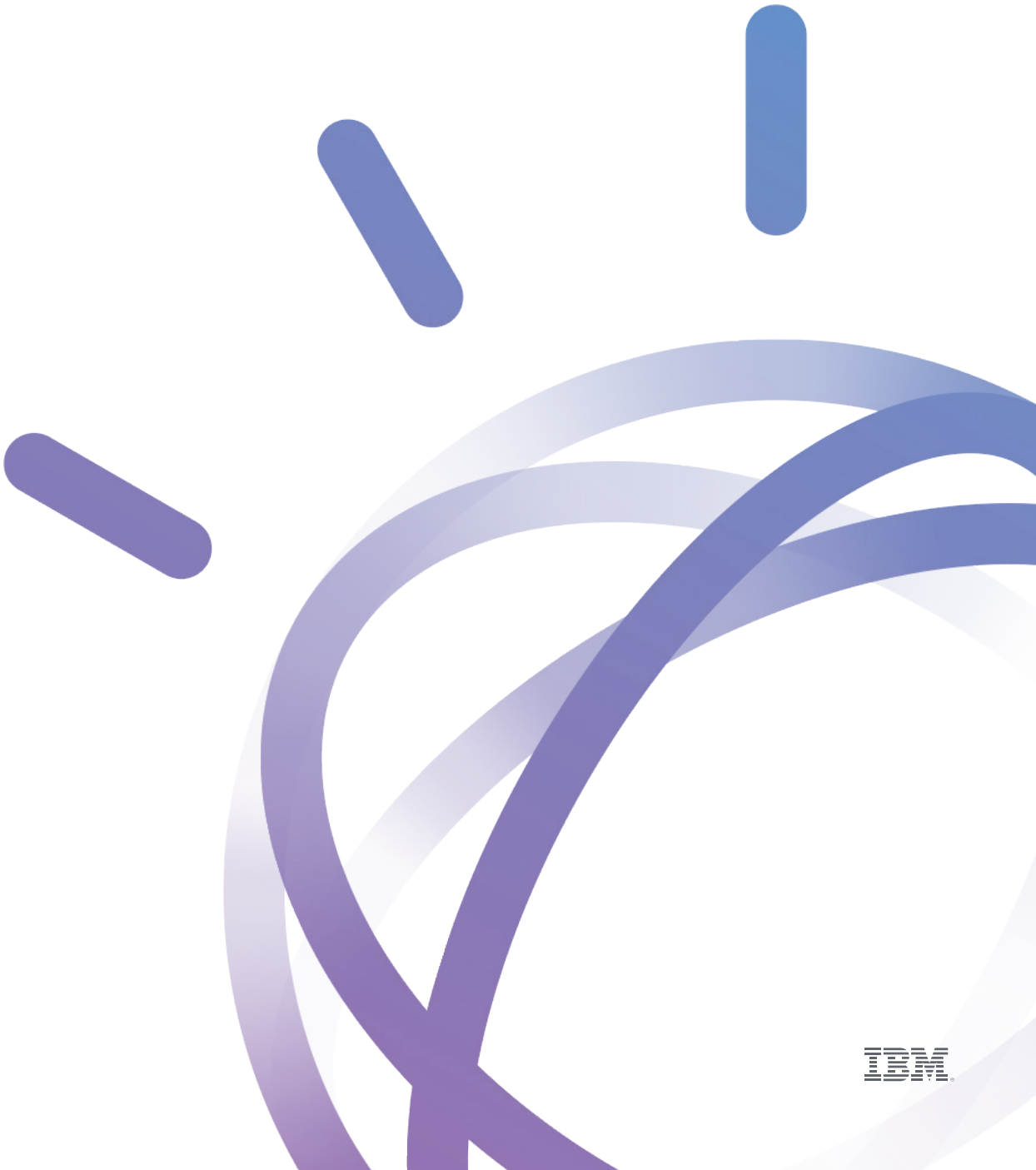
White
Paper

Unpacking the Open Banking black box



Watson Financial Services

IBM

Contents

A banking revolution - Open Banking

In today's dynamic business environment, banking regulators are taking steps to intervene in disruptive ways to drive greater access and transparency to customer information in an attempt to stimulate competition and innovation, for a more customer centric banking experience. Where banks previously had exclusive access to their customer's information, new regulation dictates much of that information must be made available to external parties via digital channels. By forcing incumbent banks to break their monopoly access on payment mechanisms – startups, aggregators and other sectors are empowered to improve customer service, lower costs and develop more innovative technology.

In the European Union, the Payments Services Directive 2 (PSD2) requires banks to open access to their back-end services for account information and payment initiation to third parties through application programming interfaces (APIs). In the UK the Competition and Money Authority (CMA) has driven a similar agenda requiring the nine largest banks in the UK to open access to all payment's accounts. Concurrently with this opening up of access to customer information, the EU has introduced data privacy legislation (GDPR) governing consumer rights in directing how customer information may be used, and in providing guidelines on how customer information must be safeguarded.

What is Open Banking?

Open Banking is the provision of third-party access to customer and account information through the use of APIs. Customers, as the owners of their information held by financial institutions in a custodial capacity, are able to direct those institutions to make their information available to other parties. In Australia, the government recently announced its adoption of recommendations from the Farrell Report which proposed similar opening up of banking data, but with a broader scope than that embraced through PSD2. Underpinning Open Banking in Australia, the government established the Consumer Data Right (CDR) which formally gives consumers ownership of their data and provides them with the means to direct its use, in a seamless, simple and secure manner. This will fundamentally remove many of the inherent barriers to moving accounts and facilities between financial institutions – in effect removing friction in much the same way number portability did in the telecommunications industry. Similarly, Open Banking as a disruptor will test the customer value proposition, by bringing to light what consumers are truly demanding. As a result, this will inevitably have a flow on impact for consumer spending and consumption behavior.

"The challenge for banks isn't becoming "digital" - it's providing value that is perceived to be in line with the cost - or better yet, providing value that consumers are comfortable paying for."

Ron Shevlin

Ron Shevlin is currently director of research at Cornerstone advisors, where his research focuses on retail banking products and services.

The net effect of this will be to make access to information, previously only available through bank channels, available for accredited third parties, should the customer choose to do so. In some cases, this is already done by information aggregators (such as personal financial management tool providers) who use screen scraping technologies and rely on the customer sharing their internet banking access credentials. However, consumer security concerns are constraining the uptake of this approach. Provision of a safe and secure mechanism for consumers to dictate what data is shared, who that data is shared with, and the duration of the sharing arrangement, is likely to drive a significant adoption uplift. The provision of this information needs to be done in a means that ensures full consent awareness and protects customer privacy as information transits between many potential organizations. In this new environment, consent must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.

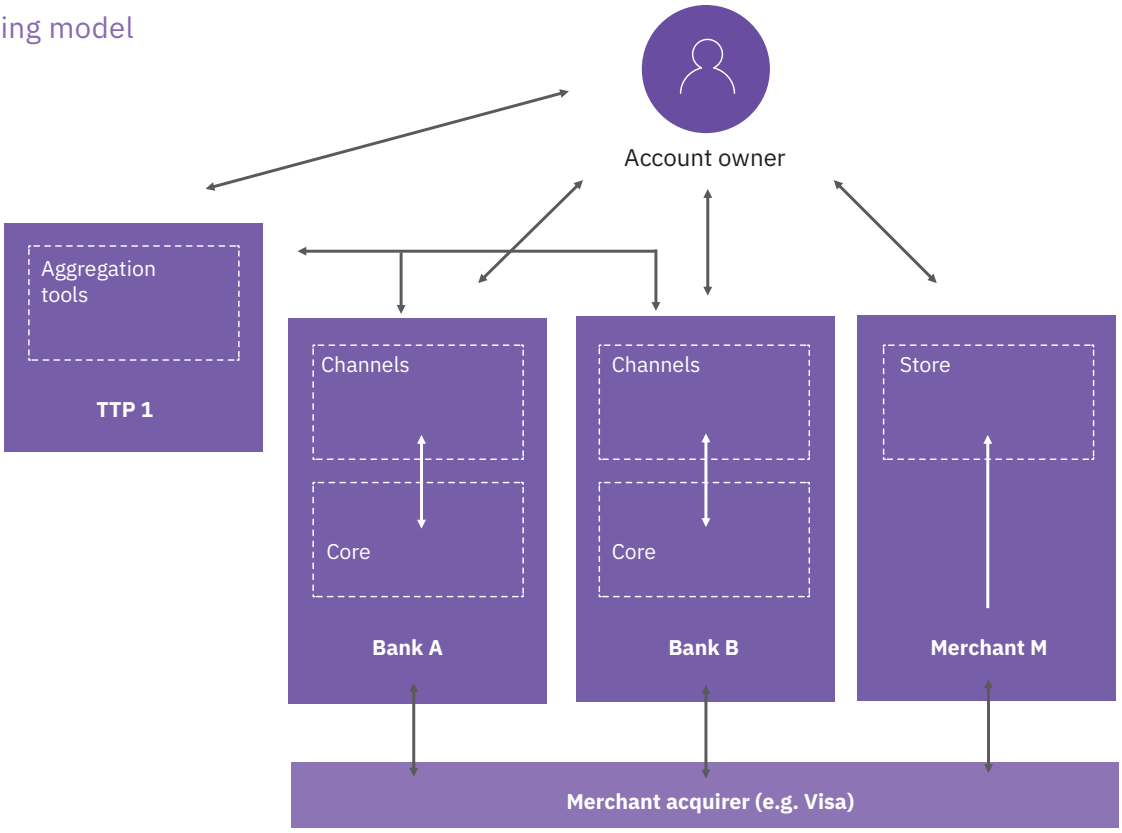
The Farrell report includes no specific recommendations on privacy or security. These standards are to be developed by Data61, an arm of the CSIRO. However, standards definitions have not been finalized in Australia. There may be similarities and lessons to be learned from the UK challenges and approach.

The scope of Open Banking

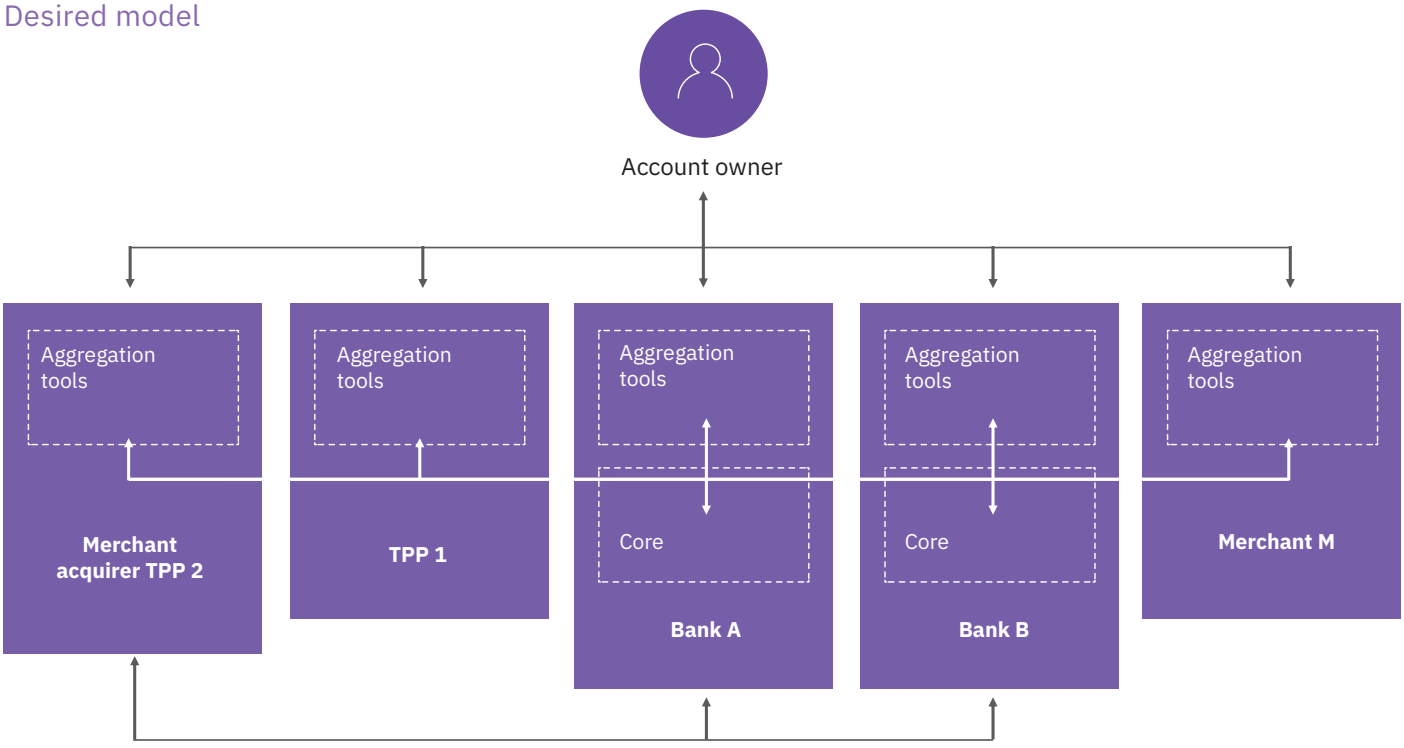
Open Banking allows external parties to access customer and account information through industry standard APIs. Through these APIs external parties can transact directly with a bank's core systems without being mediated through the bank's existing channels.

The EU and UK markets have focused on providing account information and payment initiation for payments capable accounts. The Australian approach gives a broader context, providing enquiry only capabilities, but encompasses a broader range of deposit and lending products, across all banking segments. The intent is to enforce sharing of a broader set of customer and account information, with a greater emphasis on inquiry capabilities than the payments agenda. The prescribed timeline for the Australian implementation of Open Banking requires transaction, savings and credit card accounts to be available by early 2020, with mortgages and personal loans by early 2021. Initial testing is required from mid 2019.

Existing model



Desired model



The Farrell Report has recommended that Open Banking include:

Deposit products

- Savings accounts
- Call accounts
- Term deposits
- Current accounts
- Cheque accounts
- Debit card accounts
- Transactional accounts
- Personal basic accounts
- GST and tax accounts
- Cash management accounts
- Farm management deposits
- Pensioner deeming accounts
- Mortgage offset accounts
- Trust accounts
- Retirement savings accounts
- Foreign currency accounts

Lending products

- Mortgages
- Business finance
- Personal loans
- Lines of credit (personal and business)
- Overdrafts (personal and business)
- Consumer leases
- Credit and charge cards (personal and business)
- Asset finance (and leases)

Key challenges and lessons for Australia

There are a number of issues the regulators and market participants will need to be mindful of, if Open Banking regulation is to deliver marketplace outcomes, and not create significant incremental systemic cost to the banking sector.

Establishing standards from the outset that help the consumer and market participants

Facing the pressure to deliver to a regulatory deadline, and absent clear standards for how authentication and authorization were to be implemented, each of the nine banks involved in the initial UK implementation ended up with subtly different solutions that all met the broad technical standard. While sharing a common token-based framework, the specific integration required for a third-party organization to ingrate with each of the nine banks participating in the UK implementation varies. Furthermore, the current standards have generated an awkward customer experience for account authentication, where customers are passed back and forth between each third party and the financial institution, for every instance a customer wishes to initiate a new sharing arrangement. The UK implementation allows authorizations for ninety days which requires customers to repeat this process four times per year. Whilst this may be an effective mitigate to idle authorizations, it may not deliver the most functional solution for consumers who may be using third parties for ongoing activities, whether as individuals or in the context of a business.

In addition, the varied implementations of customer account authorizations across banks means that every third-party wishing to exploit Open Banking must implement the authorization mechanisms for each of the banks (in this case - nine sets of customized code). An improved approach is planned for 2019 which should improve the consumer experience, though the diversity of implementation is likely to remain an issue for the foreseeable future.

As Australia considers its approach to Open Banking, early and thorough engagement with market participants should be an essential element to ensure standards address concerns from all stakeholders and to secure shared commitment on the implementation approaches.

Use of regulatory levers to encourage API adoption

Introducing new mechanisms, which require investment from all participants, make sense where these enable innovation or offer a benefit to industry. The UK model to require the nine largest banks to support Open Banking placed a demand on the 'supply' side of this endeavor but as of writing this only thirty-nine third parties have signed up to embrace and leverage the Open Banking APIs to enable solutions. Arguably, this is a significant investment for a relatively small adoption.

A key lesson however, can be derived through the topic of 'screen scraping' solutions. Today a number of third- party aggregators provide functionality to consumers, that rely on the consumer to input their internet banking credentials into the aggregation solution, which then digitally impersonates them. This exposes consumers to fraud and privacy related risks, but it is also an impost on the banks.

The UK implementation initially envisaged mandating that third parties would need to leverage Open Banking and that banks would be allowed to turn off access to screen scraping aggregators. A combination of factors have led to the sentiment that this may not be possible. This leaves banks open to the risk of having to build Open Banking APIs, while simultaneously being unable to minimize the continued use of screen scraping tools. Ultimately, this places a burden on the banks, given there will be no reciprocated demand from third parties.

Architectural alignment within the banks

Historically, banks have invested heavily to build up digital self-service channels and done so with a new parallel infrastructure to existing legacy channels. This proliferation of solutions has contributed to the embedded complexity and structural cost within the business.

To avoid continued growth in systemic cost, it will be important that banks are able to respond to Open Banking demands and simultaneously address the above concerns. While the intent might be that over time, the security and access control mechanisms employed to enable Open Banking will converge with those employed in other channels, the UK experience has been to deploy new mechanisms with limited retirement of traditional bank channels.

The security constructs often found within the online corporate banking solutions use sophisticated token-based mechanisms to provide multiple user access to multiple accounts with the purpose of executing a range of activities. The demands of these environments will have significant overlaps with the requirements of Open Banking, especially as this encompasses business and corporate banking.

The challenge of digital Identity' is also relevant in this discussion. Many banks have fragmented 'customer information' across the customer segment continuum. If Open Banking standards mandate common ways of addressing resolution of, and access to, customer and account information, then it is likely that some degree of alignment will be required with the underlying customer, relationships and access control information within a bank's systems environment. This may have unintended consequences for a bank's internal IT landscape driving significant cost which will demand market participant consultation.

Workload impacts on bank IT infrastructures

The impact of Open Banking on the workloads of banks' core IT systems is yet to be understood and the limited adoption to-date in the UK does not drive sufficient volume increases to have a material adverse impact. However, some early indicators have been seen.

New workload will largely fall into three categories:

- Existing customer interactive driven workloads, such as online banking with aggregated data, or new propositions driven by aggregated data (for example home buying);
- New customer interactions enabled by offline generated insight – for example, cross institution sweeping and pooling; and
- Background activities to keep customer information current and/or to drive new customer insights.

The first two types of workload will likely drive some increase in workloads of banks' core systems. However, these will mostly be driven by consumer activity and therefore already within the workload forecasting envelope attached to online banking or mobile banking channels.

The third however is net new workload and one that is driven through systems and automation. IBM modelling of potential impact on the UK banks suggests that an uplift of over 60% to core system workloads resulting from third party solutions 'polling' activities is plausible. However, the story is more complex. The UK model limits third parties to four enquiries per day (by enquiry or account) without the consumer present. Unless the workload generated by third parties is spread in a uniform workload to each bank, then these polling enquiries will likely arrive in concurrent spikes.

This will place enormous workload on the banks' core banking platforms, with potentially adverse implications to the performance of those platforms. Ultimately, any response to this issue will likely drive structural cost increases into each of the banks.

The role of digital identity

The Open Banking specifications today focus on facilitating access to customer accounts. However, there is no construct within the standards addressing the customer's identity, or their relationship with the account. It ensures that the customer has technical access to the account, not who they are

When providing access to customer account information, an issue which will be of consideration to all banks, will be the relationship of the individual to the account. Critically this new mechanism of access will also co-exist alongside the banks' existing customer relationship and account access controls.

Consider the following scenarios:

- A customer wishes to grant access to the third party to all or some of their account – will this be a repetitive process on an account by account basis as is the case with the UK implementation?
- A customer on a joint account wishes to grant access to a third party – should the account co- owner also need to grant access?
- An employee will use a third-party application to manage business finances (a common use case in corporate banking) – who grants the access and ensures that it is for the specific employee only?

Another facet to consider is the Authorization Model. This model can also be problematic in an industry where account access is granted for the purposes of verifying critical information pertinent to credit decisions. Consider a circumstance where 'access' is granted to check accounts for income verification or other debt serviceability checks. How can the requesting entity satisfy itself that the accounts to which they have been granted access, are actually the accounts of the customer in question and what responsibility, if any, does the account holding bank have in this process?

While the initial focus in Australia will be for enquiry only transactions, the ability to post transactions is on the future roadmap and so addressing these challenges beyond the immediate requirement will be essential.

Who pays for usage?

Ultimately the costs of running a bank is manifested in the profit line. In many instances fees and charges to consumers have been dispensed with by banks, as consumers push back on being charged for 'accessing their money.'

It is plausible that banks may allow consumers a notional threshold of authorized externally generated transactions within the envelope of the customer relationship. Banks will need to ascertain whether their existing IT portfolio will enable externally triggered workload to be monitored, measured, and attributed back to a customer. Where large volumes of workload are being generated by third parties, resulting in material cost impacts to the banking sector, it is reasonable that banks be compensated for these increased costs, however recent trends on fees and charges suggest consumers will be unwilling to accept these charges.

If banks need to charge third parties a transaction fee for accessing customer and account information, which results in costs, the mechanisms for identifying the requestor, and attributing the operating costs to the Open Banking transaction will need to be considered within the standards.

Perhaps more challenging will be the banks' internal ability to track and charge these fees in a new paradigm. Many bank core systems process fees against the customer based on events directly occurring on the account or triggered by customer activity (e.g., account going overdrawn, number of in-branch transactions per month, use of a specific payment mechanism, etc).

It may be necessary for banks to consider how fees and charges are processed allowing for a range of trigger events and perhaps a range of initiators. Where banks have pursued this course of action it is often referred to as 'hollowing out the core,' externalizing fees and charges functionality from the core banking platforms. This is a highly complex undertaking, requiring significant investment and carrying significant delivery risk.

Unintended consequences

One of the key intents with the UK implementation was to introduce competitive innovation and to break the monopoly the large banks enjoy. The move by the CMA in requiring the nine largest banks to implement Open Banking served a purpose to kickstart the industry activity. However, it may have also triggered some unintended consequences.

As Open Banking is rolled out to the broader industry others are now responding to the need to participate in this new ecosystem. The banks who participated in the initial deployment now enjoy a material head start on the rest of the industry in planning, architecting, and delivering solutions to meet this need.

"If you compare banks to companies like Google, it's evident that banks are still at the nascent stage of the digital and data revolution."

Vik Atal

Atal is a globally-oriented leader in the consumer financial services arena, with three decades of experience.

"If banks cannot truly be customer intimate, they are doomed to be just commodities, acting behind the scenes, like utilities."

JP Nicols
Nicols is the Managing Director of Fintech Forge.

Seize the opportunity - Why banks should embrace Open Banking

IBM® believes that embracing Open Banking offers opportunity for banks who choose to lead. Getting ahead of the curve on embracing and implementing Open Banking can give banks a head-start in their efforts to become more effectively connected into ecosystems which will power future banking offerings. Those who do so will be better positioned to combat the platform businesses such as Alibaba and Tencent whose presence will likely be felt. Left unchecked, these entrants will exploit Open Banking to capture the customer but leave the cost and complexity to incumbent market participants.

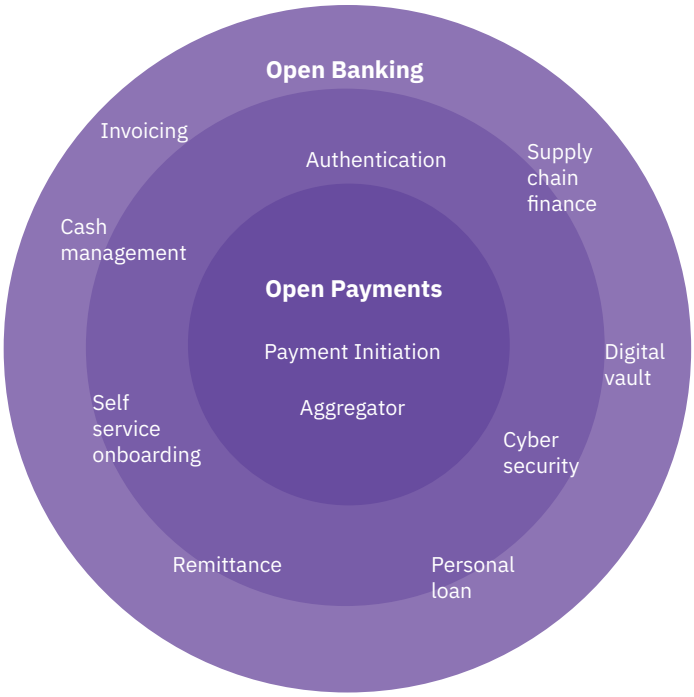
These companies enable customers to satisfy all of their needs, including the banking component, from a single platform. This is not just restricted to payments anymore but covers, for instance, the customer's borrowing or wealth management needs. In this scenario, banks will face their "Kodak" moment - an SME customer for example, that generates surplus cash from a sale made on the Alibaba platform will not have to come off the platform to invest the money in short term money market funds.

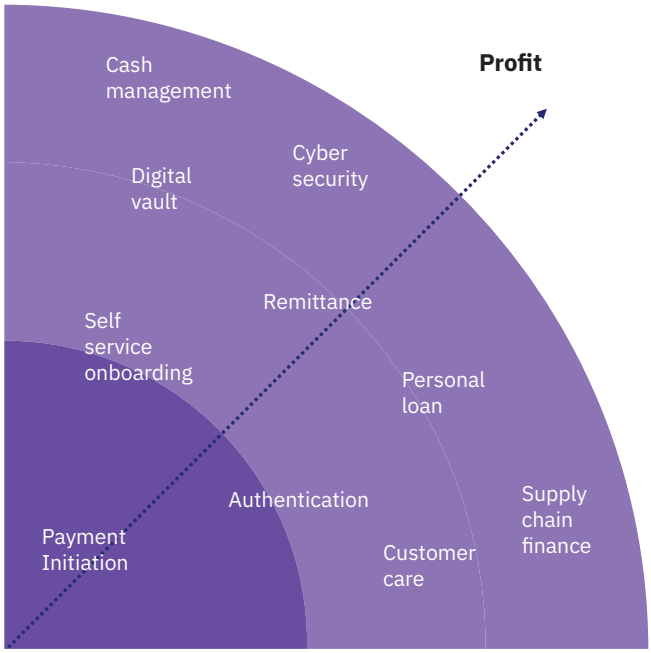
Banks must take a 'beyond banking' approach to compete effectively in this environment and not restrict themselves to just the financial services product. Open Banking will enable them to access ecosystems, for example:

- Help their clients with buying a house, moving and finding schools and not just selling them a mortgage which at best will be a commodity offering.
- Help small businesses setup their business operations including HR, recruitment, accounting and tax services, leasing premises or acquiring assets, while also meeting their cashflow and risk protection needs.

Global examples

The following case studies highlight various ways that financial institutions have exploited Open Banking and the unique offerings they present.





Free of charge services - Fee based services

BBVA

BBVA has created one of the first global, open development platforms for financial services. BBVA's approach to developer enablement encompasses both a suite of banking-as-a-service APIs, and customer data APIs. In the US BBVA's banking-as-a-service platform, BBVA Open Platform, gives third parties access to white-label banking services. Third parties can offer banking services to their customers, regardless of whether those customers are existing BBVA customers, as a native part of their application. An example of their current offerings is an API that can be integrated into a third party app so third parties can open bank accounts for their customers under their own brand.

In Mexico and Spain, BBVA's APIs provide existing BBVA customers greater control over their data via permission-only access for third parties. Customers who opt-in then benefit as those third parties build unique value-added services by accessing and integrating customers' bank data into their applications. An example of their current offerings is an API that can be integrated into the checkout process to allow customers to finance their purchase of a third-party product or service at the point of sales with a BBVA loan. Globally, BBVA's APIs empower companies to deliver better customer experiences by streamlining conversion and on-boarding processes.

A non-traditional European digital bank's banking platform provides B2B solutions in the form of banking as a platform (BAAP) and banking as a service (BAAS). They design, build and run digital banks. These services are delivered through open source APIs to provide banking functions from on-boarding, account management and credit products to analytics. This digital bank has also formed data partnerships with relevant providers that enable both parties to drive digital and mobile banking services. The data provides insights on spending behavior that enables both parties to further strengthen and drive future innovation.

A European fintech with a multi-faceted platform, utilizes API technology to provide a number of value-added services to consumers. Consumers download the application and opt-in for their financial data to be safely and securely shared on the platform. They can view all their accounts from various banks all in a singular location, smart categorization of their transactions, spending insights and take advantage of money management services. Customers are not directly charged for this service, which works as customer acquisition and retention strategy. Customers are incentivized to upsell to premium services, which is where the top line revenues are realized.

A very large Eastern European banking and financial services organization follows a 2020 strategy that aims to leverage a singular all-encompassing ecosystem where multiple niche industry banking services can be provided. Built on the cloud, this platform will leverage APIs, a product factory, process factory and decision support system to deliver an innovative and data driven eco-system. This organization also shares a forward-thinking philosophy where they aim to leverage this innovative infrastructure by creating technology labs in key business areas, such as artificial intelligence, cybersecurity, robotics, robotic process automation (RPA), blockchain, Internet of Things, virtual and augmented reality and machine learning.

"Financial institutions must be able to deliver an easy to navigate, seamless digital platform that goes far beyond a miniaturized online banking offering."

Jim Marous

Marous is currently the co-publisher of The Financial Brand and the publisher of the Digital Banking Report.

How can IBM help?

IBM has supported leading UK banks with their implementations to meet the Open Banking requirements in the UK, in addition to delivering sophisticated microservices based sales and service solutions for banks in Europe and the rest of the world. IBM is also a contributing author to the Banking Industry Architecture Network (BIAN) which is developing standardized industry definitions for APIs and microservices.

Architecture Network (BIAN) which is developing standardized industry definitions for APIs and microservices.

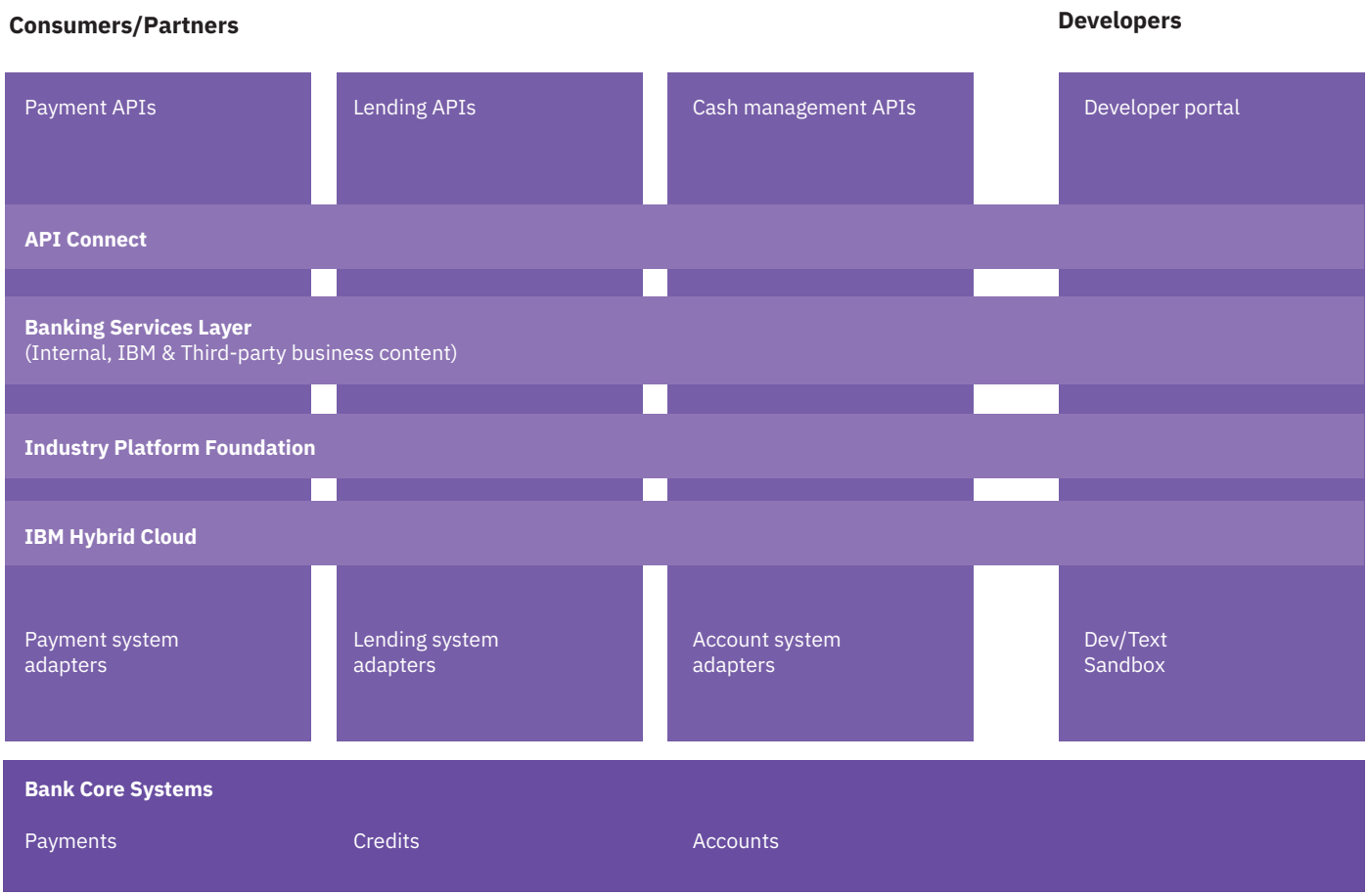
- Long standing trusted technology partner to Tier 1 banks
- Depth and breadth of financial services industry experience, including regulatory with promontory extensive expertise in both legacy systems and emerging technologies
- Secure and scalable platform, based on IBM's hybrid cloud strategy
- Defining industry API standards with BIAN
- Expanding catalogue of partner FinTechs with plug and play capability

IBM can support you with advisory services including:

- Open Banking readiness reviews
- Open Banking IT architecture review and planning
- API and microservices enablement maturity assessments, planning and design
- Cyber security model assessments, planning and design

In addition, IBM has prebuilt assets to accelerate your development of Open Banking capabilities including:

- A full implementation of the OBIE Open Banking specifications including choreographed security implementations for token-based authorization
- A cloud chassis implementation for functional and channel handling microservices which are pre-verified to operate across all major cloud providers including IBM, Amazon Web Services, Google Cloud and Microsoft Azure.



IBM Open Banking Platform

In considering an approach for responding to Open Banking, organizations should consider the overall solution architecture underpinning the sales and service capabilities. In many ways Open Banking is another channel; one that will look more like an ecosystem than a proprietary channel, but with common underlying constructs required to service the demands of Open Banking.

Powered by IBM advanced technologies including IBM CloudTM, IBM API Connect® and IBM Watson®, the IBM Open Banking Platform also includes an ecosystem that contains APIs from IBM Financial Services and third-party Fintechs, enabling financial institutions to rapidly and securely build next-generation apps.

Harnessing APIs is essential for success in the Open Banking era. In addition to monetizing your core capabilities through APIs, your bank can use IBM and Fintech partner APIs to add capabilities such as financial risk assessment, payments, artificial intelligence (AI) and blockchain to your apps. Powering analytics with AI can help you leverage the gold mine of account data you possess to distill powerful insights that improve banking functions and point the way to new digital products and services.

IBM has developed a reference architecture illustrated here, with further detail outlined in the Appendix.

Features at a glance

Key features and attributes of the IBM Open Banking Platform solution include:

- Hybrid solution built on Kubernetes with options to run on premises or in the cloud
- Business domain powered by the Banking Industry Architecture Network (BIAN), Information FrameWork (IFW) and other Open Banking standards
- Full-stack solution that spans from core systems to cloud
- Access to a modular microservices layer on top of your existing systems
- Modular Open Banking Platform packages with plug-and-play design
- Access to a curated Fintech catalog of potential partners
- Capabilities for accelerating digital transformation
- Available IBM expertise on both legacy systems and emerging technologies

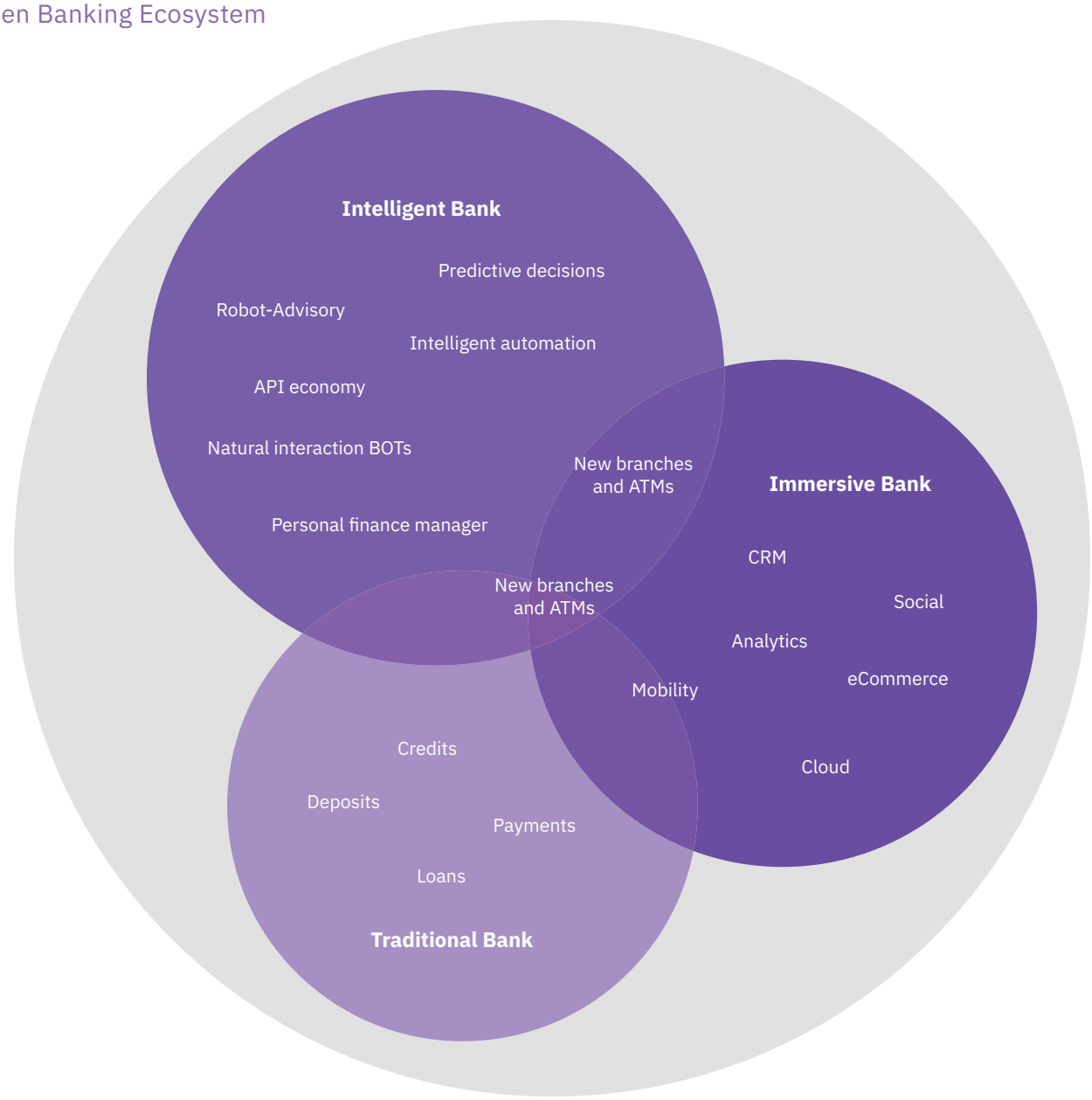
The right partner for a changing world

At IBM Global Business Services, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment. Through our integrated approach to business design and execution, we help turn strategies into action. Moreover, with expertise in seventeen industries and global capabilities that span 170 countries, we can help clients anticipate change and profit from new opportunities.

That said, Open banking is here to stay and it's changing the way financial institutions operate. The IBM Open Banking Platform helps financial institutions bridge from core systems to the cloud, so you can revitalize, not rip and replace. We enable collaboration between industry leaders and emerging Fintechs, so you can build a wider ecosystem and establish new revenue streams.

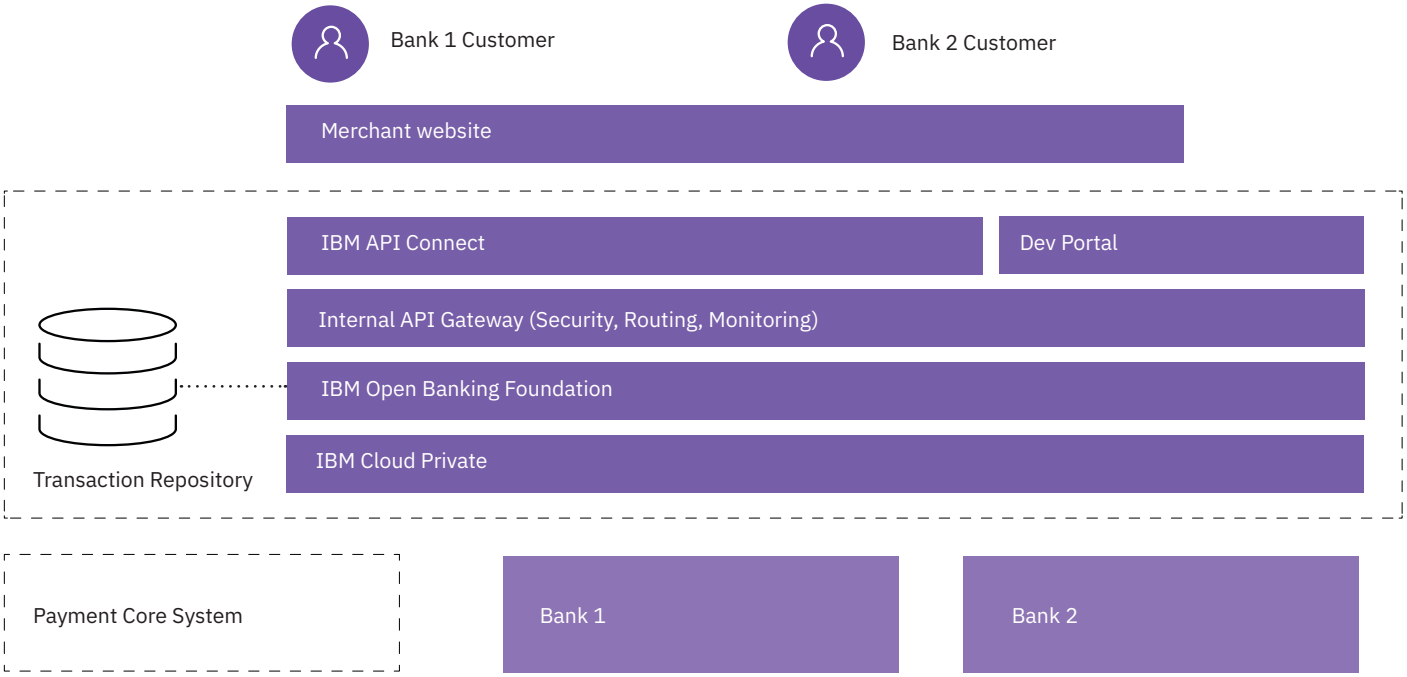
The future of banking reaches far beyond creating the next mobile banking app. With the IBM Open Banking Platform, you can move forward with confidence not only to fulfil your digital transformation objectives, but also to help reimagine the architecture that supports the world's financial transactions.

Open Banking Ecosystem



Appendix

Deep dive – IBM Open Banking Reference Architecture:



Key elements of this reference architecture for consideration include:

A functional micro-service layer to provide digital banking services

Regardless of whether customers are accessing banking information and services through a proprietary channel or through external ecosystem and Open Banking APIs, they will be executing common functions to access this information or post transactions.

Early experience in the UK suggests that enquiry volumes will far outstrip updates, which will also likely be the case in Australia, at least initially. IBM analysis of the UK implementation suggests enquiry workloads could be up to 60% higher than what is currently being experienced, which would drive a substantial uplift in processing of the Systems of Record (often located on mainframes), if this workload is passed through to the core banking platforms. For this reason, enquiries should be serviced via microservices through an Operational Data Store to which core information is replicated. Updated transactions will be posted through to the core banking platforms

Specific Open Banking API implementation

Sitting atop the functional microservices which provide the functionality are a specific set of services which implement the Open Banking API specifications and are required to support Open Banking. Importantly, these APIs will support the choreography of the authentication protocols, which the standards are specific for how third parties request, and are granted, access to customer and account information. They will also handle the specific implementation of the APIs data structures and translate these into the calls to the functional microservice layer.

Other external channel API implementations

Where other external ecosystems are being supported, but not using the Open Banking APIs set, then the patterns can be re-used to implement additional API frameworks to expose banking services to those ecosystems. It is likely that the APIs set to support additional external parties will be different to the Open Banking APIs, as they will support specific functions which are unique to the ecosystems they support.

Proprietary channel rendering support

In parallel to the external channel, and also sitting atop the functional microservices functionality, user experience microservices will support the bank's own internet banking, mobile banking, staff assisted, and other channels. These microservices will build upon the underlying functional microservices to ensure that a consistent omnichannel experience is provided to the bank's customers.

A cloud native implementation

The above elements (microservices, external channel APIs, and proprietary channel rendering) will need to be both highly resilient and able to support elasticity in capacity. Meeting this demand implies that these capabilities will need to be serviced through a cloud-based infrastructure. The external and proprietary channel handling would likely be supported in a public cloud environment. However, institutions will have varying perspectives on whether the functional microservices should be hosted in public cloud or a private cloud environment.

Authors

Alex Cuthbert
Business Transformation Consultant & Open Banking Corporate Strategy Expert
IBM Global Business Services, Australia

Tom Eck
Global CTO for Industry Platforms
IBM Global Business Services, US

Paul Lucas
Executive IT Architect & CTO for Payments, PSD2 and Open Banking
IBM Global Business Services, UK

Rakesh Shinde
Chief Integration Architect
IBM India

Mark Allaby
Managing Partner - Banks & Financial Services
IBM Global Business Services, Australia

Designer
Isabella Purchas
Visual & User Experience Designer
IBM Global Business Services, Australia

About IBM Watson Financial Services

IBM works with organizations across the financial services industry to use IBM Cloud™, cognitive, big data, RegTech and blockchain technology to address their business challenges. Watson™ Financial Services merges the cognitive capabilities of IBM Watson® and the expertise of Promontory Financial Group, an IBM company, to help risk and compliance professionals make better-informed decisions to manage risk and compliance processes. These processes range from regulatory change management to specific compliance processes, such as anti-money laundering, know your customer, conduct surveillance and stress testing.

For more information

To explore how to accelerate digital transformation with the IBM Open Banking Platform visit the IBM Open Banking page at: ibm.com/industries/banking-financial-markets/openbanking

ABN 79 000 024 733

Watson Financial Services