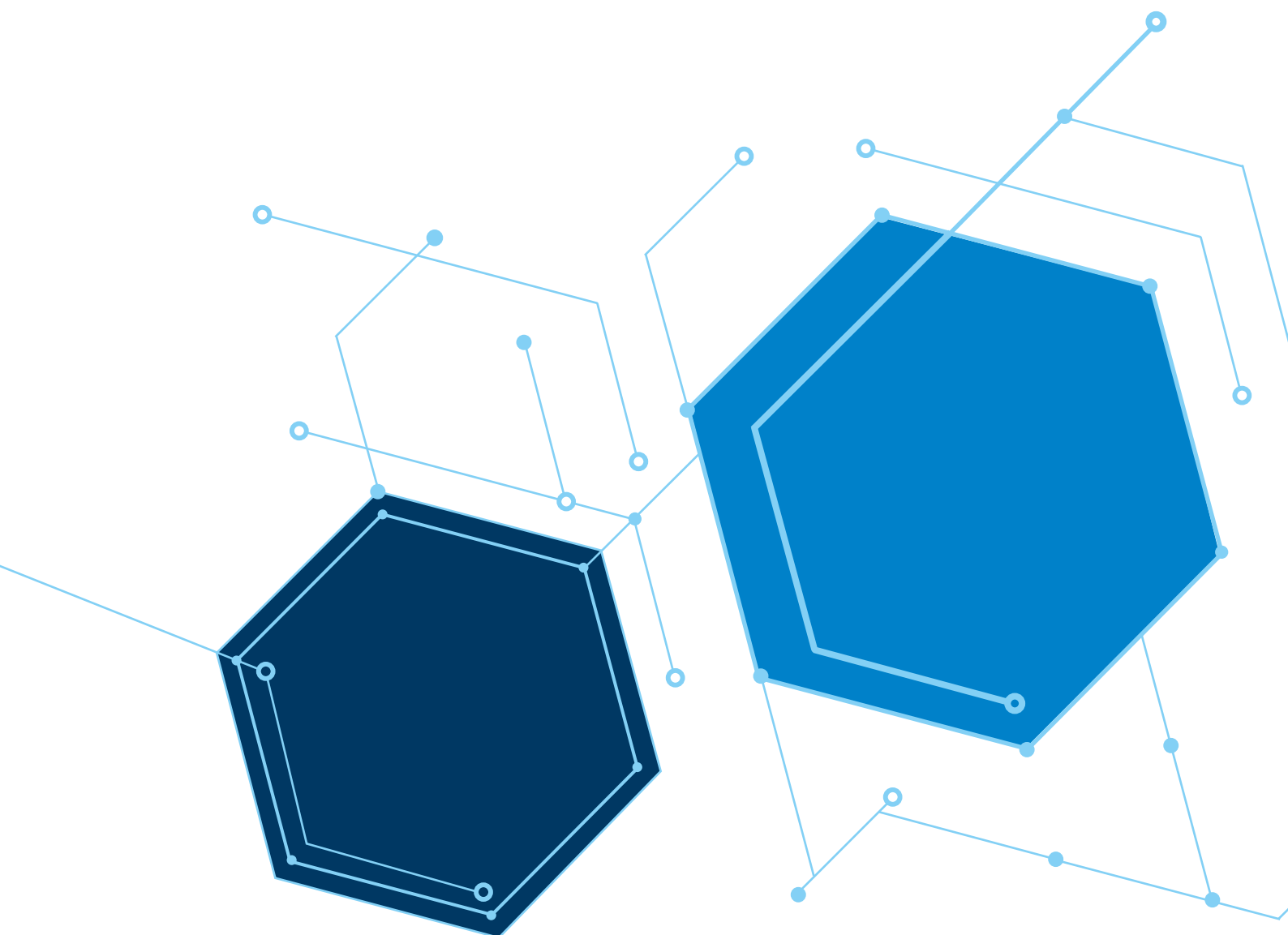


Open banking: A shared opportunity

A joint publication by Microsoft, Linklaters and Accenture



Contents

Foreword	3
Executive summary	4
1. Open banking: not just a trend	6
2. Uptake in Asia: revolution and evolution	8
3. Market drivers: technology, demand and competition	10
Data-centric technology advances	10
Changes in customer expectations	11
Competition and disruption	13
4. Challenges and opportunities for incumbents	14
Digitization	14
Cultural change	16
Customer trust: privacy and security	16
Regulatory compliance	17
New partnerships and collaborations	18
The value proposition	19
5. The regulatory perspective: broad support, diverse approaches	20
Diverse regulatory approaches: mandatory, supportive and neutral jurisdictions	20
Mandatory jurisdictions	20
Supportive jurisdictions	24
Neutral jurisdictions	26
Implications of different regulatory approaches	27
Regulatory body	27
Pace	28
Data types	28
Reciprocity	28
Standardization	29
Interrelation with other regulatory requirements	30
Banking secrecy and privacy/data protection	30
AML/CFT	31
Technology risk management and cybersecurity	31
Liability	32
Lack of harmonization of laws	34
Need for engagement by regulators	35
6. Looking forward	36
Perspectives on the future of open banking in Asia	36
Recommendations for industry and regulators	38
Interviewees	39

Foreword

Digital transformation is an imperative for businesses in today's economy. As Microsoft CEO Satya Nadella has said, "Each one of us in our organizations, whether it's public sector or private sector, will have to build our own digital capability. Because now every company is a software company, every company is a digital organization." Microsoft is dedicated to supporting its customers to reimagine the client experience, empower employees, optimize operations, and develop new products as they digitally transform.

Data has become one of the most valuable assets in this new era, the so-called Fourth Industrial Revolution. People have said "data is the new oil." But it is different from oil in a crucial way:

“Data, as economists put it, is 'non-rivalrous.' When a factory is powered by a barrel of oil, that barrel is not available to any other factory. But data can be used again and again, and dozens of organizations can draw insights and learning from the same data without detracting from its utility. The key is to ensure that data can be shared and used by multiple participants.”

Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (2019), p.275.

Open banking, which is based on data sharing, is poised to be the next wave of digital transformation in the financial sector.

Open banking has momentum because it has an extra push from regulators, who generally support it and in some countries even mandate it. In fact, one might say regulators are ahead of the industry in this regard in certain jurisdictions. Because of this regulator support, open banking is unlikely to be a short-lived trend. To remain competitive, incumbent financial institutions will need to embrace the opportunity presented by open banking. And given the jumpstart that open banking has received from regulators, the time to do so is now.

For open banking to take hold, incumbent financial institutions need to see the value for their businesses, and not feel that they are taking on substantial additional risk or compliance burden. Incumbents and new entrants must collaborate. Customers must feel assured that their data is secure and is being shared appropriately for their benefit.

In this paper, co-authored with Linklaters and Accenture, we explore the various drivers behind open banking in Asia and the issues financial institutions and regulators will have to address to ensure that all participants — financial institutions, third party providers, and consumers alike — can reap the benefits of open banking. Finally, we offer recommendations for the industry and regulators towards increased successful adoption of open banking. This paper includes the insights and perspectives of over a dozen interviewees representing different parts of the open banking ecosystem, including incumbent financial institutions, fintechs, technology companies, consultancies and others.

Each of our organizations is committed to partnering with our customers and clients in their digital transformation journeys. We hope you find this paper to be a useful resource, and we look forward to continuing the open banking conversation with you.

Joy Fuyuno

Asia Regional Senior Counsel, Financial Services Industry, Microsoft

Co-authors

Peiying Chua
Partner
Financial Regulation Group
Linklaters Singapore Pte. Ltd.

Peter Fairman
Associate
Financial Regulation Group
Linklaters Singapore Pte. Ltd.

Andrew McFarlane
Global Open Banking Lead
Accenture

Executive summary

Open banking is another important stage in the digital transformation of the financial services industry, yet it differs from previous stages in some fundamental ways. It is part of a wider movement to open up data to allow users greater flexibility and access, while also building new services and industries atop that data. Notably, open banking is increasingly supported by regulators across Asia and the rest of the world, either through mandatory regimes or overtly supportive environments. This means that open banking is unlikely to be a short-term trend, but rather an ongoing development that financial institutions will need to address — or, better, embrace.

At its core, open banking generally relies on application programming interfaces (APIs) — the bridge that makes it possible for two systems to talk to each other and share data — to give consumers the right and ability to port and share their financial data with third-party providers and other financial institutions. This will put banks around the world in competition (and cooperation) with a range of new players, from fintech startups to technology companies.

Nevertheless, as discussed further in Part 2, uptake of open banking in Asia today is somewhat limited. However, open banking is highly likely to continue to pick up pace, especially as open banking frameworks are implemented, for example as the Australian consumer data right regime takes effect over the coming months and years. Banks that act now are likely to have a first-mover advantage when open banking comes of age.

The momentum behind open banking is driven by several factors: technological advances, changes in market demand and customer expectations, competitive pressure and supportive regulations and government policies. These drivers are examined further in Parts 3 and 5. Digital transformation is disrupting most industries, including financial services, and data has proliferated and become more valuable. Advancements in API technology are making it easier and safer to share data, while developments in mobile and social technology are driving profound changes

in consumer expectations and behavior. These changes in consumer behavior are also contributing to the rise of new, more agile financial services providers, putting competitive pressure on incumbent banks.

Without doubt, the implementation of open banking does pose challenges — and opportunities — for incumbent banks, as discussed in Part 4. There is a clear need for digitization and cultural change, while remaining compliant with regulatory requirements. Banks will also need to address concerns about privacy and security to retain customer trust. Ultimately, they need to establish what the value proposition is for their business and form new partnerships and collaborations to realize their objectives. If incumbent banks can address these issues, then their experience with regulatory compliance and long-standing trust fostered with their customers will likely prove to be a competitive advantage over newcomers to the industry.

As mentioned above, open banking is set apart from other forms of digital transformation by the level of regulatory support behind it. In Asia, governments on the whole seem to support open banking, although regulatory approaches vary by jurisdiction, with some even mandating it. These differences are explored further in Part 5. There are pros and cons to the different regulatory approaches. While mandating open banking is certainly a strong statement of support, Accenture's Global Open Banking Lead Andrew McFarlane notes that, "market practice for geographies that have introduced formal regulations has been for incumbent banks to strongly focus on compliance first, and then move to a 'compete' mindset post regulatory compliance." It is also important that regulation does not front-run innovation, an ethos that is adopted by the Monetary Authority of Singapore. Regardless of the approach taken, regulators face similar issues, such as the scope of data to be shared, reciprocity, and standardization of data sets. While there is no single answer to these issues (and different industry players will have a diverse range of views on the optimal outcome), it is crucial for regulators to provide clarity, solicit feedback from industry, and avoid overly prescriptive or burdensome requirements.

Open banking can implicate other legal and regulatory issues, such as banking secrecy, privacy and data protection, anti-money laundering and countering the financing of terrorism, technology risk management and cybersecurity, and liability. This complexity is exacerbated by a lack of harmonization of laws and regulations around the region and even within a single jurisdiction. Regulators have a key role to play here to provide clarity and ensure regulatory compliance does not become so complex that it impedes adoption of open banking.

Although open banking is still in early stages in Asia, we are entering a new phase that is likely to bring more innovation and a wider range of products and services. At the end of this paper, we provide recommendations for regulators and financial institutions to pave the way for successful future adoption of open banking. Most importantly, to realize the shared opportunity of open banking, all participants and stakeholders will need to engage and share learnings and challenges as they embark on the journey together.



Open banking will put banks around the world in competition (and cooperation) with a range of new players, from fintech startups to technology companies.

1 Open banking: not just a trend

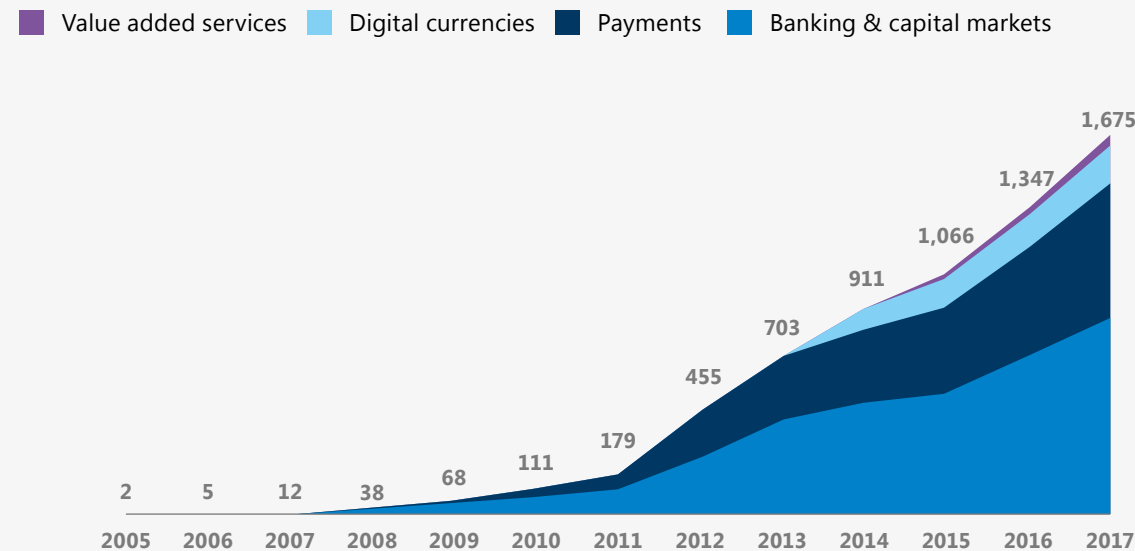
The advent of open banking marks another important stage in the digital transformation of the financial services industry.

However, it differs from previous stages in some fundamental ways. For one thing, it is part of a wider movement to open up data both to allow users greater flexibility and access to that data, and to build new services and industries atop it. For another, open banking is increasingly supported by regulators, either through mandatory regimes or supportive environments. The 2008 financial crisis prompted regulators to shake up the banking industry in part to drive innovation and protect consumers. This has led to policies supporting open banking in many markets, and in a few, such as the UK, EU, Australia, and Hong Kong, even mandating it.

Open banking will inevitably change the financial landscape, generating clear winners and clear losers. The winners will be the banks that embrace open banking and modernize their business models, opening up to third parties and not relying on their incumbent status. Those that focus on simply harvesting or protecting their current business, on the other hand, are likely to face rapidly increasing erosion.¹

At its core open banking relies on application programming interfaces (APIs) — the bridges that make it possible for two systems to talk to each other and share data — to improve existing banking services and allow new ones by unfettering the data from the institution that holds it. Accenture research shows their number globally has climbed rapidly in recent years.

Growth in Financial Services-related APIs



Source: The Time is Now, Accenture (2019). See: https://www.accenture.com/_acnmedia/pdf-99/accenter-time-is-now-open-banking-hong-kong.pdf

1 The Brave New World of Open Banking, Accenture (2018), at https://www.accenture.com/_acnmedia/pdf-77/accenter-brave-new-world-open-banking.pdf

Open banking goes beyond traditional banking to give consumers the right to control and port their financial data. This will put banks around the world in competition and cooperation with a range of new players, from fintech startups to technology companies.

What is open banking?

At its heart, open banking is about data. It is a process in which customers authorize their banks to share their financial data with third-party providers (TPPs), and also — for multi-banked customers — among banks.

Ecosystems can be built on this data through application programming interfaces (APIs) — the bridges that connect banks with TPPs — and bring together financial and non-financial services on new platforms.²

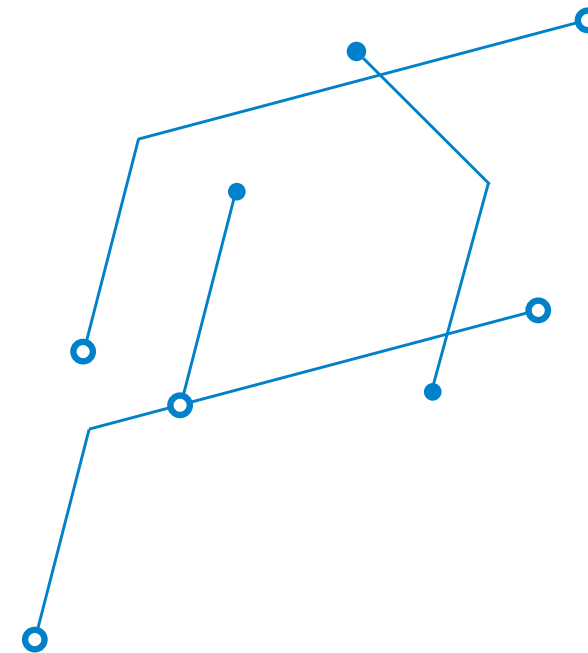
Open banking needs to be seen in the context of a broader revolution — as a specific variant of a broader trend: open data. As business models have evolved around the value of data — from individual browsing habits to traffic patterns of cities — so too has a movement arisen to unlock that data from the silos that control it. Governments and organizations are slowly opening up their data and making it available in an accessible format. Banking is at the cutting edge of a transformative age.

“We really prefer to talk about open data as compared to open banking because really that’s what we feel open banking is,” says Andrew McFarlane, Accenture’s Global Open Banking Lead. “It is the freedom of sharing the data between banks and registered third party providers [TPPs], to improve the customer journey as well as the preparation of tailored offers, products, and services for their customer bases. It’s also important to note that when we talk about customers and open banking, this is wholly applicable across all the customer segments — retail, small business and corporates.”

The regulatory push behind open banking, and broader open data initiatives, means it is unlikely to be a short-term trend, but is something that financial institutions will have to address — even embrace. Open banking offers the financial services industry an opportunity to transform itself, upgrade aging IT systems, forge new partnerships with players inside and outside the industry, and engage with regulators and other agencies in the process. Those that do so, early and effectively, will be rewarded with a head start in this new era of open banking.

In this paper, we will take a closer look at the market and regulatory drivers behind open banking, as well as the challenges, opportunities, and regulatory considerations for incumbent financial institutions and regulators as they embark on this journey. We conclude with perspectives on the outlook for open banking in Asia and recommendations for financial institutions and regulators to maximize the shared opportunity offered by open banking.

Open banking offers the financial services industry an opportunity to transform itself, upgrade aging IT systems, forge new partnerships with players inside and outside the industry, and engage with regulators and other agencies in the process. Those that do so, early and effectively, will be rewarded with a head start in this new era of open banking.



2 Open Banking in Canada: Opportunity Knocks, Accenture (2019), at https://www.accenture.com/_acnmedia/pdf-100/accenter-open-banking-in-canada-opportunity-knocks-pov.pdf

2 Uptake in Asia: revolution and evolution

Open banking is the latest in a wave of technology disruptions to sweep across industries, driven by changes in consumer behavior wrought by rising connectivity and smaller, cheaper computing.

The internet transformed media, while the smartphone has transformed the telecommunications industry, allowing new and existing players to offer compelling content and services in exchange for rich data on consumer behavior. Consumers in the developing world, where banking penetration is low and mobile phone penetration is high, started using mobile phones for money transfers as early as 2002. The global financial crisis of 2008 stimulated further innovation, with regulators opening the way, for example, to alternative financing in the U.S. and automated bill payments in Hong Kong.

In China, Alibaba, Taobao and other marketplaces created their own payment gateways organically, jumpstarting a revolution in mobile commerce that has largely bypassed the banking system. The rise of direct banking in China, where consumers could set up online accounts without visiting a branch, has helped foster an ecosystem where few consumers carry cash and, according to Ernst & Young, 78 percent of smartphone users have adopted mobile banking apps.³ For some, China's embrace of mobile finance is open banking in all but name. "If you define open banking as the ability for third parties to do banking transactions on consumers' behalf, arguably China has that already," says Jochen Nimtschek, Vice President, Digital and Emerging Partnerships at Mastercard. "Consumer tech platforms such as Alibaba connect to the banks and facilitate transactions for consumers and businesses that go beyond financial services, e.g., government services, healthcare, transport among them."

Elsewhere in Asia it's still early days, but some banks are forging ahead. DBS Bank in Singapore built its Developers API hub at the end of 2017 and has published over 155 APIs in 20 categories, onboarding more than 50 companies

to develop consumer solutions.⁴ Standard Chartered Bank's aXess portal features over 100 APIs spanning both corporate and retail use cases, with the aim of driving more connectivity and partnerships between developers, corporates and fintechs, to co-create better client products and services. Developers are invited to register to test their APIs in a sandbox and be instantly onboarded to the test environment. In Hong Kong, Standard Chartered launched the first phase of Open APIs for Retail and Wealth Management, which included Product Information APIs for Retail and Wealth, APIs to provide Branch and ATM listings and FX Rates APIs for retail clients.

Other banks in Asia are tapping into promising niches in anticipation of broader disruption. According to Accenture's McFarlane, "we're seeing the best use cases here come from Asia where DBS Bank, for example, has established marketplaces to help customers with all aspects of owning and operating a car in Singapore. UOB, on the other hand, has become involved in the travel business by exposing already existing APIs with minimal investment." Today 42 financial institutions and 108 fintechs are participating in API Exchange (APIX), an online global fintech marketplace and sandbox platform for financial institutions created by the ASEAN Financial Innovation Network.⁵

While the UK is one of the early markets to adopt Open Banking, driven in part by the EU's second Payment Services Directive, Connie Leung, Senior Director, Asia Financial Services Business Lead at Microsoft, notes that, "Recently, we have seen many other challenger banks in the market which have adopted cloud and open APIs, for example, in Australia and all across the globe. Our latest customer example is Anglo-Gulf Trade Bank in Abu Dhabi, the first digital trade bank in market."⁶

Open banking will play out differently in Asia compared to Europe. There is no uniform regulation like the second Payment Services Directive in the EU (PSD2), so the regulatory environment will differ across markets. In

Open banking will play out differently in Asia compared to Europe.

³ "How China's open banking experiment is unfolding", at https://www.ey.com/en_gl/banking-capital-markets/how-chinas-open-banking-experiment-is-unfolding

⁴ The Time is Now, Accenture (2019). See https://www.accenture.com/_acnmedia/pdf-99/centre-time-is-now-open-banking-hong-kong.pdf

⁵ See <https://apixplatform.com/landing>

⁶ See <https://news.microsoft.com/en-xm/2019/07/31/anglo-gulf-trade-bank-partners-with-publicis-sapient-and-microsoft-to-launch-worlds-first-end-to-end-digital-trade-finance-bank/>

addition, "a key difference between Asia and Europe is that in Asia you have a handful of consumer tech platforms with large customer bases and clear ambitions or capabilities in financial services," says Mastercard's Nimtschek. "So the power balance between the banks and the TPPs is probably different in this region than it is in Europe. A PSD2-like trigger isn't really necessary to make them work together — that will happen organically, as we've already seen in parts of Asia."

Most early players have opted for low-hanging fruit. Accenture's McFarlane says so far it is aggregators — apps that pull together account balances and transaction details from multiple sources — that lead the market. A key part of open banking — indeed, the initial focus in some jurisdictions — has been product description data, with banks sharing details of the products they offer to enable customers to compare like with like, via the aggregator apps and services that draw on open banking APIs. "Accenture's view is that retail aggregation has very much become table stakes," says McFarlane. "You then take it a step further and you look at the analysis of the customer's spending and present interesting offers tailored specifically to their needs, like Monzo is doing."

Also capitalizing early on the open banking opportunity is Look Who's Charging, an Australian startup recently acquired by Experian, which provides background information on merchants to add detail to unrecognized bank transactions. European companies in the open banking space are also expanding into the region: Revolut has launched its app and card in Singapore, while TrueLayer, a developer platform which allows third parties such as fintech and retail companies to access bank APIs and consumer data, has raised US\$35 million in funding led by Chinese tech giant Tencent and Singaporean sovereign wealth fund Temasek to expand into Asia.

Open banking initiatives are not limited to the retail sector. It is with small- and medium-sized enterprises (SMEs) that fintechs see opportunities, especially in providing a better experience for those seeking trade finance, says Jon Scheele, an API strategy consultant. It is an area where banks sometimes fall short, because SMEs aren't big enough to merit relationship managers. Ludovic Blanquet, Global Head of Product Strategy at Finastra describes SMEs as "our focus as a company." Its FusionFabric.Cloud product, which runs on Microsoft Azure, taps into the rich functionality of banks' legacy cores and instead of rewriting it, channels it into new technology via APIs. "There are some critical access points in the value chain in that functional richness that we want to expose in an open API and the first to benefit are SMEs."

Banks are taking notice of fintechs leveraging APIs to target SMEs. IncomLend, a Singapore platform funded by two ex-BNP Paribas executives, allows SMEs to sell their invoices to third parties, getting cash on the spot in exchange for a discount. Now banks are coming to the platform, which

provides a new, cost-effective distribution channel for them over dealing with SMEs directly. In parallel, banks are actively launching integrated propositions for their SME customers and are looking at Business Financial Wellness. CIBC's Smartbanking for Business, for example, integrates with multiple accounting packages and key payroll providers.

For all the activity, some still feel open banking has yet to ignite. A survey of global banks by Capgemini concluded that "[o]pen [b]anking adoption levels remain low, with banks facing operational and cultural obstacles that hinder implementation and acceptance."⁷ "At the moment by and large open banking is a failure," says Finastra's Blanquet. "Everyone speaks about it but there's been no single really huge success." Despite the lack of any so-called killer app to date, the promise is evident, as many different players are entering the market with new and interesting offerings.



⁷ World Payments Report, Capgemini Research Institute (2019), at <https://www.capgemini.dk/globalassets/denmark/world-payments-report-wpr-2019.pdf>

3 Market drivers: technology, demand and competition

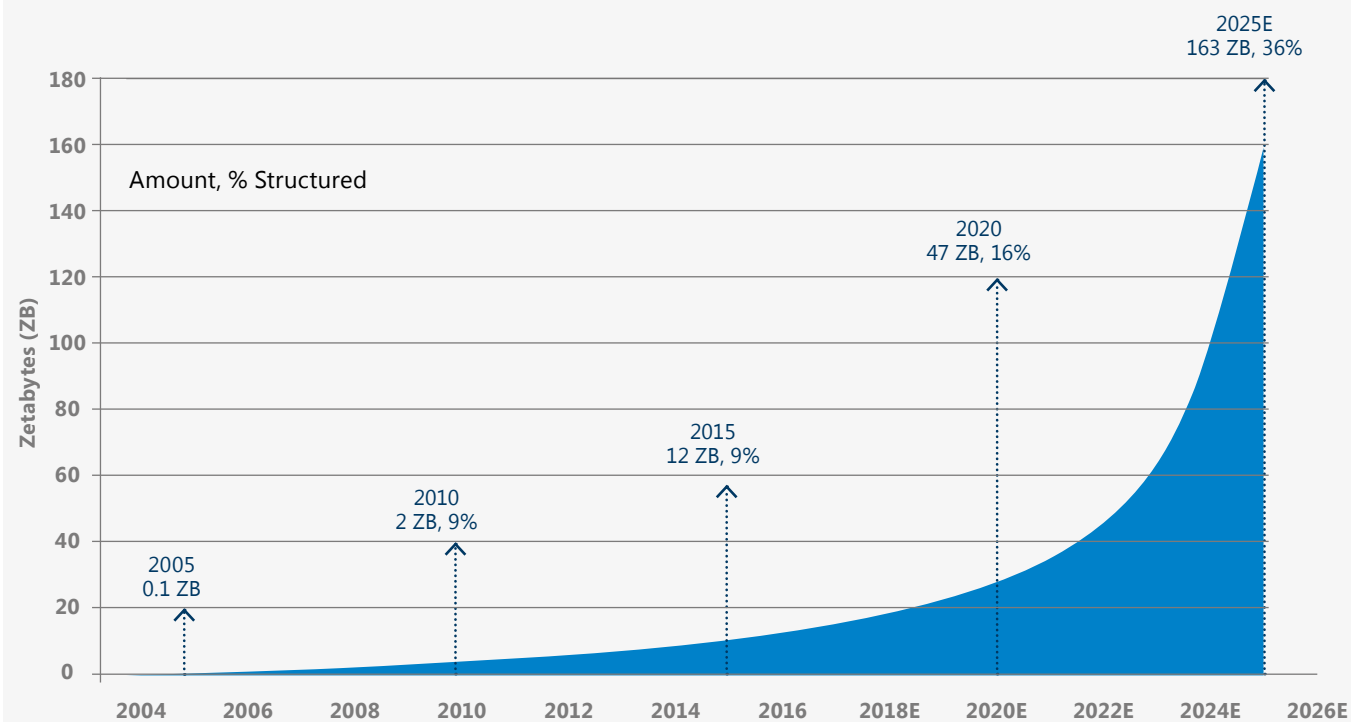
Even if uptake is somewhat limited today, open banking is likely to rapidly gain momentum rapidly. This is because there are several factors coming together to drive adoption of open banking: technological advances and increasing importance of data; changes in market demand and customer expectations; competitive pressure; and supportive regulations and policies. We will examine the first three in this section, and the last in Part 5.

Data-centric technology advances

Digital transformation — the application of technologies from big data and the cloud to artificial intelligence and robotics — is fundamentally changing all industries, including financial services. As Satya Nadella, CEO of Microsoft has said, “Each one of us in our organizations, whether it’s public sector or private sector, will have to build our own digital capability. Because now every company is a software company, every company is a digital organization.”

With the advent of cloud computing and mobile platforms, and the attendant proliferation of data, it has become increasingly important for businesses to find ways to capture the value of such data.

As the world’s information grows exponentially, so does its value



Source: Internet Trends 2018, Mary Meeker (Kleiner Perkins)

Secure APIs are the technology that underpins open banking. APIs provide a simple way to share and extract value from data, by allowing one computer and its data or services to talk to another without any complicated prior step. APIs as we know them today started with a revolution in Representational State Transfer (RESTful) APIs, a standard developed in 2000 to make it simple for any server to talk to another. It forced APIs to be simpler than their predecessors, and flattened the learning curve for developers trying to integrate software. This transformed the industry, allowing companies like eBay to publish simple APIs, which meant their market was no longer limited to people visiting their website. Instead, any site that could access their API could become a stall in eBay’s marketplace.

The development of RESTful APIs in turn made it simple for apps to access other services — a map on a mobile phone, for example, could be used by a taxi company. Once these economic needs were created, there was a need for payments: paying the map provider and being paid by one’s customer.

However, because offering a payment capability was traditionally the province of banks, payments options weren’t readily available. Consequently, different solutions were developed. According to Irving Wladawsky-Berger, a retired technologist from IBM, the relatively low penetration of credit cards and debit cards in China and other Asian countries meant that tech companies wanting to provide e-commerce and other services had to build their own cashless solutions, usually in the form of mobile wallets. “Such payment apps are now a way of life for over one billion users in Asia,” he wrote on his blog in June. “While linked to banks in the back end, payment app companies control the customer relationship and the vast amounts of data that give them insights into their customers’ preferences and behaviors.”⁸ Through services like Alipay and WeChat Pay, China has been able to bypass credit cards and debit cards, leapfrogging directly to mobile payments. It “exemplifies the radical shift that’s been taking place in the provision of financial services since the advent of the iPhone and App Store in 2007, a shift that goes well beyond China’s borders,” Wladawsky-Berger wrote. As Rohini Goyal, APAC Digital Strategist at Temenos, said after a recent visit to India, “It’s the culture and the need in the market that give way to innovation. For example, digital wallets are one of the biggest trends in India right now.”

At the same time, banking data was already being shared, albeit in a limited way: “Bank data has been used for a long time,” says James Varga, CEO and founder of DirectID. Companies like Kabbage, he points out, have for years used bank data to help SMEs get loans and financing. They did so using a technique called screen-scraping, where a third party will obtain log-in details from the user, then log in as the user (often without the knowledge of the bank) to capture, or scrape, data from the user’s account or banking portal.

For example, a customer will share their bank credentials with a third party like Kabbage, which will use those credentials to access their accounts (e.g., at Paypal, their bank(s) and QuickBooks, an accounting software) to determine their creditworthiness. Screen-scraping requires the user to entrust their credentials with a third party. While the practice within the financial industry is more limited and focused than the mass screen scraping of public data in other industries, there are still concerns about security and consumer protection, as the disclosure of user credentials for online banking accounts will often constitute a breach by the customer of its terms and conditions with the bank, leaving the customer without recourse for any data breaches that might occur.

Open banking, through pioneering use of APIs, represents the next stage in data sharing. Some governments, such as Canada’s, are considering measures to encourage open banking in order to eliminate the reliance on screen-scraping and shift to information sharing via APIs. The U.S. Treasury has also been supportive of moving away from screen-scraping and towards the use of APIs, although its view in July 2018 was that this should be left to the private sector.⁹ Finally, the EU’s PSD2 has the practical effect of banning screen scraping in most contexts.

Changes in customer expectations

The upsurge in mobile and social technologies means consumers are more powerful than ever. Their always-connected status and ability to find information in seconds puts them in control of their experience.

This trend has forced businesses of all sizes to rethink how they engage and connect — and financial services firms more than most, as Accenture’s recent survey of 47,000 financial services consumers in 28 markets shows. According to the 2019 Global Financial Services Consumer Study, of the consumers surveyed:¹⁰

- ✓ Half expect their financial providers to offer propositions addressing core needs — not only traditional financial services.
- ✓ Half indicate an interest in personalized financial advice from banks that is shaped by their personal circumstances.
- ✓ 80 percent are willing to share their data with their providers in return for better advice and more attractive deals.

The advent of open banking and open data makes creating ecosystems that can deliver such services easier than before, while the fact that customers can switch to competitors at the push of a few buttons makes delivering such ecosystems more urgent and important than ever.

⁸ Is the Digital Revolution at Last Shaking Up Banking?, at <https://blog.irvingwb.com/blog/2019/06/is-the-digital-revolution-atlast-shaking-up-banking.html>

⁹ A Financial System that Creates Economic Opportunities – Nonbank Financials, Fintech, and Innovation, U.S. Department of The Treasury (2018). See <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi...pdf>

¹⁰ Accenture Global Financial Services Consumer Study (2019), at https://www.accenture.com/_acnmedia/pdf-95/accenture-2019-global-financial-services-consumer-study.pdf

80%

of consumers are willing to share their data with financial services providers in return for better advice and more attractive deals

64%

of consumers in Asia are active fintech users, with India and China leading consumer adoption globally at 87%

When it comes to open banking, Asia is particularly promising. The EY Global FinTech Adoption Index 2019¹¹ shows that 64 percent of people in the region are active fintech users (in keeping with the global average), up from 16 percent in 2015, with India and China leading consumer adoption globally at 87 percent.

At the same time, as Accenture's survey shows, customers are now more willing than ever to share their data. "It matters to banks because there is a threat of being left behind should they take no action or really decide to do the bare minimum. We see a real risk of disintermediation and the threat of losing that customer stickiness that banks have worked so hard for years to build up," Accenture's McFarlane has said.¹²

The opportunity is not just for markets underserved by banks. Some services that banks consider to be core to

their business may be under threat. A July 2019 Finastra survey showed market dominance of banks in delivering corporate treasury services is under threat from non-bank market entrants. Its survey of 380 corporate treasurers from enterprises across Europe, the Middle East and Africa found that 70 percent believe a shift from bank to non-bank services will take place within their organizations over the next two to five years. Sixteen percent say that has already happened. The findings reveal strong demand for open banking-enabled services among corporate treasurers: 29 percent said it was a key opportunity for their business in 2019, citing benefits such as lower costs, cash visibility, and new services being made available from non-bank market participants. Some 83 percent of respondents said they would like to use dedicated corporate APIs provided by their bank to connect to third-party providers.¹³

11 Global FinTech Adoption Index, Ernst and Young (2019), at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf

12 Microsoft's "20-on-the-Go" Financial Services Industry podcast series.

13 Digital Disruption Comes to the Corporate Treasury, Finastra (2019), at https://www.finastra.com/sites/default/files/documents/2019/07/market-insights_digital-disruption-corporate-treasury.pdf

Competition and disruption

Few industries have escaped the impact of technological disruption, yet even before the word "fintech" entered common currency, regulators, rival industries and startups were looking to disrupt banking. Startup investment in Asia-Pacific fintechs has risen from US\$400 million in 2012 to US\$3.5 billion in 2015, according to an Accenture analysis of CB Insights data.¹⁴

On a global basis, both the number of fintech deals and the funding that fintechs attract have climbed year-on-year, if 2018's extraordinary US\$14 billion Ant Financial deal is stripped out. The first half of 2019 saw US\$22 billion invested, a rise of 28 percent on the previous period (excluding Ant Financial).¹⁵

Disruption is also occurring with the entry of so-called "neobanks," or digital banks. By July 2019, year-to-date funding of challenger banks had surpassed 2018's record of US\$2.3 billion, adding more than 30 million accounts, according to CB Insights.¹⁶

Regulators are welcoming the competition. In Australia three neobanks have been given licenses to become authorized deposit-taking institutions (ADIs) in the last year. Xinja and 86 400 opened their doors in September; Volt Bank has yet to launch. The receptiveness to these new players, in a market where the top four banks dominate, "evens the playing field," Temenos' Goyal says. "Hong Kong has given several virtual banks licenses because they realize unless they bring more competition into the market, the big incumbent banks won't change. So I believe it's a unique way that governments can drive the banks to embrace change. And every country will find their own way to reach the equilibrium," says Goyal. Indeed, the Monetary Authority of Singapore (MAS) has said it will be issuing up to five digital retail and wholesale bank licences, with the objective to "add diversity and help strengthen Singapore's banking system... with innovative business models and strong digital capabilities."¹⁷

All of these drivers — technological advances, evolving customer expectations, and the entry of new competitors — lead to the same imperative: incumbent financial institutions based on traditional models must transform and branch out into new areas such as open banking to succeed in today's financial services market.

Disruption is also occurring with the entry of so-called "neobanks," or digital banks. By July 2019, year-to-date funding of challenger banks had surpassed 2018's record of US\$2.3 billion, adding more than 30 million accounts, according to CB Insights.



14 Fintech Investment in Asia-Pacific set to at least quadruple in 2015, Accenture (2015), at https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_12/accenture-fintech-innovation-lab-asia-pacific.pdf

15 Global Fintech Fundraising Fell in First Half of 2019, with Decline in China Offsetting Gains in the US and Europe, Accenture Analysis Finds, Accenture (2019). See: <https://newsroom.accenture.com/news/global-fintech-fundraising-fell-in-first-half-of-2019-with-decline-in-china-offsetting-gains-in-the-us-and-europe-accenture-analysis-finds.html>

16 Global Fintech Report Q2 2019, CB Insights (2019). See https://www.cbinsights.com/reports/CB-Insights_Fintech-Report-Q2-2019.pdf

17 <https://www.mas.gov.sg/news/media-releases/2019/mas-to-issue-up-to-five-digital-bank-licences>

4

Challenges and opportunities for incumbents

Today it may seem, particularly for incumbent banks, that the path to open banking poses several challenges. These include the need for digitization and cultural change, the importance of securing customer trust, compliance with regulatory requirements, the need for new partnerships and collaboration, and, perhaps most fundamentally, understanding of the value proposition of open banking for their business. While these challenges are real, from a different perspective, they are also opportunities for incumbents to modernize their businesses and stake their claims in the new era of banking.

Digitization

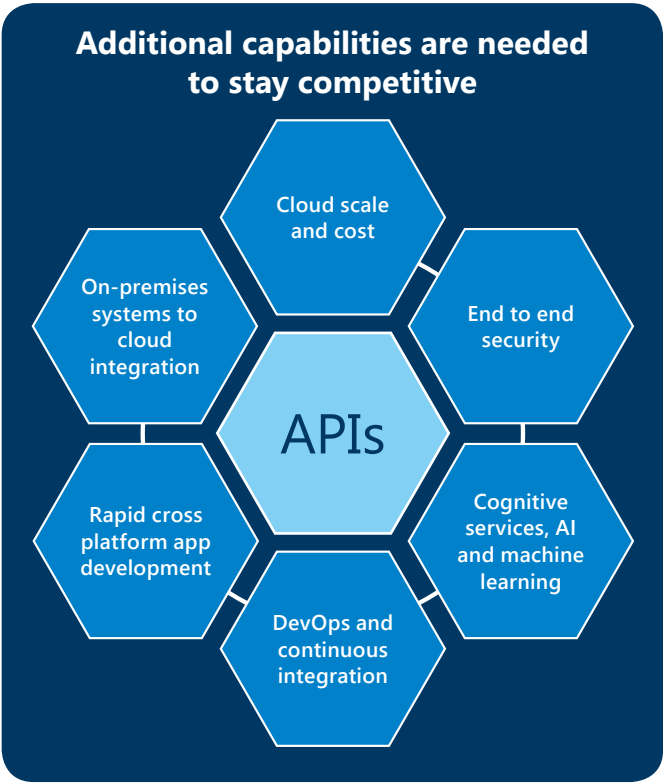
Banks will need to move up the curve with technology to partake in open banking. For many, it is a big leap from where they are today to being fully ready for open banking. A good approach, if an institution has not already done it, is to start by gradually replacing legacy infrastructure.

Any open banking strategy must be incorporated into a broader digitization process. Defining that, says Accenture’s McFarlane, requires ensuring it “aligns with your overall technical architecture for your institution, including your cloud and API strategies.”

A key challenge is that this is not simply about preparing for a stream of small fintech startups making a modest number of API calls. TPPs “are [typically] architected to scale rapidly and seamlessly — increasingly utilizing flexible, virtual computing from ‘cloud’ providers. These businesses have also achieved unprecedented levels of frequent interaction and growth of customers, particularly the mass market digital platforms.”¹⁸ That is why, according to the

Fintech Association of Hong Kong, “[o]pening an API from a traditionally architected bank to a modern digitally-scaled business (WeChat or Facebook Messenger for instance) could rapidly and suddenly increase the load on these ‘legacy’ systems, which without investment in scalable infrastructure would be unlikely to operate with the required robustness and resilience.” As Richard Peers, founder of Responsible Risk Ltd underscores: “For many people, their legacy technology and their core banking platform is a constraint, because it’s difficult to get the APIs onto that, get the data out of that, to handle the kind of volume that comes from a chatty set of fintechs requesting data. And that is definitely a barrier for people worrying about security and scalability and so forth.”

At the same time, this provides banks with an opportunity to modernize infrastructure, something that will be necessary for financial institutions to stay competitive.

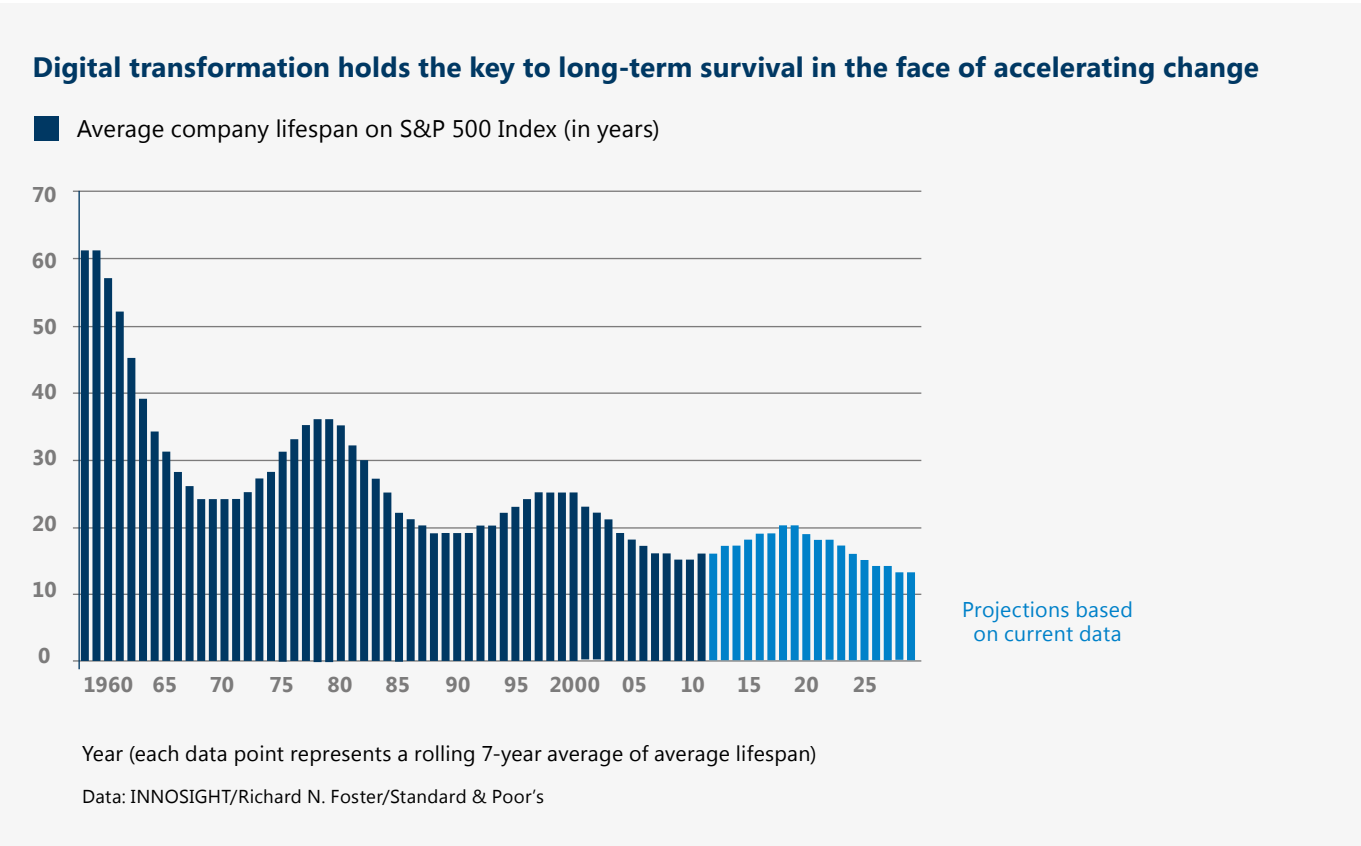


18 Consultation Paper on Open API Framework for the Hong Kong Banking Sector – Fintech Association of Hong Kong response, March 2018, at <https://ftahk.org/sites/default/files/inline-files/FTAHK-response-to-HKMA-Open-API-Framework-consultation-March-2018.pdf>

Microsoft’s Leung advises that financial institutions should focus on ensuring the customer experience is as good as possible and developing digital services quickly in response to demand. “Today it’s about the race of technology adoption and the better, faster and smarter way of adopting technology will win in this market... Smart is how you can re-imagine the customer experience — using data and AI to bring value to customers with personalized products and services — and do it in such a quick manner that you can launch an app or service in weeks. That’s the new benchmark for China and parts of Asia now. So you prioritize on your digitalization journey and start modernizing what you need to replace to bring agility to your business.”

Regardless of the approach, it cannot be done all at once. “A phased approach to providing APIs, as suggested by the Hong Kong Monetary Authority (HKMA), permits industry-led structuring and refinement of the commercial models over time.”¹⁹ Financial institutions can also test-run open banking strategies and products through pilots or sandboxes such as APIX in Southeast Asia.

This does not mean postponing moving forward, which Accenture’s McFarlane believes would be costly. “One thing for us is very clear... any banks that delay will definitely be outrun by hungrier competitors.”



19 Consultation Paper on Open API Framework for the Hong Kong Banking Sector – Fintech Association of Hong Kong response, March 2018, p. 6 (citation omitted), at <https://ftahk.org/sites/default/files/inline-files/FTAHK-response-to-HKMA-Open-API-Framework-consultation-March-2018.pdf>

Cultural change

Digital transformation requires cultural change. Building a relationship with the customer is more important than ever, as customers can switch suppliers as easily as tapping on an alternate application. Financial institutions need to acknowledge this or risk either their products becoming obsolete or being outmaneuvered by more agile and efficient competitors. With open banking, “unless you’re adding value for the end customer, it won’t stick,” says Temenos’ Goyal.

Where it used to be a risk to do something new, the risk in today’s hypercompetitive landscape is to not do something new or different. To generate new sources of revenue and stay relevant, companies are seeking to reimagine the customer journey and experience. As they reinvent how to connect and engage with their customers in new and exciting ways, they must also ensure their operational and organizational processes are likewise internally empowered to support and effect that change. Empowering employees drives optimized operations and processes, and in turn leads companies to transform their products and services.

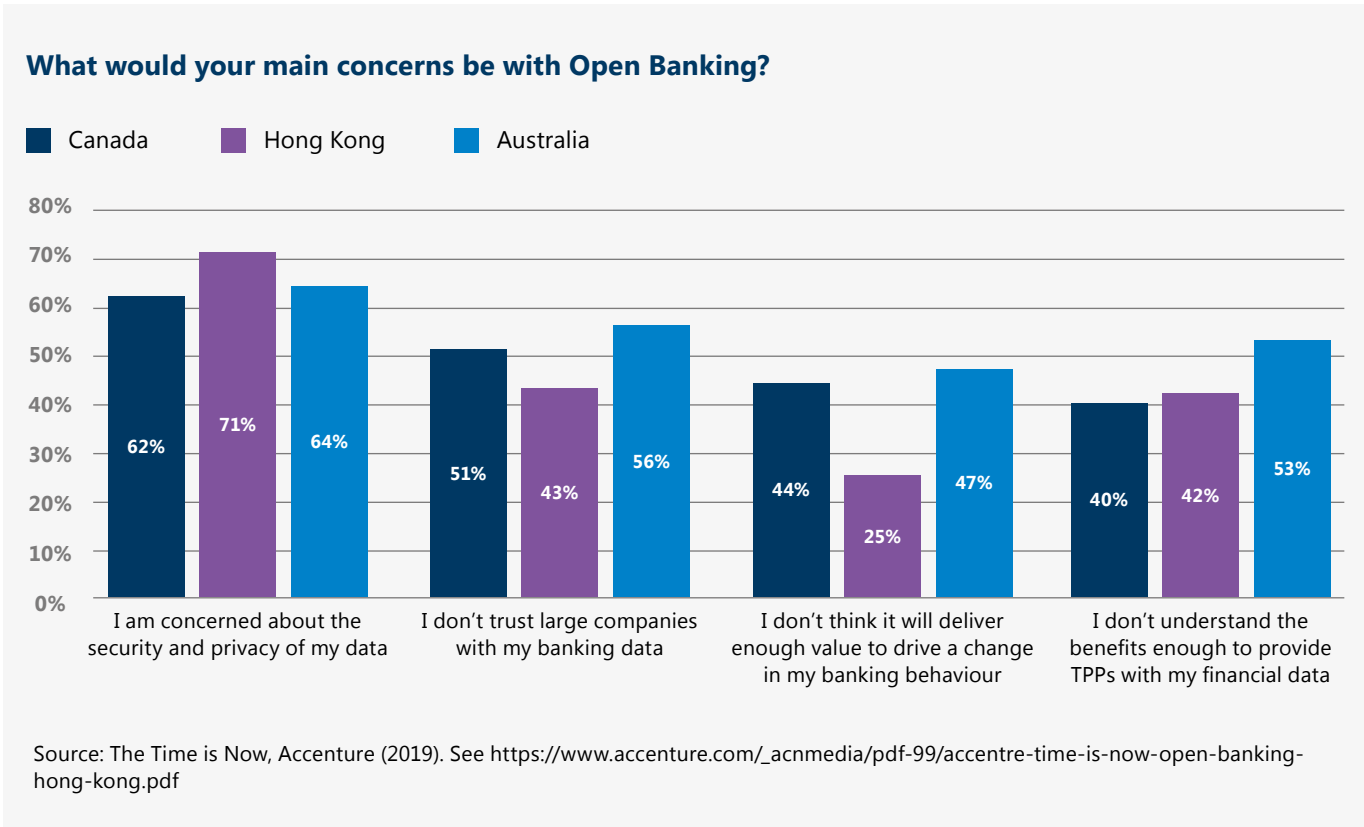
Leaders of digital change need a vision of how to transform their businesses. The combination of foresight and appetite for transformation of a business’ leadership team can influence this change. Microsoft’s Leung believes the change in mindset needs to happen throughout the organization, not just at the top or in the innovation team. “Technology

adoption is a mindset change rather than a technological one,” she says. “Everyone needs to change, and they need to think about how they can do better for their customers every day. This is not a technology question. This is actually a business question: what business problems are you trying to solve and what do you need to solve them?”

One approach to effecting cultural change is to establish cross-disciplinary teams focused on digital transformation. Microsoft’s Leung has seen how financial institution customers establish new virtual teams to effectively tackle the essential business challenges that an organization needs to resolve, including: what business and operations models need to change; how to address the core values of the organization and its customers; what services they want to provide; and what partners and technology are required. “Very quickly it becomes clear that all these changes lead to a cultural change,” she says, “and that’s top of mind for CEOs.”

Customer trust: privacy and security

While we have seen there is demand for the new types of services made possible through open banking, consumers are likely to have concerns about sharing their data. An Accenture global survey found security and privacy of data was the main concern of 71 percent of Hong Kong consumers surveyed, with Australians and Canadians not far behind. Other worries included a lack of trust of TPPs and a lack of understanding of the benefits of open banking.²⁰



20 The Time is Now, Accenture (2019). See: https://www.accenture.com/_acnmedia/pdf-99/accentre-time-is-now-open-banking-hong-kong.pdf

Customer trust is crucial to the success of open banking, and it is here that incumbent banks have a competitive advantage.

This means participants in the open banking ecosystem must ensure that privacy and security of data are addressed comprehensively. That is particularly true for incumbent banks, as their businesses rely on a foundation of customer trust.

Regulated incumbent financial institutions must already comply with stringent requirements on security and privacy, which actually puts them at an advantage over fintechs and unregulated entities. That is why incumbent financial institutions should focus on transparency — informing customers about the security and privacy measures they take. “There remains a lack of understanding from the general public on what it means to share their data in the context of open banking and there would be benefits in spending more to educate customers, including from public authorities,” says Sophie Lloret, Head of Regulatory Change, Technology & Innovation at Standard Chartered Bank. “It will mean different things, depending on different jurisdictions and how they are implementing open banking.”

Open banking initiatives are based on the informed and valid consent of the customer to share data, so service providers will need to be transparent in explaining the scope of consent to customers. That means ensuring the customer fully understands any consent forms, especially when it comes to providing their transaction history to third parties. Likewise, customers need to be educated about what to do if things go wrong. In Australia and the UK, the open banking regimes include the design and implementation of dashboards that customers can use to easily view, track and manage the consents they have provided. Tools like this can prove helpful in ensuring transparency and trust.

With respect to security, participants in the open banking ecosystem must ensure they are building on secure, scalable platforms. Cloud services provide the necessary scalability and allow open banking service providers to avail themselves of the huge investment cloud service providers put into cybersecurity, as well as security and privacy by design, on an ongoing basis. Participants in the open banking ecosystem should work with cloud service providers to understand the security of their offerings and be able to explain it to customers.

Customer trust is crucial to the success of open banking, and it is here that incumbent banks have a competitive advantage. A 2019 survey by Ernst & Young found that, after lack of awareness and understanding, trust is the second-most common reason why people opt for incumbents over fintechs.²¹ The survey found 59 percent of Hong Kong consumers would trust their own bank with their financial

data, far ahead of another bank (6 percent). International payment firms (15 percent) and local payment firms (12 percent) were second and third. The reason non-adopters choose to stay with incumbents, the survey concluded, is that “they trust them more than fintech challengers.”

Incumbents should not rest on their laurels, as their trust advantage could dissipate as new entrants become established players, or other recognizable names enter the fray. Mitesh Soni, Senior Director, Innovation and Fintech at Finastra, has said: “For the consumer, open banking is really a secure way to give regulated providers access to your personal financial data. Think of it as an end to the banks’ monopoly of customer data.”²²

Regulatory compliance

Financial services is known to be a heavily regulated industry, with compliance considerations making it difficult for financial institutions to move quickly. “As a heavily regulated industry, we need to comply with a robust set of requirements before we can open up (such as data protection, KYC, AML, operational resilience and even prudential requirements). Similarly, new entrants should be subject to proportionate and fair requirements (based on materiality) to ensure that innovation does not supplant competition,” Standard Chartered’s Lloret says.

That said, considering the existing open banking regulatory mandates (extending to third party providers and entities not typically regulated by financial services regulators), and the likelihood that other regulators will issue guidance around open banking, incumbent banks’ accountability and experience with regulatory compliance is likely to be an asset.

The regulatory support behind open banking has other benefits. For some, the regulatory approach validates their internal push for change, providing what DirectID’s Varga calls a comfort blanket, “where the risk-averse financial services [providers] don’t have the excuse anymore.” Microsoft’s Leung agrees. “When the regulators say that you need to do it or the regulators say that this is the direction, it gives [banks] a blessing. They don’t have to second guess whether they are doing the right thing or if they will get regulatory approval at the end of the day.” This makes selling open banking internally much easier. “Often it’s not just about the business case itself but it is what’s involved to get internal compliance and regulatory approval. [The regulator involvement in open banking] kind of makes that journey easy.”

21 Global Fintech Adoption Index 2019, Ernst and Young (2019). See https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf

22 Microsoft’s “20-on-the-Go” Financial Services Industry podcast series

New partnerships and collaborations

As different enterprises venture into the new world of open banking, new partnerships and collaborations will be essential. “The environment is more collaborative today because I think fintechs realize they can’t operate standalone,” says Microsoft’s Leung. “Fintechs need the banks as much as the banks need them.” Banks too are changing their mindset. “Banks are more open because they understand that for them to build in-house would take a lot more time. Banks are trying to find the proper balance between agility and the traditional approach of building solutions in-house. They are starting to assess what capabilities fintechs and start-ups have that they can bring in to accelerate the digital transformation journey. It’s a mix and match. And I see more of that approach.”

In September, for example, Deutsche Bank acquired a stake in German-based fintech Deposit Solutions, whose open banking technology allows banks across 18 countries to offer their customers products from third-party banks.²³ And last year, Australia’s WestPac partnered with Melbourne-based Assembly Payments — a rival to companies like Square, Stripe and Adyen — to launch a payments platform for its business clients.

Banks should be open to new partnerships, but should have a clear view of the total customer value proposition and which partner is best placed to deliver each component of that value proposition, says API consultant Scheele. He points to platform companies like Salesforce and Xero, which have core products and publish APIs for others to build modules and services with enhanced functionality. In Xero’s case, its core accounting system is the same globally, but local payroll or tax modules may be provided by a partner with better knowledge of local regulations. The partner’s extension increases the geographies in which Xero’s product can be distributed. A bank might start similarly with a core product, but as it learns from experience it might decide to create its own module that competes with its partner’s. This “channel conflict” is nothing new and arises wherever platforms emerge. The key for banks is to focus on what they can do well and better than (or before) anyone else.

Some banks — including HSBC, Commonwealth Bank of Australia and National Australia Bank (NAB) — are using innovation labs as a way to fast-track this process. Standard Chartered Bank’s innovation, fintech investments and ventures arm, SC Ventures, fulfills a similar role. “They are the eyes and ears of the markets to bring that external view but also to understand what exactly the bank needs and to bring in that capability,” says Microsoft’s Leung.



As different enterprises venture into the new world of open banking, new partnerships and collaborations will be essential. “The environment is more collaborative today because I think fintechs realize they can’t operate standalone,” says Microsoft’s Leung. “Fintechs need the banks as much as the banks need them.”

23 Deutsche Bank acquires a 5 percent stake in fintech Deposit Solutions, at https://www.db.com/newsroom_news/2019/deutsche-bank-acquires-a-5-percent-stake-in-fintech-deposit-solutions-en-11590.htm
24 Microsoft’s “20-on-the-Go” Financial Services Industry podcast series.

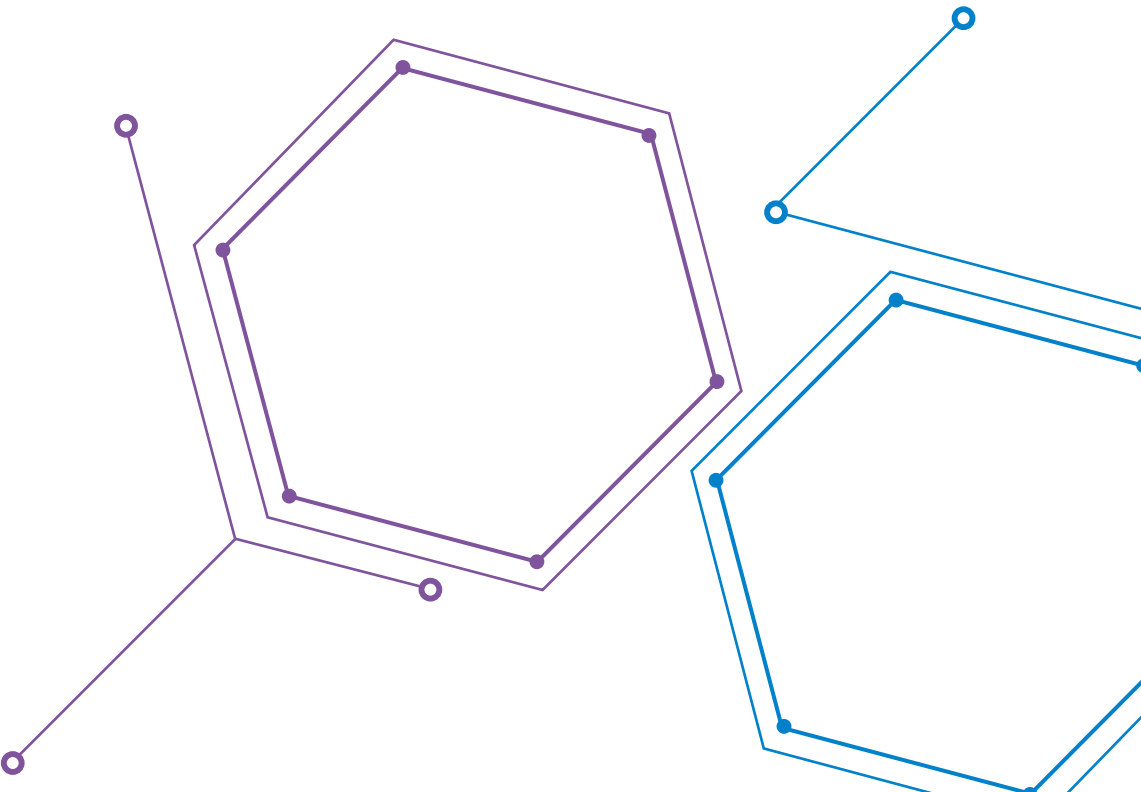
The value proposition

Ultimately, incumbent financial institutions will only realize the benefits of open banking when they fully understand the value to their business. Banks that recognize the value early, instead of viewing it as a necessary compliance exercise, will have a head start. It’s a question of working out what niche to fill and what the value proposition is, and building the partnerships necessary to achieve that goal.

With open banking likely here to stay, understanding how to capture value is vital. “PSD2 is a regulation and as the name suggests there is likely to be multiple releases of this regulation—PSD3, 4, 5,” says Finastra’s Soni. “So, getting in early and establishing a robust architecture means long term revenue opportunities on a recurring basis.”²⁴

Opportunities for incumbent banks to create value with open banking:

- ✓ Banks can become aggregators for consumers with multiple relationships
- ✓ Banks can boost customer acquisition and reduce attrition by becoming one-stop shops
- ✓ Crowdsourcing of new products will let banks meet the needs of a fragmented market
- ✓ Smaller banks can offer their customers access to a wider range of products
- ✓ Integration of products from incubator and accelerator programs will be easier
- ✓ Banks will be able to access external data sets for added consumer insight
- ✓ Banks can open up new revenue streams by selling access to their own data
- ✓ New revenue streams will arise from selling access to a bank’s core systems
- ✓ Banks can access data at the point of origination to improve risk analysis and inform credit decisions (e.g. in agriculture, banks could partner across the value chain with farmers to see their usage of pesticides, fuel, water etc. to anticipate drought and effect on yields, which would impact loan serviceability)
- ✓ In wealth management, many small pools of wealth are left unserved due to the high cost. Aggregators could provide efficient models in a B2B market for independent financial advisors to connect to these customers with low cost advice and improved returns





The regulatory perspective: broad support, diverse approaches

As discussed above, there are several drivers behind open banking. The market drivers — advances in technology, changes in customer expectations, and competitive pressure — are somewhat similar for any form of digital transformation. However, unlike other forms of digital transformation, for example blockchain or AI-driven developments, open banking has broad and explicit support of various regulators around the world, many of which have backed initiatives or made positive pronouncements about open banking, and in some cases even mandated it. The Open Bank Project, a Berlin-based open source API solution provider, says open banking has so far been adopted or is under discussion by regulators in more than 47 countries.²⁵

Open banking's appeal to regulators is simple: it supports their policy objectives. Regulators in the UK, EU and Australia are among those supporting open banking to boost competition in the financial services industry. Open APIs and data sharing are likely to level the playing field among incumbents and new industry players and encourage new entrants, which in turn benefits customers. For some regulators, as in Hong Kong, it is a way to increase national competitiveness by driving innovation. In other markets such as Nigeria, Mexico, and India, open banking is seen as driving financial inclusion, for example through payments innovation.

In Asia, the ASEAN Financial Innovation Network, established by the International Finance Corporation, MAS, and the ASEAN Bankers Association (ABA), with support from Japan, the Netherlands and the UK, is leading a supranational drive for connectivity and open APIs across the ASEAN region with the November 2018 launch of APIX, an online global fintech marketplace and sandbox platform for financial institutions. ABA Secretary General Paul Gwee Choon Guan described APIX as "vital to deepening financial inclusion in ASEAN markets."²⁶

Diverse regulatory approaches: mandatory, supportive and neutral jurisdictions

While on the whole governments seem to be behind open banking (and it does not appear that any explicitly opposes it), the regulatory approach varies by jurisdiction. The approaches can be classified as follows:

Mandatory jurisdictions — where open banking has been mandated by the regulator(s), including in phased deployments based on different categories of financial institutions, products or customers;

Supportive jurisdictions — where clear shifts towards open banking are occurring and regulators openly encourage, but do not mandate, open banking; and

Neutral jurisdictions — where there have been little to no regulatory statements on open banking, but there has been some industry-led adoption and experimentation.

Although the approaches and underlying policy objectives may vary, the direction of travel is clearly towards encouraging adoption of open banking. Below we discuss the approaches of selected Asian jurisdictions, as compared to the UK, European Union and the U.S.

Mandatory jurisdictions²⁷

European Union

PSD2 is considerably broader than open banking, as it provides the legal foundation for a single European market for payments, to establish safer and more innovative payment services across the EU. Member states were required to transpose PSD2 into their national laws and regulations by January 2018.

Crucially, PSD2 helps to give rise to open banking by (a) introducing regulation for account information service providers (AISPs), payment initiation service providers (PISPs) and card-based payment instrument issuers; and (b) placing a requirement on all payment account providers (such as banks) to permit open access to payment account information for third parties with the necessary permissions and authorizations (i.e., AISPs and PISPs), without requiring the third party to contract with the bank, provided that the explicit consent of the customer has been obtained. However, to ensure that the process of information sharing is effective and secure, PSD2 places obligations on both payment account providers and data recipients. PSD2 also prohibits screen-scraping in most cases;²⁸ however, it does not mandate that information must be shared through APIs (in contrast to the UK, as well as other non-EU jurisdictions, as discussed further below).

United Kingdom

In the UK, open banking is mandated by the Retail Banking Market Investigation Order 2017 (RBMIO), which is overseen by the Competition and Markets Authority (CMA), in parallel with the Payment Services Regulations (PSR), which transpose PSD2 into UK law and are overseen by the Financial Conduct Authority (FCA). The open banking measures were initially proposed by the CMA to open up competition in the retail banking market, and were only mandatory for the nine largest UK banks, but were effectively superseded by the PSRs. Today there is overlap between the RBMIO and the PSRs. In essence, the PSRs prescribe that Account Servicing Payment Service Providers (which includes incumbent banks) must open up and share in-scope data, while the RBMIO prescribes that data must be shared using APIs. While the RBMIO remains mandatory only for the nine largest retail banks in the UK, numerous other banks have opted to comply with the standards published pursuant to the RBMIO, to facilitate with their obligations under PSD2 and the PSRs.

Notwithstanding efforts made, open banking was available only 83 percent of the time in the first quarter of 2019.²⁹ As late as April 2019, some aspects of the open banking program, in particular with regard to mobile app functionality, were reportedly delayed.

In addition, a survey this year found that only one in four people in the UK had heard of open banking, and only one in five of those who had heard of open banking said they knew what it meant or entailed, according to the Financial Times.³⁰

Still, the Financial Conduct Authority (FCA) has to date approved over 150 entities to offer open banking services, ranging from simple account aggregation to finding loans.³¹ More than 65 PSD2 licenses have been granted in the UK to date.³² By comparison, most European countries are still in single-digits.³³ When it comes to standardizing how banks share data, the UK's framework leads the way.

Australia

The Consumer Data Right (CDR)³⁴ legislation was passed by the Australian Parliament in August 2019.³⁵ It is sector-agnostic, but will be rolled out in the banking sector first, starting with specified categories of product data and progressing in phases to eventually cover all banks and other categories of product and consumer data. Over time, the CDR is intended to be implemented in other sectors, such as energy and telecommunications.

The CDR is broadly similar to the UK and EU open banking regimes, in that it empowers consumers to instruct their



banks (as data holders) to share their data with accredited data recipients. Like the UK regime, Australia's open banking program requires data recipients to create dashboards so that consumers can easily review and control their consents. However, there are some significant differences, for example, in respect of reciprocity and derived data. These are highlighted in the comparison chart on pages 22-23.

Hong Kong

As part of the HKMA's initiatives to move Hong Kong into a new era of Smart Banking, it launched an Open API Framework in July 2018. Although there is no new legislation to mandate the regime per se, the cooperation of the retail banks with the HKMA to follow the framework is, for all intents and purposes, mandatory. The framework required retail banks to adopt open APIs in a four-phased approach from January 2019, beginning with financial product information and gradually allowing third party providers increased access to other types of information, such as customer acquisition and transactional processes.

Since the launch of Phase I in January, the 20 participating retail banks have made available more than 500 Open APIs. The HKMA said in July that as a result new websites and apps have provided services such as foreign exchange rate information and deposit rate and loan comparisons. Since Phase III and IV Open APIs involve access to customer data and processing of transactions, the HKMA has said these phases would require "stronger control measures" and more detailed standards "to facilitate secure and efficient implementation across the industry before setting out a concrete implementation timetable."³⁶ The HKMA is working with the industry with a view to publishing a set of technical standards in 2020.

²⁵ The Four "Os" of Open Banking (2019), at <https://www.redhat.com/en/blog/four-os-open-banking>

²⁶ ASEAN Financial Innovation Network launches API exchange (2018), at <https://www.fintechfutures.com/2018/09/asean-financial-innovation-network-launches-api-exchange/>

²⁷ Please refer to the chart on pp. 22-23 for a comparison of the mandatory open banking regimes.

²⁸ Screen-scraping where the TPP identifies itself to the bank as acting in that capacity will continue to be permitted. Screen-scraping where the TPP impersonates the customer will be banned.

²⁹ Is Open Banking being hobbled by outages?, Finextra (2019), at <https://www.finextra.com/newsarticle/33870/open-banking-hobbled-by-outages>

³⁰ Open banking: the quiet digital revolution one year on, Financial Times, Jan. 11, 2019, at <https://www.ft.com/content/a5f0af78-133e-11e9-a581-4ff78404524e>

³¹ See directory of regulated service providers, at <https://www.openbanking.org.uk/customers/regulated-providers/>

³² See FCA's Financial Services Register at https://register.fca.org.uk/ShPo_HomePage.

³³ See InnoPay TPP Radar, at <https://www.innopay.com/en/publications/innopays-tpp-radar-europe-gearing-use-access-accounts-under-psd2>

³⁴ Treasury Laws Amendment (Consumer Data Right) Act 2019.

³⁵ Treasury Laws Amendment (Consumer Data Right) Act 2019.

³⁶ Open API Framework for the Banking Sector: One Year On, Hong Kong Monetary Authority, July 31, 2019, at <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2019/07/20190731-3/>

Mandatory open banking jurisdictions

Comparison	EU	UK	Australia	Hong Kong
Regime / legislation	Second Payment Services Directive (PSD2) PSD2 covers all aspects of payments, including issuance of e-money	Open Banking Regime: Retail Banking Market Investigation Order (RBMIO)/ Payment Services Regulations (PSR)	Treasury Laws Amendment (Consumer Data Right) Act 2019 (CDR) CDR is a cross-sector open data initiative	Open API Framework
Primary regulator	European Commission	Competition & Markets Authority (oversees RBMIO) / Financial Conduct Authority (oversees PSRs)	Australian Competition & Consumer Commission	Hong Kong Monetary Authority
Effective date	Jan. 12, 2016 Member states required to transpose PSD2 into their national laws by Jan. 13, 2018. Phase I: End of January 2019; Phase II: End of October 2019; Phases III and IV: TBC	Jan. 13, 2018	Pending finalization of rules and legislative instruments. First phase anticipated to start from Feb. 1, 2020.	July 18, 2018, with phased approach for different data:
Key open banking requirements	Requirement of all payment account providers to share payment account data with authorized third parties with the necessary permissions (without requiring the authorized third party to enter into a contract). Screen-scraping is banned in most cases. PSD2 does not mandate the use of APIs.	PSR: Same as PSD2. RBMIO: Develop and use open API standards for sharing account information and initiating payments.	Data holders (e.g., banks) must share (a) customer/consumer data with third parties subject to and in accordance with consent from the customer/consumer; and (b) product data upon request by any third party. APIs used by data holders and ADRs under the regime must comply with data standards issued by the Data Standards Body.	Implementation of Open APIs within prescribed timeframes. Adoption by banks of formal governance processes for data recipients.
Mandatory?	Yes.	Yes, subject to penalties.	Yes, subject to penalties.	In practice, yes. HKMA expects banks to implement the Open API Framework.
Which entities must share data	A broad range of institutions involved in payment services, including banks.	Mandatory for the nine largest current account providers in the UK, although other firms may choose to participate (and many have done so).	A broad range of institutions across sectors. For the financial services sector, all Authorized Deposit-taking Institutions and Accredited Data Recipients.	All banks with retail operations.
Reciprocity	None mandated.	None mandated.	Applies in a phased approach.	None mandated.
Data scope	Customer payment accounts, including current accounts, credit card accounts and e-money accounts.	Similar to PSD2 but provides more detailed definitions of personal current account and business current account data sets covered by the RBMIO.	At implementation, specified product data. Further phased rollout to other categories of product and consumer data. Currently, it is not anticipated that the CDR regime will extend to data that has been "materially" enhanced.	Phase I: Product and service information Phase II: Subscription and new applications for product/service Phase III: Account information Phase IV: Transactions
Regulation of third party providers	Yes; PSD2 introduces regulation of account information and payment initiation services, as well as card-based payment instrument issuers.	Yes; same as PSD2.	Yes; data recipients must be accredited and are subject to regulatory requirements. Accredited data recipients may share data with other, non-accredited third parties which are treated as outsourced providers and indirectly regulated as such.	No; banks are required to have governance processes in place (e.g., onboarding checks and ongoing monitoring).
Stated policy objectives	a) Contribute to an integrated payments market across the EU. b) Improve the level playing field for payment service providers (including new players). c) Make payments safer and more secure . d) Protect consumers . e) Encourage lower prices for payments.	a) More competition and innovation in the interests of consumers. b) Greater consumer protection . c) Enhanced market integrity .	a) Enhance customer focus . b) Encourage competition . c) Create opportunities . d) Promote efficiency and fairness .	a) Ensure the competitiveness of the banking sector. b) Encourage more parties to work with banks to provide innovative/integrated services that improve customer experience. c) Keep up with worldwide development on delivery of banking services.

Supportive jurisdictions

Singapore

MAS explicitly supports data sharing and open banking. It views open banking as a “larger good” giving “consumers ownership over their financial data, to make that data portable, and therefore [enabling] switching and choice among financial service providers,” which “should promote competition to improve pricing and service quality.”³⁷

MAS has not prescribed regulations on open banking, but it has taken concrete steps to facilitate it. In particular:

- ✓ In March 2019, MAS published a consultation paper on proposed revisions to the Guidelines on Technology Risk Management. It includes a section on API development, which aims to encourage the adoption of open banking while managing technology risk;
- ✓ It co-founded APIX, which was launched at the Singapore FinTech Festival in November 2018; and
- ✓ In 2016, MAS and the Association of Banks in Singapore (ABS) produced an e-book on best practices for the implementation of APIs in financial institutions, along with an API Playbook which identified common and useful APIs for the financial services industry.

Other government bodies are also looking into initiatives that would benefit open banking. In May 2019, the Personal Data Protection Commission (PDPC) launched a consultation on introducing a data portability right into the Personal Data Protection Act. And in June this year, the Infocomm Media Development Authority launched the Trusted Data Sharing Framework together with the PDPC.

Japan

Open banking is not compulsory in Japan, but the National Diet amended the Banking Act in June 2018, requiring that banks make efforts to open up their APIs to electronic settlement agency services providers by 2020. This is consistent with the Japan Financial Services Agency’s Financial Digitalization Strategy, which broadly aims to encourage financial institutions to implement technological advancements while avoiding associated risks and providing the best financial services to the Japanese people.³⁸

Prime Minister Shinzo Abe has set a target of 80 banks to have open APIs by 2020.

Malaysia

The Bank Negara Malaysia (BNM), the Central Bank, has been actively promoting the adoption of open APIs since 2018. That includes establishing Open API Implementation Groups for the banking/Islamic banking and insurance/takaful industries, to identify and develop standardized open APIs for high-impact use cases.

Following a public consultation in September 2018, BNM issued a Policy Document on Publishing Open Data using Open APIs in January 2019.³⁹ In it, BNM makes recommendations around open API standards, third-party governance processes and adoption and publication of open API specifications, citing its objectives to:

- ✓ Enhance access to financing products and services offered by financial institutions;
- ✓ Promote comparability of motor insurance/takaful products;
- ✓ Facilitate development of fintech to allow consumers to compare a wide range of financial products and services matching their specific needs and circumstances, besides improving experience and providing choices to customers; and
- ✓ Leverage on technology for the provision, distribution and consumption of financial services.

BNM plans to issue a Discussion Paper on open banking for public and industry consultation.

U.S.

While some open banking developments are underway in the U.S., there is no pending legislation or regulation at the federal level. However, government agencies have shown support for the market moving away from screen-scraping and towards using APIs, given that they are more secure.

The U.S. Treasury recently made several recommendations on open APIs, and innovation in the financial services industry more generally.⁴⁰ The driver was to “promote economic growth, increase consumer satisfaction, and improve choice, opportunity, and economic inclusion for all Americans” and “also stimulate innovation, increase competition, and enhance the global competitiveness of the United States.”

The Treasury also reviewed the UK approach to open banking and determined that an equivalent US regime was “not readily applicable,” but recommended that U.S. financial regulators should “observe developments and learn from the British experience.”

37 The Future of Banking – Evolution, Revolution or a Big Bang?, Introductory Remarks by Mr. Ong Chong Tee, Deputy Managing Director, Monetary Authority of Singapore, at the German-Singaporean Financial Forum (Apr. 16, 2018), at <https://www.mas.gov.sg/news/speeches/2018/the-future-of-banking>

38 To turn challenges into opportunities, Financial Services Agency of Japan (2018), at <https://www.fsa.go.jp/common/conference/danwa/20181128/speech.pdf>

39 Policy Document on Publishing Open Data using Open APIs, Bank Negara Malaysia (2019), at http://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=687

40 A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech, and Innovation, U.S. Department of the Treasury (2018), at <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities-Nonbank-Financi....pdf>

Taiwan

Taiwan’s Financial Supervisory Commission has taken steps to encourage open banking, instructing:

- ✓ the Bankers Association of the Republic of China to conduct research and to consider how to regulate the relationship between banks and TPPs;
- ✓ the Financial Information Services Co., Ltd., a government-owned financial information company, to propose standards for open APIs and to develop an Open API Management Platform for banks and service providers; and
- ✓ NCCU GLORIA, a government-subsidized academic center, to work with FISC to review its initiatives.

The Bankers Association has proposed to implement a three-phase implementation approach covering (1) public financial information; (2) non-public account information; and (3) transactional information.

South Korea

The South Korean government has identified the introduction of an open banking system as a key national agenda item. In his keynote speech at Korea’s 2019 Fintech Week, then-chairman of the Financial Services Commission (FSC) Choi Jong-Ku stated that “the FSC will build a legal and institutional framework to help fintech grow into a new growth driver. To this end, the FSC will create an open and competitive financial ecosystem, with the introduction of the open banking system and the commercialization of personal financial data.”⁴¹

In February 2019, the FSC announced plans to launch an open banking system by the year-end. In the first phase, the FSC has proposed that commercial banks voluntarily open their payment networks to technology firms and other banks. Currently, only traditional lenders can access those payment networks. In the second phase, Korea’s Electronic Financial Transactions Act will be amended to require all banks to offer payment service providers standardized APIs for funds transfers. A third phase contemplates providing qualified fintech payment service providers direct access to payment systems, without relying on banks’ services.

41 FSC Holds Korea Fintech Week 2019, Financial Services Commission (2019), at http://www.fsc.go.kr/eng/new_press/releases.jsp?menu=01&bbsid=BBS0048&selYear=&sch1=&sword=&nxPage=2

42 Report of the Working Group on Fintech and Digital Banking, Reserve Bank of India (2017), at <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF>

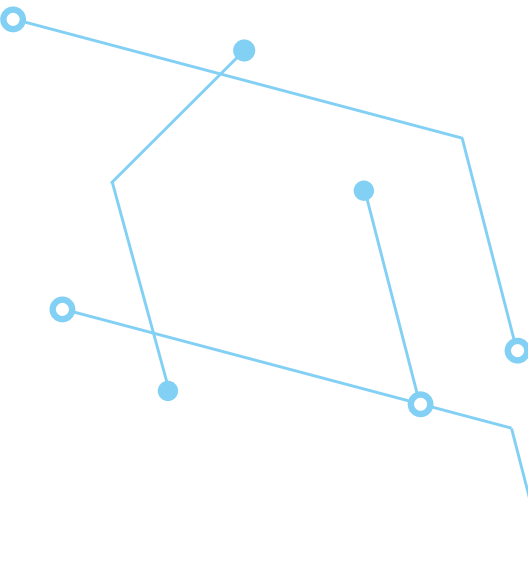
43 Open Banking, Preparing for lift off, Open Banking Ltd (2019), at <https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf>

India

In 2017, the Reserve Bank of India (RBI) released a report on regulatory issues relating to fintech and digital banking in India, drafted by an inter-regulatory working group made up of representatives from the RBI, other government ministries and fintech companies. The report stated that regulators need to “examine whether and how their regulations impose barriers to innovation and whether, and to what extent, these can be removed,” and recommended that an “environment [be provided] for developing FinTech innovations and testing of applications/APIs developed by banks/FinTech companies.”⁴²

Measures brought by the government to encourage digitalization in the banking sector include:

- ✓ The introduction in 2016 of the Unified Payments Interface (UPI), which creates an interoperable payments system that allows instant inter-bank fund transfers using a single “Virtual Payment Address.” DBS India uses UPI to enable customers to manage all of their bank accounts held with other banks via their digibank application. As of March 2019, UPI is used by 142 banks, accounting for just under 800 million transactions a month with a combined value of US\$19 billion.⁴³
- ✓ India Stack, which is a series of open APIs that was created in collaboration with the private sector. India Stack enables the creation of digital financial infrastructure to promote financial inclusion and e-commerce. Aadhaar, India’s national biometric identification system, was built using India Stack and is used by financial institutions for KYC purposes.



New Zealand

In New Zealand, the development of open banking is being led by PaymentsNZ, an organization formed in 2010 by the industry with support of the Reserve Bank of New Zealand (RBNZ) which governs New Zealand’s core payments systems and works with industry to lead the future direction of payments. A pilot in 2018 included account information services and payment initiation services (similar to PSD2), and API standards were released in March 2019. Once the API standards service is open, interested API providers and third parties will be able to apply to become registered standards users, who are authorized to enter into bilateral arrangements.

The RBNZ has noted that open banking could “improve the soundness and efficiency of the financial system” and “increase competition and reduce concentration in the provision of financial services, reducing the systemic importance of large banks and reducing the cost of financial services,” but also acknowledged that open banking carries risks, such as reputational risk for banks. For now, the RBNZ has chosen to observe developments and act only if necessary in the future.⁴⁴

Neutral jurisdictions

China

Open banking appears to be thriving in China, despite the lack of specific regulation or pronouncements in the area. Instead of regulation, the move towards open banking is driven by an innovation-focused economy and the world’s most digitally connected consumers.⁴⁵

The Chinese tech giants, such as Alibaba, are leveraging open APIs and driving their broad adoption to allow third parties to offer services to their customers and make data more portable within their ecosystems. This has led to banks also leveraging open APIs to redefine their roles in the economy — becoming technology companies and lifestyle partners, as well as financial institutions.

Indonesia

There are currently no government mandated frameworks or regulations in place, or any proposed timelines for implementation of open banking initiatives. Regulatory bodies like Bank of Indonesia and Otoritas Jasa Keuangan (the Financial Services Authority) are currently more focused on the goal of improving financial inclusion through fintech for unbanked individuals in Indonesia and improving payments infrastructures, as opposed to open banking specifically.

Nevertheless, there is some early adoption and experimentation, as some major Indonesian banks such as Bank Mandiri and the Bank of Central Asia have opened their APIs to the public.

Sri Lanka

As in Indonesia, there have not been formal governmental measures to promote open banking. Still, Nations Trust Bank in Sri Lanka launched Sri Lanka’s first open banking product in April 2018. The CEO noted that the “future of banking lies in being one of safe public places, transparency and inclusivity.”⁴⁶

Although the approaches and underlying policy objectives may vary, the direction of travel is clearly towards encouraging adoption of open banking.

44 An Open Mind on Open Banking, Reserve Bank of New Zealand (2018). See <https://www.rbnz.govt.nz/financial-stability/financial-stability-report/fsr-may-2018/an-open-mind-on-open-banking>

45 How China’s open banking experiment is unfolding, Ernst and Young (2018), at https://www.ey.com/en_gl/banking-capital-markets/how-chinas-open-banking-experiment-is-unfolding

46 Nations Trust Bank debuts Open API Banking in Sri Lanka, Daily FT (Apr. 25, 2018), at <http://www.ft.lk/financial-services/Nations-Trust-Bank-debuts-Open-API-Banking-in-Sri-Lanka/42-653964>

Implications of different regulatory approaches

There are pros and cons to these different regulatory approaches to open banking. Where open banking is mandated, that is a strong statement of support by the government which can jumpstart innovation. On the other hand, such requirements might be perceived as just an additional compliance burden, in which case they are unlikely to spur innovation. Accenture’s McFarlane explains, “Market practice for geographies that have introduced formal regulations has been for incumbent banks to strongly focus on compliance first, and then move to a ‘compete’ mindset post regulatory compliance.”

Regulators might be ahead of where the market is or what regulated entities are ready to take on. For example, regulated entities might not be far enough along the curve with technology to truly capitalize on open banking. The Open Banking Monitor, a portal set up by Amsterdam-based payments consultancy Innopay, estimates that more than 300 open banking-related developer portals are currently live, most of them launched by EU banks seeking to comply with PSD2 requirements. Only half of those PSD2-banks say their APIs are ready for use: the rest are sandboxes using example data generated by the bank itself.⁴⁷

In mandating open banking, regulators also risk setting overly prescriptive requirements which can become outdated rapidly, especially where technology is involved. This can then affect innovation, according to Hans Brown, Managing Director, Global Head of Innovation at Bank of New York Mellon (BNY Mellon). “The difficulty with a ‘hard rule’ is it can sometimes become overly onerous and therefore lose sight of the outcome it is trying to affect.” He points to the Association of Banks in Singapore’s API playbook as a good example in bringing together the regulator and industry participants to develop guidance.

In contrast, a neutral approach may not be a clear enough statement of support if the government wants to encourage open banking. In the absence of clarity from the regulator, financial institutions are unlikely to move forward with something new.

Regardless of what approach is taken, if governments want to encourage adoption of open banking (which generally appears to be the case), it is important to (i) provide clarity regarding the regulatory stance towards open banking; (ii) be aware of and stay in sync with industry readiness; and (iii) avoid the perception that it is merely a compliance box to be checked or something that increases compliance burden. It is also helpful for the regulator to be clear as to its policy objectives with respect to any open banking initiative.

Other important considerations include what regulatory body is overseeing open banking and the pace and scope of any regulation.

If governments want to encourage adoption of open banking (which generally appears to be the case), it is important to:

- ✓ provide clarity regarding the regulatory stance towards open banking;
- ✓ be aware of and stay in sync with industry readiness; and
- ✓ avoid the perception that it is merely a compliance box to be checked or something that increases compliance burden.

Regulatory body

The decision of which regulatory body will oversee open banking is largely reflective of the government’s policy objectives, and informs what the focus will be in assessing the success of open banking from the government’s perspective. In Australia, for example, the government is perceived by some as approaching the issue from a competition and market access perspective, rather than one of prudential policy, as the open banking process has been driven by the Australian Competition and Consumer Commission (ACCC). This seems to indicate that the government will largely be looking at whether open banking is increasing competition in the banking sector, through the introduction of new players, lower prices, innovation and the like. Should the Australian Prudential Regulation Authority (APRA) issue its own guidance or requirements that touch on any aspect of open banking, it would be important to ensure they are consistent with those issued by the ACCC. Otherwise, financial institutions engaging in open banking would be subject to differing, possibly conflicting requirements, which would likely increase their compliance burden and potentially slow or lessen innovation based on open banking.

Conversely, in Hong Kong, the Open API Framework has been established by the banking regulator, the HKMA. The fact that the HKMA is overseeing this initiative suggests a focus on ensuring that Hong Kong retains its status as an international financial center, which is one of the HKMA’s four main functions.⁴⁸

In Singapore, the government has taken a more coordinated approach. MAS engaged early with the PDPC on the development of the latter’s proposed data portability framework, which would apply across all industries.

47 Open Banking Monitor: Banks Moving Beyond the PSD2 Requirements, Innopay (2019), at <https://www.innopay.com/en/publications/innopay-open-banking-monitor-banks-moving-beyond-psd2-requirements>.

48 See https://www.hkma.gov.hk/media/eng/publication-and-research/annual-report/2011/04_About_the_HKMA.pdf

Pace

As noted above, a key consideration is whether regulations are ahead or behind of industry and/or technology. Too far ahead, and businesses may feel compelled to take a leap before they are ready, which in the financial services industry could be risky. Too far behind, and the industry may lack guidance needed to move forward in a secure and compliant manner. Ravi Menon, Managing Director of MAS, has said, “Regulation must not front-run innovation. Introducing regulation prematurely may stifle innovation and potentially derail the adoption of useful technology.”⁴⁹

One way of calibrating the pace of regulation is to allow for pilots and phased deployment, such as in Hong Kong, which could be based on different categories of financial institutions, products, or recipients. In Australia, due to delays in the passage of legislation and recognition of the complexity of the issues, the ACCC decided to start with a pilot that applied to the four major Australian banks, in respect of one category of data, product information. The full implementation of open banking is expected to take place over several phases stretching into 2021. Many banks have welcomed this approach, which allows them to start with low-risk data.

To ensure the regulatory approach is in sync with what is going on in the market, it is important that there be ongoing dialogue and engagement between regulators, industry participants, and technology providers. For example, in Australia, draft legislation released for consultation in August 2018 indicated that the CDR would apply to aggregate or value-added data derived from consumer data. Following significant pushback from industry, a revised version of the legislation was released in line with industry feedback.

Data types

As a threshold matter, it is important for regulators to consider what kind of data should be shared in any open banking regime. Some banks have suggested that customers’ personal information, like a date of birth, address, or phone number, which could be maliciously misused in scams or fraud, should not be included in the regime.

Financial institutions may also have concerns over being required to share derived or value-added data. This is data that incorporates additional information derived from calculations or other sources. This could include financial statistics on the state of the economy which are derived from business activity.

This has been an issue in Australia, where the CDR legislation includes a very broad definition of data, which could potentially include value-added data sets, imputed information and information that is the subject of intellectual property rights. Such concerns were taken into account, as noted above, and the Australian Treasury clarified in October 2018 that, as a broad principle, “data that results from material enhancement by the application of insight, analysis

or transformation” was not intended to be the subject of the CDR. However, the Australian Treasury department retains the power to broaden the CDR to certain derived data, if necessary.

A lack of clarity around the information that must be shared, or an overly broad requirement, will likely diminish banks’ appetites for open banking. Nevertheless, banks’ concerns could be mitigated in this area, if regulators follow the Australian example in taking into account industry feedback and clarifying the scope of data covered.

Reciprocity

Another key regulatory consideration is whether reciprocity should be required or recommended. The principle of reciprocity requires any organization who wants to become part of the open banking ecosystem to also share the data it holds with other accredited stakeholders. This should be good news for consumers, because the data is being shared by all participants and this should help level the playing field from their perspective. Some banks however argue it may end up having the opposite effect by allowing free-riding and/or by enabling fintech or technology players to effectively take on banking functions, while the banks themselves would be prevented from doing the opposite. Whether reciprocity is required, and to what degree, should depend on the regulator’s policy objectives, but, as with the type of data covered, the approach should be made clear and should ideally be informed by feedback from industry participants.

Standard Chartered Bank’s Lloret hopes to see this issue resolved via more reciprocal and symmetrical data sharing frameworks, where participants are incentivized and rewarded for their contribution in, say, developing data analytical capabilities, as outlined in a July 2018 paper by the Institute of International Finance. The paper concluded that, among other features, such frameworks should include “the right incentives to actually share their data (in the case of customers) and to build value added proposals for customers based on those shared data (in the case of service providers).”⁵⁰

Standardization

Even when such issues of what data to include and on what terms are resolved, the problem of what that data should look like, and whether this should be something that the regulator determines, has also become a key area of debate.

Some banks see a role for governments and independent standards bodies when it comes down to defining what the data should look like. “Some taxonomy definitions are essential,” says BNY Mellon’s Brown. The more complicated the taxonomy, “the more friction gets generated because then you’ve got more things to keep in sync, which is where standards like the ISO 20022 can make a huge difference,” says Brown.

49 Financial Regulation: The Way Forward, Speech by Mr. Ravi Menon, Managing Director, Monetary Authority of Singapore (Apr. 20, 2017), at <https://www.mas.gov.sg/news/speeches/2017/financial-regulation-the-way-forward>

50 Reciprocity in Customer Data Sharing Frameworks, Institute of International Finance (2018), at https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf

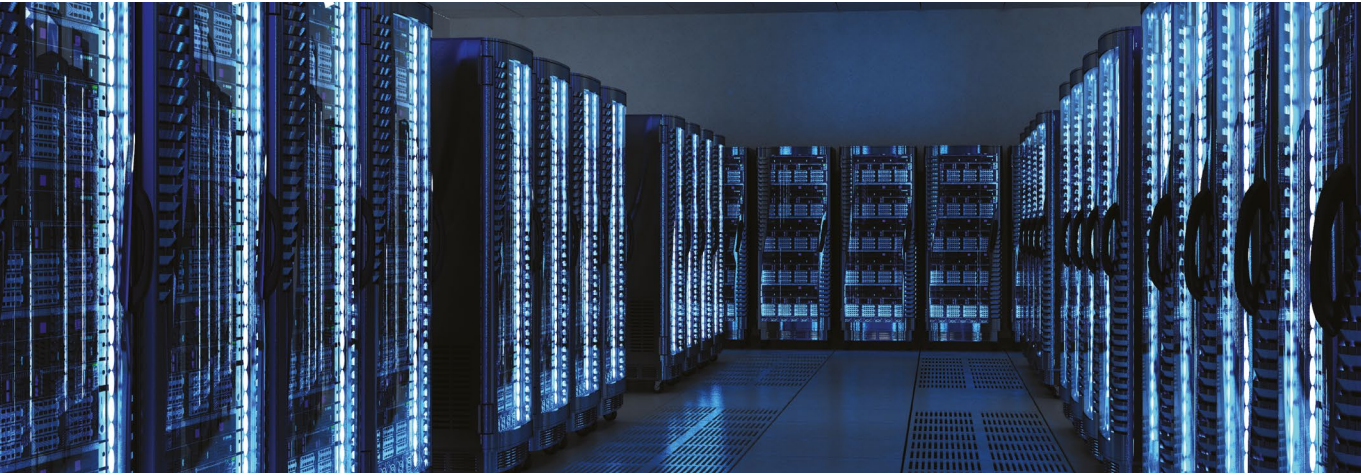
Standards can also be developed by industry. Microsoft’s Leung says, “When it comes to data sharing, standards are very important. That’s why Microsoft, together with partners, developed a Common Data Model to provide shared and consistent metadata definitions for common banking and financial industry data elements such as loans, mortgages, etc., and this common schema allows customers and partners to build interoperable open banking solutions.”⁵¹ The Association of Banks in Singapore’s (ABS’) playbook, developed with MAS, wins plaudits for the detail it goes into and the pioneering approach it has taken. “It became the first to basically say these are common building blocks across the different facets of the industry that we can agree on,” says BNY Mellon’s Brown. “The ABS playbook wasn’t a rules-based approach; it laid out an approach that said ‘here is the collective position of all the participants.’ I think that’s the kind of thing, going forward, that we need more of — bringing all the stakeholders in the industry together to focus on ways we can reduce the barriers and the friction between our interactions so we can focus on the clients.”

With respect to regulatory standards, the distinction between defining but not imposing is key, says Graham Dickens, Associate Founder and Chief Technology Officer at Judo Bank. If governments over-prescribe, and make things mandatory, it incurs costs on organizations and ends up favoring bigger businesses which can absorb the costs. Finding that balance is key. “Having anything that tries to get too intrusive isn’t going to work,” he says. “And also conversely having anything that’s too loose is not necessarily going to promote a clear approach. You end up with people going in different directions.” Temenos’ Goyal says, “Regulators should not make it difficult for smaller fintechs or banks to interact with each other. If there are standards on information security on APIs, it makes it easier for everyone in the ecosystem.”

Deciding what to standardize and what to leave to the market should also involve considering the pace of innovation.

“To decide between standards versus laissez faire,” says API strategy consultant Scheele, “you have to think about how rapidly things are changing, and how many stakeholders are involved.” He explains, “If it’s an area that’s innovating fast, then standards will always be a step behind, whereas if an area is more mature, where the same things are being done over and over again, it makes more sense to coalesce.” Payments are a classic example. For a long time, access to the payments network was restricted to a limited number of players. The result was the evolution of standards such as SWIFT’s MT messages and more recently the ISO 20022 standard. The need for certainty of delivery and verification, and the lessons from legacy networks, drove the push for standards. Fields like product information could be harder. Since product information doesn’t require access to sensitive data, Scheele points out that it’s exactly the area attracting disrupters. “The idea of fostering innovation is that people will come up with new services and products. So beyond basic deposit and loan accounts, whatever standard you set up for product information today is going to become obsolete.”

The danger of too little standardization is to increase complexity and therefore cost. New Zealand, says Accenture’s McFarlane, got the balance right, after listening to banks advocating for more standardization of APIs. “In the UK, one of the comments we hear regularly is that the participants wished the API standards were a little more specific in the UK,” he says. “[Then] every bank would have been building the APIs the same.” Where standardization was not sufficient, that created opportunities for ecosystem players offering services integrating APIs and linking up the loose ends. “That’s why I like the New Zealand approach — because they’ve done the work via their pilot,” says McFarlane. “They’ve gone through the teething pains, they’ve understood what it means to get the standardized API approach and now they’ve got a good robust set of APIs that they can build from. Most importantly, they have been fully tested and proven which gives them an excellent baseline to move forward with.”



51 See <https://powerplatform.microsoft.com/en-us/common-data-model/>

Interrelation with other regulatory requirements

Open banking can implicate several areas of law and regulation, which could present a challenge to financial institutions concerned about complying with existing legal and regulatory requirements.

Banking secrecy and privacy/data protection

On its face, sharing of consumer data between financial institutions seems to cut across established principles of privacy, data protection and, in some countries, banking secrecy.

Banking secrecy

Banking secrecy is a duty imposed on banks to protect the information of their customers, and specifically not to disclose it except in certain prescribed circumstances. Because of such duties imposed in many jurisdictions, banks often view themselves as stewards of their customers’ information.

Nevertheless, banking secrecy should not be a major barrier to implementation of open banking. In some jurisdictions such as the UK, it is permissible to disclose customer information where such disclosure is compulsory by law — e.g., under a mandatory open banking regime. This exception is not available in all jurisdictions — for instance, in Singapore where there is no mandatory open banking regime. However, another common exception is for disclosure with the customer’s prior informed and express consent. Given that open banking is typically premised on the customer’s consent to share its data, banking secrecy laws should not create a major impediment to implementation of open banking.

At the same time, regulators should be mindful to ensure that any open banking requirements or guidelines are compatible with banking secrecy requirements. In some cases, banking secrecy laws may need to be modernized to accommodate data sharing and open banking.

Privacy/data protection

In implementing open banking, all businesses must also comply with applicable privacy and data protection laws. As a general matter, both open banking regimes and privacy laws are premised on the principle that individuals should have control over how their personal data is used and with whom it is shared, and can consent for their data to be shared with or used by others.

Challenges may arise where requirements between an open banking regime and privacy laws differ. In Australia, for example, banks are facing challenges arising from the CDR regime, where CDR protections go beyond the requirements under general privacy law. For example:

- ✓ The CDR regime introduces a concept of ‘Privacy Safeguards’ which govern data transferred and accessed under the Australian open banking regime. These safeguards are similar to, but more restrictive than, the Australian Privacy Principles which govern the handling of personal information. This could lead to banks having to effectively silo data under the CDR from other personal information, which could be operationally difficult.
- ✓ If an entity no longer requires CDR data for a purpose permitted under the CDR legislation or rules or another Australian law, it must take the steps specified in the rules to destroy that data or ensure it is de-identified. The rules are significantly more detailed and prescriptive than the de-identification obligation under the Privacy Act, which only requires that entities take reasonable steps to ensure personal information is de-identified.

Nevertheless, change is starting to occur across Asia to modernise and enhance data privacy laws in a manner that may benefit the adoption of open banking. For example, in Singapore, the PDPC is introducing a data portability framework. Data portability has also been introduced in Thailand’s Personal Data Protection Act. As with banking secrecy, it would facilitate adoption if any open banking rules, guidelines, or requirements were consistent with existing privacy and data protection requirements.

Open banking can implicate several areas of law and regulation, which could present a challenge to financial institutions concerned about complying with existing legal and regulatory requirements.

AML/CFT

Implementation of broad data-sharing arrangements, and opening up systems to access by APIs, may also raise questions around anti-money laundering and countering the financing of terrorism (AML/CFT). In particular, does the implementation of open banking expose banks to significantly more AML/CFT risk? This is an assessment that all banks will need to conduct when launching or implementing any kind of new business practice, service or developing technology, and would feed into the overall enterprise-wide assessment of money laundering and terrorist financing risks that are faced by the bank.

The AML/CFT risks associated with merely providing data through an open banking platform would seem to be low, because such activity does not involve the provision of a new financial product, or the provision of an existing financial product through a new delivery channel, to a customer (rather, it is just a commercial arrangement between two institutions). However, AML/CFT challenges may arise when considering open banking more widely — particularly in the areas of onboarding of customers and transaction monitoring.

Customer onboarding

A question might arise where a bank is a data or customer recipient — for example, where one bank (Bank A) onboards a customer from another bank (Bank B), can Bank A rely on the AML/CFT measures conducted by, and information received from, Bank B? The answer to this will depend on the risk appetite of Bank A, the due diligence that has been conducted on Bank B, and local regulatory requirements. For example, in Singapore, reliance on third parties for AML/CFT is permitted, provided certain conditions are fulfilled. Ultimately, Bank A might feel more comfortable completing its own AML/CFT measures before onboarding the customer, particularly where Bank B is located in a foreign jurisdiction, but this should not impede banks from implementing open banking.

The answer to this question above would likely change if Bank B were to be replaced by a new market entrant such as a data recipient or fintech firm. Particularly where the entity is unregulated, it is much less likely that a bank would be permitted to rely on their AML/CFT measures (or that a bank would feel comfortable to rely on such measures). In such case, a bank would likely need to revert to conducting its own full AML/CFT measures before onboarding the customer; however, as this is usual practice for most new bank customers, it should not significantly impede the implementation of open banking.

Transaction monitoring

Banks may also have concerns that wider uptake of open banking could compromise or weaken transaction monitoring controls, as such controls are typically reliant on transactions being processed by or through the bank, not other institutions. If open banking leads towards customers departing from a single-bank relationship and taking business to and opening accounts with a variety of banks, the effectiveness of existing transaction monitoring controls may be diminished.

At present, there is no clear solution for this potential issue. Ultimately any solution will likely require collaboration between regulators and both the banking and fintech industries, as a bank or third party could build and potentially monetize a transaction monitoring platform, but it may require regulator backing or support to obtain sufficient data and become effective. Potential solutions could be regulator-led (e.g., by mandating banks to develop methods to share transaction-related data), or industry/bank-led (e.g., by a bank, or a service provider, designing a system that can monitor transactions on a market-wide basis).⁵²

Technology risk management and cybersecurity

Regulated financial institutions are generally required to comply with technology risk management (TRM) requirements imposed by financial services regulators around the world. Such requirements typically include, among other requirements:

- ✓ Establishing a framework, governance and controls to assess and manage technology risks
- ✓ Management of third-party vendors and outsourced providers
- ✓ Ensuring system reliability, business continuity and operational resilience

In addition, many countries have enacted cybersecurity laws, which in some cases have varying requirements by sector. For example, there may be heightened requirements for financial services, which may be viewed as critical infrastructure, as in China. In some countries, financial services regulators will set their own sector-specific cybersecurity requirements, as in Singapore and Hong Kong.

A potential issue, similar to that described above in connection with AML/CFT, is that through open banking regulated financial institutions may be partnering and sharing data with unregulated entities which are not subject to the same TRM or cybersecurity requirements. If they are not, but the financial institution is, then the responsibility for compliance will likely remain with the financial institution, but the same standard may not be met by all the service providers involved in open banking. Financial services regulators generally contemplate and require regulated entities to supervise outsourcing relationships, but it is unclear whether outsourcing guidance would be applicable to TPPs and data recipients in open banking.

52 Open banking, open risk? Managing financial crime in a disrupted world, Deloitte (2017), at <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-financial-crisis-open-banking-report-2017.pdf>

In Singapore, MAS has set forth some guidance on open APIs in proposed revisions to its TRM Guidelines. These provisions recommend that financial institutions should:

- ✓ implement a well-defined vetting process, taking into account (amongst others) the third party's nature of business, security policy, industry reputation and track record;
- ✓ perform risk assessment before allowing third parties to connect to its systems via APIs; and
- ✓ have robust security screening and testing of the API between the financial institution and the third party.

These guidelines place a similar responsibility on financial institutions as they have with respect to outsourced service providers. Although data recipients and TPPs in open banking may not technically provide a service to the bank, regulators may want to draw on existing principles and guidance in outsourcing guidelines. Treating data recipients in the same way as outsourced service providers could be helpful for regulated financial institutions, as they are familiar with technology and vendor risk assessment and outsourcing requirements.

While this approach is helpful in clarifying roles and responsibilities, it also imposes further obligations (and, therefore, potential liability) on regulated financial institutions, which could have the effect of diminishing their appetite towards adopting open banking.

Another approach, as exemplified in Australia and the UK, is to regulate the TPPs. This approach is explained further below.

Regardless of the approach, regulators should ensure that it is clear what requirements each entity must comply with, so that technology and cybersecurity risks are sufficiently addressed by all entities involved in open banking.

Liability

The uncertainty around liability in the context of open banking may be an impediment to broader uptake. In the absence of agreements between financial institutions and data aggregators, data aggregators may elect to continue screen-scraping, where it is permitted, which poses well-established concerns around cybersecurity and fraud. Screen-scraping also generally leaves liability for data loss with the consumer themselves, as the practice of divulging sensitive login credentials is often a breach of bank terms and conditions, an outcome which is far from ideal in the eyes of regulators.

Even where the law is clear and financial institutions take all possible security measures and are technically not liable for data loss or breach (or violations of other potentially applicable laws discussed above), consumers may nonetheless expect the financial institution to compensate them for any losses suffered, and the reputation of the bank may suffer. The problem is exacerbated by a conception held by many banks that the security practices of data aggregators are often not comparable to the standards applied in regulated financial institutions.

Nevertheless, solutions do exist to the liability issue. Whatever the legal solution that may be adopted (and while greater clarity would undoubtedly be beneficial), part of the solution lies in banks being open to formally partnering with data aggregators and other fintechs. Partnerships can allow banks to obtain comfort around data security, while also allowing them to capitalize on their incumbent advantages.



The benefit of regulating data recipients is that it provides clarity around liability and compliance requirements and helps ensure the security and stability of the ecosystem.

Potential solution (1) — regulation of data recipients

One potential solution, which has been adopted in Australia and the UK, is to directly regulate data recipients.

Under the UK's open banking framework, data recipients (i.e., Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs)) are regulated directly by the FCA. For an AISP or PISP to be authorized, it will have to meet a number of requirements, such as having in place sound governance arrangements and internal control mechanisms (including technology and cybersecurity risk management) and processes to monitor, handle and follow up on security incidents.

Once authorized, AISPs and PISPs will also need to comply with ongoing conduct of business requirements enforced by the FCA. Broadly, these requirements fall into two main categories. The first category requires certain information to be provided to the customer before and after execution of a payment transaction. The second category relates to the rights and obligations of both PISPs and customers in relation to payment transactions, covering areas such as charges, liability for unauthorized transactions and the authorization of payment transactions.

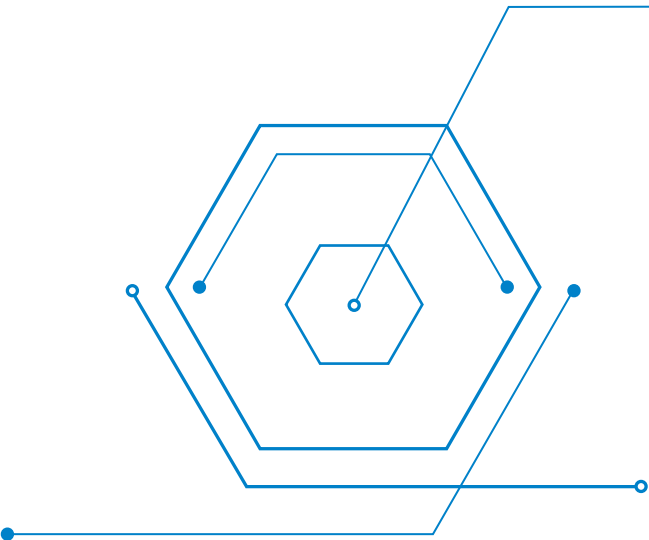
In addition, the UK's Open Banking Implementation Entity (OBIE) has established a dispute management system that banks and regulated TPPs can sign up to, which sets out a code of best practices for handling complaints and disputes. While the system is entirely voluntary (and OBIE itself does not play any role in resolving disputes), it is hoped that it will promote clear, consistent, transparent and ethical dialogue among ecosystem players.

Australia takes a hybrid approach to regulating data recipients. Under the CDR in Australia, only persons accredited by the ACCC can request CDR information. To be accredited, a person must meet several criteria such as being fit and proper, having adequate practices and procedures in place to manage relevant data and information security risks, and having adequate insurance to be able to compensate consumers for losses arising from a breach of relevant laws. Further, the CDR imposes several privacy safeguards that are

imposed on accredited persons. Thus accredited recipients of CDR data — not CDR data holders — will find themselves liable for any loss of such data resulting from a breach of the privacy safeguards. Breaches of the CDR, including by accredited data recipients, can be enforced by the ACCC with sizeable civil penalties.⁵³

Data recipients that are not accredited, which are called third party service providers (TPSPs) under the CDR,⁵⁴ can only receive CDR data from an accredited recipient under limited circumstances (e.g., for the purpose of providing goods or services to a CDR consumer). The TPSP is considered to be an outsourced service provider of the accredited data recipient, and the outsourcing agreement must comply with the CDR requirements, including requiring TPSPs to comply with similar obligations to accredited recipients. Unlike accredited recipients, TPSPs are not themselves directly supervised by the ACCC, meaning that liability remains with the accredited recipients for any failures of their TPSPs.

The benefit of regulating data recipients is that it provides clarity around liability and compliance requirements and helps ensure the security and stability of the ecosystem. However, this approach requires government resources and consideration of what entity is best equipped to oversee data recipients, which for the most part are not likely to be traditional financial institutions.



53 The ACCC can impose fines of AUD 10 million, 3 times the value of the benefit directly or indirectly obtained, or 10 percent of annual turnover (where the value of the benefit obtained cannot be determined), per breach. In addition, it can apply for injunctions or apply for the disqualification of individuals from managing corporations, among other remedies.

54 This term is not to be confused with the term "third party provider" (TPP) as we use it in this paper, to refer to both accredited and unaccredited data recipients of all kinds.

Potential solution (2) — obligations for regulated institutions

While the regulation of data recipients may be a feasible option in countries that have mandated open banking, it may not be so where there is no standalone open banking regime, often because the mandate of the financial regulator does not extend to TPPs that are not engaged in the provision of financial services. In such case, one solution is to impose further risk management requirements and controls on regulated financial institutions, as discussed above in the context of TRM guidelines in Singapore.

Data recipients could be deemed to be outsourced service providers, like TPSPs under Australia’s CDR. Since most financial services regulators have outsourcing guidance and requirements, this is one way for regulators to indirectly oversee data recipients without substantially increasing their burden. However, this would likely require outsourcing contracts between financial institutions and all data recipients, which is difficult to scale.

Should regulators decide to follow this route, it is recommended that they leverage existing guidelines and requirements, and avoid imposing additional compliance burdens on regulated entities to the extent it could deter adoption of open banking.

Potential solution (3) — private safeguards

Private safeguards may provide another solution. For example, banks may choose to treat data recipients in the same way as outsourced service providers. Banks may also seek indemnification from TPPs.

However, there are several potential problems with this approach. First, like the outsourcing solution discussed above, this approach is difficult to implement at scale, as it requires contracts for every data recipient. Second, it is likely to have uneven results, as each contract will be subject to individual negotiation to some extent. This also tends to favor larger, more sophisticated TPPs both in terms of their willingness to engage in contractual negotiations with banks and the deal that is struck. Third, it is likely to result in both commercial and consumer disputes.

One way to address these issues is to standardize the approach to such contracts, whether through regulatory guidance (as with outsourcing contracts) or an industry body. It may also be helpful to set up a system for disputes resolution, as the OBIE did in the UK.

Regardless of what approach is taken, it seems there is a need for clarity and regulatory guidance in some form with respect to the relationship between banks and TPPs, including liability issues, for the benefit of banks, TPPs and consumers alike.

Regardless of what approach is taken, it seems there is a need for clarity and regulatory guidance in some form with respect to the relationship between banks and TPPs, including liability issues, for the benefit of banks, TPPs and consumers alike.

Lack of harmonization of laws

There is no doubt that today’s regulatory landscape is complex. There is generally a lack of harmonization among various types of laws, regulations and policies, as discussed above, both among different countries and even within a country. This general misalignment, particularly with regard to privacy and data protection laws, could make open banking difficult to implement for companies offering cross-border financial services. In particular, financial institutions operating in countries with less developed data protection and banking secrecy regimes may experience a market that is less inclined to engage, because open banking adoption generally relies on consumer confidence that their data is secure.

There is, unfortunately, no easy short-term solution for this issue. In the data protection context, the advent of the General Data Protection Regulation (GDPR) has united the data protection regime in the EU and initiated the shift of countries adopting GDPR-like laws (e.g., Japan). Further global alignment of privacy and data protection laws would help foster open banking, particularly if such new laws are aligned with the GDPR’s requirements of data portability.

Finastra’s Blanquet adds his own note of concern: that while the EU and the UK have set helpful benchmarks, uncertainty will likely persist as long as large countries like China and the U.S. have yet to clearly articulate their own approaches to open banking.

As a further challenge, a handful of countries around the world and in Asia (e.g., India, China, Indonesia, and South Korea) have implemented data localization requirements and/or other restrictions on the cross-border transfer of data. Such restrictions at a minimum prevent businesses from fully realizing the potential of open data initiatives and likely deter adoption. To foster adoption of open data initiatives such as open banking, it is important for regulators and industry to engage in a dialogue about their respective concerns, towards finding less restrictive means of achieving the same ends and achieving greater harmonization.

Need for engagement by regulators

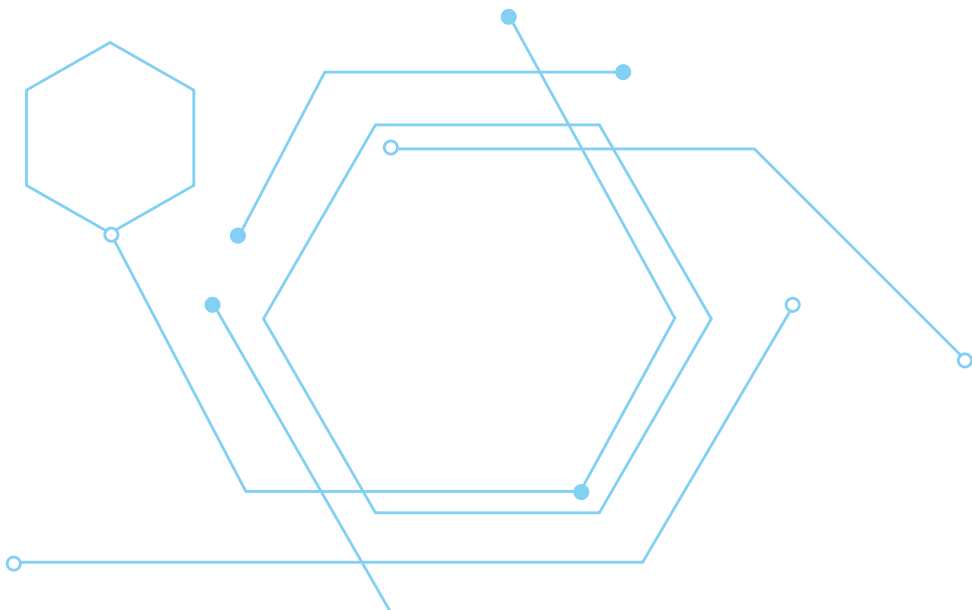
For governments trying to promote open banking, engagement of stakeholders, by convening fintechs, banks and consumer-interest groups and creating safe spaces for discussion and experimentation, is key. Temenos’ Goyal credits Australia’s ACCC with working closely with Data61 (the data sciences arm of the Commonwealth Scientific and Industrial Research Organization, Australia’s national science agency) and the banks to ensure implementation of the CDR is secure and scalable. “They’re building an ecosystem together rather than each party working in its silo.”

National Australia Bank has suggested that the Australia government could release an open source app with the aim of helping educate users. It could, for example, aggregate account balances for different banks. Coming from the government or government organization, customers would be likely to trust it and would learn not only about the benefits of having access to multiple accounts across different institutions, but also about what it actually means to provide consent. By making it open source, others could build something similar.

Despite, or perhaps because of, the range of approaches taken by regulators, there is still no clear overall best practice. “We don’t necessarily have a market to point to and say, this is the way to do it,” says Standard Chartered Bank’s Lloret. “I would look at the best practices across the different jurisdictions. But one thing that would tend to work better is to do hand-in-hand initiatives between the regulator and the industry, rather than a top-down approach that is imposed on the industry without much of a dialogue.”



For governments trying to promote open banking, engagement of stakeholders, by convening fintechs, banks and consumer-interest groups and creating safe spaces for discussion and experimentation, is key.



6 Looking forward

Looking forward, there is substantial momentum behind open banking, fueled by the confluence of technology, demand, competition, regulatory and policy drivers. This momentum will only continue if the industry participants see the benefits and capitalize on the shared opportunity presented by open banking. To enable industry participants, including regulated financial institutions, to do so, it would be helpful for regulators to minimize impediments, such as additional compliance burden or risk, and maximize clarity.

Perspectives on the future of open banking in Asia

Many believe open banking is entering into a new phase. "Phase 1 has been banks opening up their data to the market," DirectID's Varga says. "Phase 2 will be the consumption of data. Data is only data, it's what you do with it that counts." So while initially the focus was on 'reading data' — aggregating accounts and neobanking — now it's about writing data, he says. Banks are shifting from focusing on being compliant with PSD2 and other mandatory regimes to a proactive stance. This is a shift, our interviewees said, both of strategy and product. "We've now seen a much stronger pivot to a wider range of products and services, including payment innovation," says Accenture's McFarlane, "that really benefits small business and small corporates." Banks are now trying to assess and understand customer demand, and importantly generate a return on their compliance investment. This is particularly the case in the UK and Europe, where there are relatively mature regulations. The banks that thrive will be those which provide products and services to customers that they actually want, and that add value to their daily lives, says McFarlane. "Those will be the banks that will succeed and the ones that don't will really be struggling and scrapping for the rest and then trying to compete with hungry competitors."

All financial services providers will need to make the decision — "Am I going to be the primary platform, the interface with the customer, or will I be one step away from the customer?" says API strategy consultant Scheele. "This is not always binary." Financial institutions have an opportunity to broaden how they distribute their products, he says, pointing to how niche players may choose to make their service "plug and play" in someone else's ecosystem. Payments firm Stripe's product is an API that grants access to their payments service. Robo-advisor Bambu publishes APIs to enable banks to white-label its robo-advice service into their own customer offering. This approach is not exclusive to startups. Insurance giant AXA has developed its insurance-as-a-service model by publishing APIs allowing third parties to offer real-time protection to their customers from within their own app or site.

One approach, says Peers of Reponsible Risk Ltd, is to become a platform player, where the bank sits at the center of an ecosystem it builds itself. He points to Royal Bank of Scotland in the UK, which established a ventures business to build independent platforms, such as NatWest Tyl for merchant acquisition and Esme for digital lending to SMEs.

Another option — to take a more white-label approach — is one already being adopted by some of the larger fintechs. TransferWise, for example, has its own consumer product, recently launching in Singapore, but has also allowed neobanks like Monzo to use it for foreign exchange. It recently signed up with Novo, a U.S. banking startup, and the Stanford Credit Union, a bank serving students and staff at Stanford University, to allow them to provide international payments under their own brands and within their own apps.

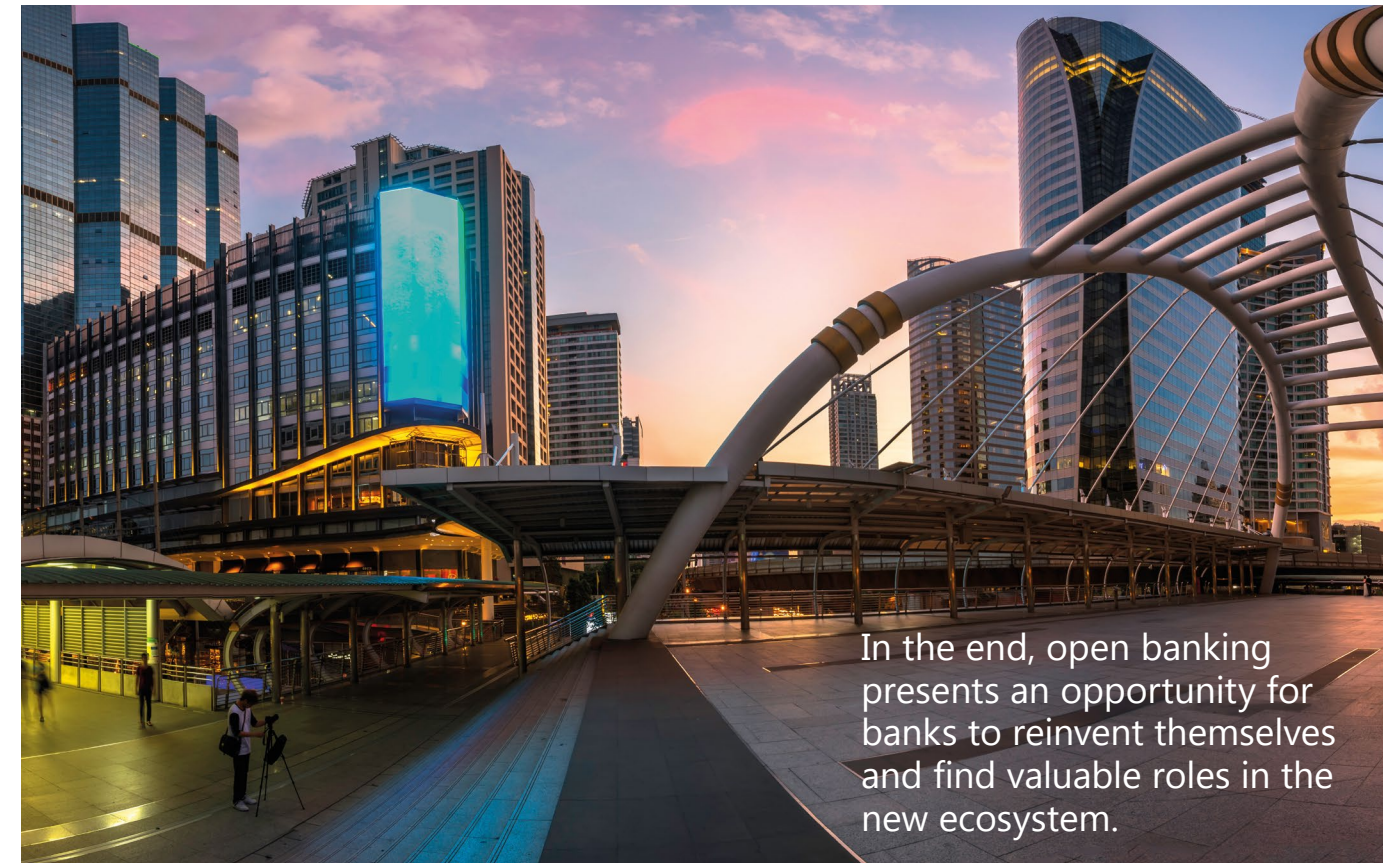
Banks are shifting from focusing on being compliant with PSD2 and other mandatory regimes to a proactive stance.

"A re-definition of role may not be a bad thing for banks," says Temenos' Goyal. Presently banks are both manufacturers of the product and distributor of those products. These functions, she says, will evolve in the future, as niche fintechs will start coming into the market and causing banks to lose that foothold. She adds, "I believe banks may choose to be either manufacturers of product or a distribution network to their customers. Today we are seeing fintechs owning the customer experience, like aggregator services, on a path to becoming the Amazon of banking."

BNY Mellon's Brown sees it slightly differently. "I don't think there's a wariness [among banks with respect to open banking]," he says. "Where the challenge is, is that different organizations are at different stages in their own digital journey." As Mastercard's Nimtschek says, "Open banking won't take off overnight, it will develop in phases. Industry participants will learn from other examples, try out new services and adjust over time... Innovation is important. But to make open banking work, you also need to build customers' trust, make them feel empowered, and ensure inclusion of the parts of Asia that are still largely unbanked or underbanked."

In the end, as Standard Chartered's Gatiganti says, "Open banking offers a great opportunity to expand and go after untapped use cases and customers through creating platforms, partnerships and ecosystems." From his time in the telecommunications industry BNY Mellon's Brown recalls the dire predictions of how big players like British Telecom would disappear. "Just like the fixed line telcos didn't know what would happen with the advent of mobile, or the car companies didn't know what would happen with Tesla's entry," he says, "if we look back, any disruption in an industry gives rise to new opportunities, new paradigms and new ways of creating value."

Microsoft's Leung is similarly optimistic: "The good news is that regulations are opening up to drive industry innovation; banks are considering different roles in the ecosystem; and technology such as cloud, data, AI and advanced security are available. The key is that end customers are already benefiting and participants are already adding value. Collaboration will be across industries, as we have seen already between retail and banking, and health and insurance, for example. I believe what we are seeing in open banking in Asia is just the beginning, with more to come in new business models and new partnerships."



In the end, open banking presents an opportunity for banks to reinvent themselves and find valuable roles in the new ecosystem.

Recommendations for industry and regulators

In this paper we looked at the uptake of open banking to date, the technology, demand, competition, and regulatory and policy drivers behind it, and the various challenges and opportunities for financial institutions and regulators. From this we can derive recommendations for regulators and financial institutions to ensure the successful future adoption of open banking:

Financial Institutions

- ✓ Take a phased approach, starting by gradually replacing legacy infrastructure and ensuring technical scalability to support open banking
- ✓ Test-run open banking through pilots or sandboxes
- ✓ Effect cultural change: consider establishing a team focused on digital transformation
- ✓ Be transparent with customers about security and privacy measures
- ✓ Leverage your competitive advantages: customer trust and experience with regulatory compliance
- ✓ Consider new partnerships and collaborations
- ✓ Identify the value proposition for your business and seize the opportunity

Regulators

- ✓ Provide clarity regarding the regulatory stance towards open banking
- ✓ Ensure financial institutions do not see open banking as a mere compliance exercise or something that increases their compliance burden
- ✓ Avoid overly prescriptive mandates, which could become outdated as technology advances and which could limit innovation
- ✓ Consider what entity will oversee open banking and take a coordinated approach across government
- ✓ Stay in step with industry readiness
- ✓ Use pilots and sandboxes to develop the open banking regulatory approach with industry
- ✓ Consider the scope of data covered, reciprocity, and standardization
- ✓ Avoid restrictions on cross-border data flows
- ✓ Leverage existing regulatory frameworks
- ✓ Establish a framework for third party provider accountability
- ✓ Work with other regulators towards greater harmonization and avoidance of conflicting compliance obligations

Most importantly, to realize the shared opportunity of open banking, all participants – including banks, fintechs, TPPs, regulators, technology companies and customers – will need to engage and share learnings as they embark on the journey together.

Interviewees

The authors would like to thank the following interviewees who contributed to this paper:

- Andrew McFarlane** – Global Open Banking Lead, Accenture
- Connie Leung** – Senior Director, Asia Financial Services Business Lead, Microsoft
- Graham Dickens** – Chief Technology Officer, Judo Bank
- Hans Brown** – Managing Director, Global Head of Innovation, Bank of New York Mellon
- James Varga** – CEO, Founder, DirectID
- Jochen Nimtschek** – Vice President, Digital and Emerging Partnerships, Mastercard
- Jon Scheele** – API Strategy Consultant
- Ludovic Blanquet** – Global Head of Product Strategy and Portfolio, Finastra
- Rama Gatiganti** – Head of Technology Strategy and Standards, Standard Chartered Bank
- Richard Peers** – Founder, Responsible Risk Ltd
- Rohini Goyal** – APAC Digital Strategist, Temenos
- Sophie Lloret** – Head of Regulatory Change, Technology and Innovation, Standard Chartered Bank
- Steve Day** – Executive General Manager, Infrastructure, Cloud and Technology, National Australia Bank



