MONOCLE

OPEN BANKING: DISRUPTION OR DISTRACTION?

Monocle Research Team

2020

Open banking is growing rapidly throughout Europe and the United Kingdom, and industry commentators are predicting that it will soon disrupt the banking industry globally. In an open banking environment, financial institutions provide third-party organisations – such as FinTechs – access to their customers' data, with the explicit authorisation of the customer to do so.

This open exchange of customer data is highly beneficial for third parties, enabling these businesses to improve access to their specialised offerings and grow their presence in the banking market. However, the fundamental nature of open banking poses a threat to a key competitive advantage traditionally held by banks – the control of customer data. As a result of this, banks' participation in an open banking environment has thus far been driven by regulators compelling them to share customer data with third parties and customers putting pressure on banks to offer more advanced products and services.

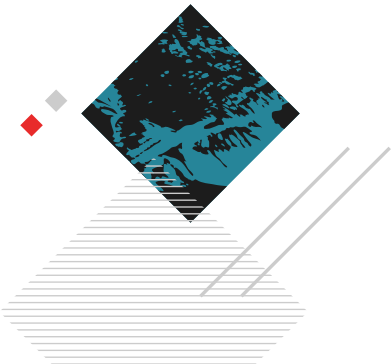
Currently, open banking regulations have not been implemented in South Africa. However, given the rapid growth in open banking in other parts of the world, it is becoming increasingly important for banks to consider the implications of this trend and prepare themselves for it as a part of their digital strategies. Banking will be the first industry to face disruption, however, the trend is set to expand to other data intensive sectors such as insurance and telecommunications.

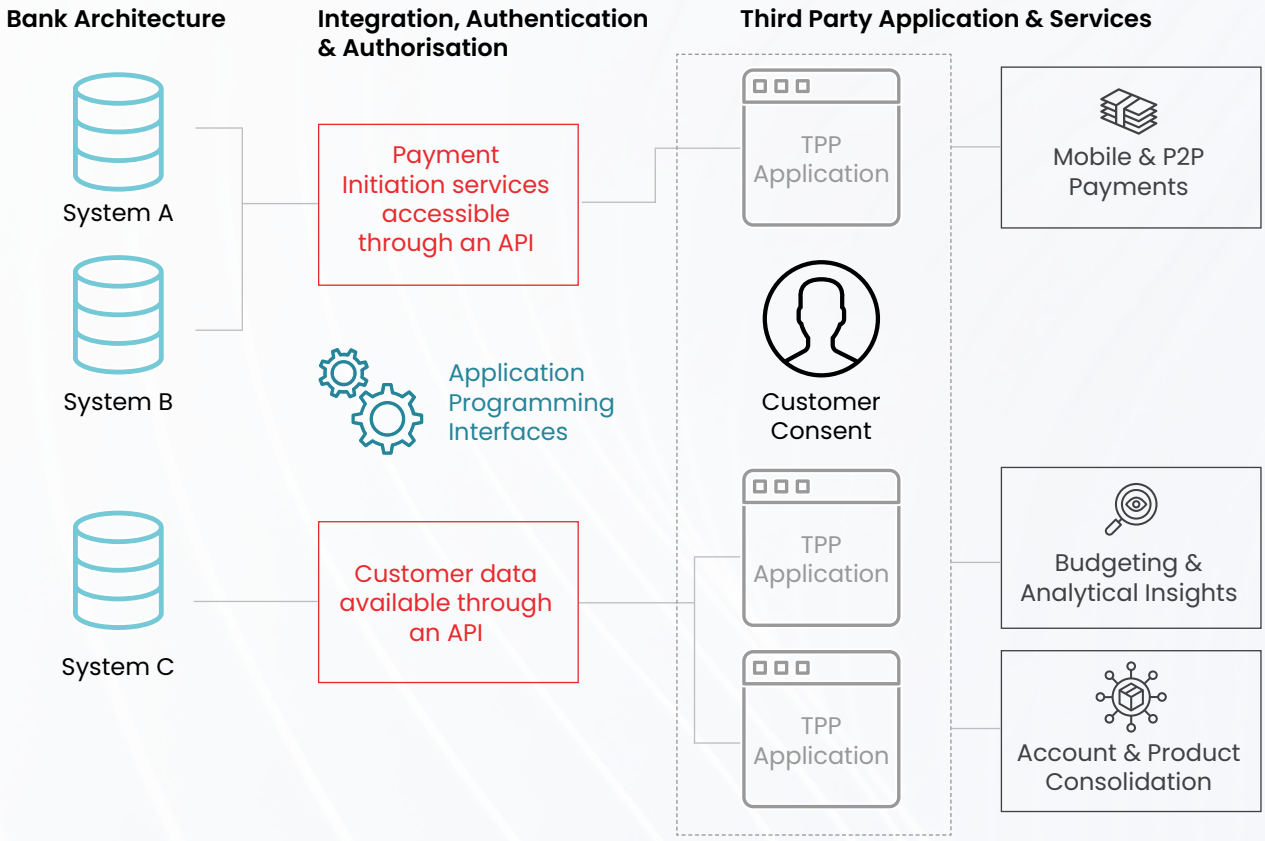
> **It is becoming increasingly important for banks to consider the implications of this trend and prepare themselves for it as a part of their digital strategies.**

WHAT IS OPEN BANKING?

Open banking essentially enables third party providers (TPPs) to access the banking and financial data of banking clients and to initiate payments into or out of a user's account. This is done with the authorisation of the client to do so.

TPPs are able to build applications on top of a bank's existing systems as open banking is facilitated by **Application Programming Interfaces (APIs)**, which provide real-time secure access to customer data. APIs are a set of codes and protocols that determine how different applications and systems interact with one another. An API bridges the gap between a bank's established databases and core systems, and other financial institutions and third-party applications. Critically, APIs provide a secure gateway through which TPPs can access customer data within a bank's systems, ensuring the open flow of data and payment initiation.





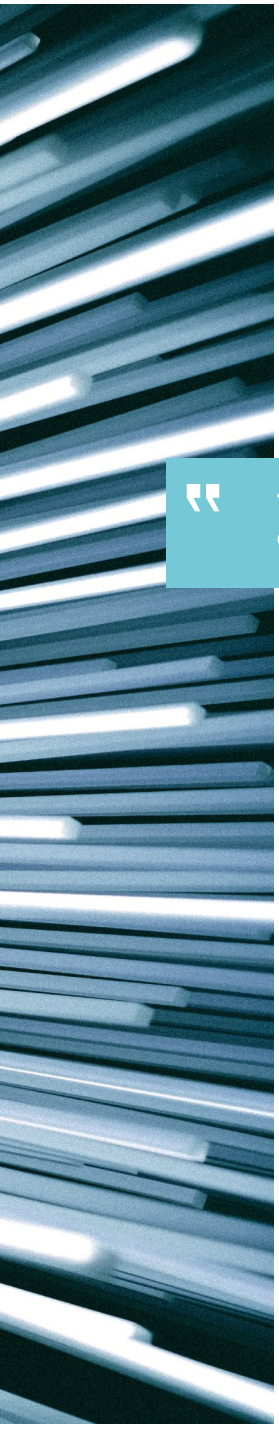
The structure of the open banking environment creates two distinct third parties: **Account Information Service Providers (AISPs)** and **Payment Initiation Service Providers (PISPs)**. AISPs are TPPs that are authorised to retrieve account data from banks and financial institutions with consent from the account holder. **These third parties are able to provide a consolidated view of all a customer's accounts, as well as money management, product comparison and advance analytics functionalities.**

PISPs refer to TPPs that are authorised to initiate payments out of or into a user's bank account using the bank's own payment systems. These third parties provide businesses with the capability to use bank-to-bank transfers rather than traditional card payments. **This allows direct initiation of their customers' payments and collections and removes costly card transaction fees. Customers also benefit as open banking allows consumers to make payments from a single account aggregated interface.** While third parties such as FinTechs and online payment providers have been offering innovative payment options for a number of years, open banking APIs provide structured, direct access to bank's payment systems for bank-to-bank payments without the need for customers to disclose sensitive card details.

WHAT IS DRIVING OPEN BANKING?

Open banking is still an emerging trend that has not yet fully infiltrated the global banking market. However, as the adoption of this model advances throughout Europe and the UK, banks in other countries are increasingly feeling the pressure to adapt to an open banking environment.

This is being driven by three key factors: **regulation**, **consumer pressure** and **technology**.



1. Regulation

Open banking has advanced significantly more in the European Union and the United Kingdom than in other regions, as banks have been required by law to allow third-party access to their data. In 2015, the European Commission introduced the Revised Payment Services Directive (PSD2), which came into full effect in September 2019. Whilst essentially a payments-focused directive, PSD2's most significant impact has been to open up bank-held customer data. The Directive aims to drive increased competition, foster innovation and ultimately empower the customer to share their financial data as they see fit. The Open Banking Standards were adopted by the Competition and Markets Authority in 2016 in the UK with a similar goal, as well as providing a standard for API specifications, customer experience and operational guidelines.

> **The Directive aims to drive increased competition, foster innovation and ultimately empower the customer to share their financial data as they see fit.**

Different regulatory approaches have been taken in other countries, such as Hong Kong and Australia. The Hong Kong Monetary Authority has taken a phased approached to API development and data sharing but unlike Europe, it has endowed banks with the authority to decide which third parties they will integrate with. In Australia, the passing of the Customer Data Rights Act has impacted not only the banking sector, but other industries as well. As a result of the Act, the Australian financial sector will be the first to open their customer data entirely, followed closely by the energy and telecommunications sectors, with the aim of creating a more consumer-focused data environment.

In South Africa, there has been no regulatory directive regarding the implementation of open banking or determining the technical standards for API technology in the financial industry. However, in its "Vision 2025 for the National Payments System Framework and Strategy" publication, the South African Reserve Bank has identified the need to explore an appropriate framework to allow direct access by non-banks into payments systems, to assess the impact of API technology, and to ensure the future-proofing of banking infrastructure in South Africa.

Whilst South African banks are currently not required to open their data to specific third parties as a result of a formal open banking standard or regulation, it would be prudent for these institutions to continue to monitor the uptake of open banking globally, and to track local regulatory developments carefully.

2. Consumer Pressure

South African banks are operating in a rapidly changing banking landscape that is trending evermore towards digital banking. An important factor driving this digital disruption is a customer preference for more technologically advanced banking products and services. Research has shown that South African millennials (born between 1980 and 2000), in particular, are seeking personalised, data-driven banking solutions accessible through their mobile phones.[1] Significantly, a study by the South African Customer Satisfaction Index found that 25% of bank customers were willing to move from their current bank to a financial institution that could better meet their current needs.[2]

Given the decline in customer loyalty to the financial institution where their primary transaction account resides, banks are increasingly being incentivised to adapt to meet customer demand for more technologically advanced banking. This may encourage South African banks to consider open banking as an opportunity, enabling them to provide value-added offerings to customers through collaboration with innovative FinTechs.

In addition, a ruling in a South African customer data sharing rights case in 2020 has potentially set a precedent regarding the legal rights of customers to own and share their data as they see fit. The South Gauteng High Court ruled that a customer be legally allowed to share their personal data collected by one corporation with another. Judge J. Keightley stated that the court should not restrict the choice of the consumer to share their data and thereby infringe on their proprietary interest in their data.[3]

Whether compelled either by banking regulations requiring financial institutions to share customer data, or by legal directives giving banking customers the right to share their data with multiple organisations, South African banks may soon be placed in a position where they cannot avoid implementing open banking practices. In such an environment, banks must look to the opportunities open banking provides for meeting changing consumer demands through collaboration with innovative third parties.

In addition, South African banks should look for opportunities to benefit from the agility and innovation that third parties provide, seeking to partner earlier on with brands that can offer untapped markets and new products and services. A well-structured partnership could be mutually beneficial, enabling banks to focus on their core competencies whilst TPPs are able to enhance their capabilities, unhindered by prohibitively expensive and complex core banking infrastructure.

Whilst increased competition will become a reality for banks and financial institutions, research company Gartner has also predicted the possibility of increasing annual banking revenue by as much as 30% from new revenue streams, such as charging to use their APIs and new fee opportunities.[4]

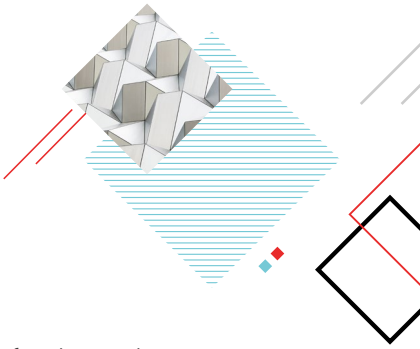
1. Consulta, '2019 – The year of rapidly rising customer expectations and fierce competition in the banking sector', Consulta [Website], 25 March 2019, https://blog.consulta.co.za/sa-csi-banking-results-2018/.
2. Ibid.
3. Discovery Ltd and Others v Liberty Group Ltd 2020 (4) SA160(GJ).
4. Gartner Research, 'Hype Cycle for Open Banking, 2016', Gartner [Website], 12 July 2016, https://www.gartner.com/en/documents/3374517/hype-cycle-for-open-banking-2016.

3. Technology

Growth in open banking has also been facilitated by advancements in open-API technology. Whilst similar services and applications – such as money and account management applications or non-card payment services providers – have existed for some time without open banking, they have relied heavily on screen-scraping and HTML parsing. These tools do not allow direct, structured access into the banks' IT architecture, but require the user to provide third parties with their banking login details – an inefficient and costly process.

This also creates security risks for banks as third parties encourage users to share sensitive login details (contrary to bank-customer policy), and banks are unable to monitor the activities of third parties, who may in fact have access to more information than a user consented to. APIs, in contrast, are more secure, managing access to data through tools such as OAuth 2.0, an open standard that increases safety by awarding access tokens to TPPs, rather than granting them access using sensitive user login credentials.

The South African financial sector does not yet have an API industry standard that provides guidance regarding authorisation, data exchange and managing bank-TPP partnerships. However, multiple regions including Japan, Singapore and the UK have released API standards – playbooks that should be leveraged to evaluate global benchmarks for API security, scalability, and efficiency.



Open banking should result in better personalisation, transparency and convenience for the end user, who will be able to cherry-pick apps, products and services, designed through intense data-driven analytics, to suit their individual requirements. This would challenge the current South African banking model and could transform the industry into a marketplace, where – much like Mobile Phone App stores – various banks, non-banks and financial service providers will offer customised offerings to the consumer on one consolidated ecosystem.

In this environment, banks are presented with the opportunity to become the infrastructure-providers that create and manage the marketplace. By considering the implications of open banking now, banks can position themselves at the centre of the marketplace, with their core banking suite maintaining the bank-customer interaction, whilst providing the customer with access to innovative and customised third party offerings that complement the bank's digital strategy.

> **"By considering the implications of open banking now, banks can position themselves at the centre of the marketplace..."**

The potential benefits of opening up access to customer data in the financial sector has perhaps been most widely explored in Australia, where regulators are considering the possibility of end-to-end process centralisation, where processes that require input from several independent stakeholders could be centralised through one interface. An example of this would be buying property that requires the services of banks, estate agents, lawyers and various other third parties, who could be connected by one interface to centralise the supply chain. This would facilitate the transfer of not only the buyer's financial data but legal, tax and niche customer data that could be accessed by banks for their own data analytic operations – addressing the problem of non-reciprocity in open banking, which has been widely criticised by banks.

OPEN BANKING IN SOUTH AFRICA: NEXT STEPS

Globally, the banking industry is embracing open banking to varying degrees. While South Africa has no open banking regulation or API standards in place as of 2020, there has been a market-driven demand for increased data sharing and payment innovation, such as mobile and cashless payments, by South African consumers. This has fostered increased competition and innovation by FinTechs and start-ups who are ready to meet these new digital consumer demands.

The commercial opportunities for open banking are being increasingly realised globally, and South African banks should look to capitalise on this momentum and consider collaborating with FinTechs and other good-fit third-party providers to offer innovative propositions. Novel monetisation of data and banking services will become available along with expansive, digital distributions models through third parties that will allow banks to reach high volumes of potential customers while the operational efficiencies achieved through APIs and the marketplace will reduce costs.

Banks in South Africa are well established and trusted institutions that have been considered a core part of the South African economy for decades. They now find themselves in a position to control their open banking strategy using their existing strengths and advantages, including their already established client bases, access to significant capital and freedom of choice to proceed with open banking as they see fit. This places banks in the driver's seat in determining their open banking strategy as the world moves to a future that is shifting away from the current closed-channel banking model.

To prepare for open banking in South Africa, banks should consider the following factors in their IT and open banking strategies:

1. IT Architecture & Data Governance

Open banking will require banks to spend money and effort on developing and adapting their IT systems and data architecture. The following will need to be considered:

- Banks will need to develop **robust data and system architectures** that meet the requirement for 24/7, real-time processing and integrate seamlessly across the bank's complex legacy systems. Most importantly, banks should begin specifying and deploying the necessary API connectors that will allow the integration and flow of data between the bank and service providers (TPPs).

- These open banking processes, achieved through API integration, will require **accurate and complete datasets** to meet the data requested and exchanged between parties. The requested data may be stored and processed across multiple systems, databases and functions that will require the design of comprehensive data taxonomies and business requirement specifications to establish a fully integrated view of the customer and financial transactions. Additional databases and development to existing databases may also need to be considered to meet any gaps that exist in the bank's current data landscape.

- A key consideration in mitigating the risk involved in exposing data via APIs is implementing industry standard **cyber security technology and processes** for the authentication and authorisation of third-party access points and client consent management. PSD2's electronic payments authorisation requirement in the form of Strong Customer Authentication (SCA) as well as the use of OAuth 2.0 as the industry standard for authentication are some of the measures being put in place globally to address security concerns.

- A **robust data governance framework** will be necessary to ensure any open banking enhancements to the bank's architecture meets compliance of regulation including **BCBS239, POPIA and IT security standards**. The added responsibility of managing third-party integration will require banks to adopt a proactive approach to data and security governance that fosters cross-business communication and transparency, and which is sufficiently versatile to address the changing demands of regulators, customers and third parties. Banks should also ensure that they implement processes for TPP and customer incident management.

2. Privacy

Open banking initiatives will require banks to consider and comply with personal data protection regulations such as the Protection of Personal Information Act (POPIA). The European Union has introduced similar regulations in the form of the General Data Protection Regulation (GDPR). **Both regulations were drafted to fill the regulatory void that emerged as technological advances relating to data processing, collection and transfers outpaced the laws previously passed by legislators.**

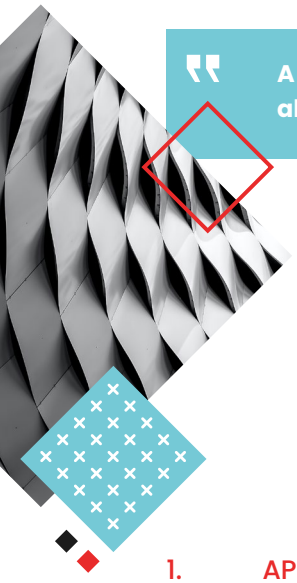
POPIA in South Africa, much like the GDPR in the EU, seeks to protect the data rights assigned to the people of South Africa and protect individuals from inappropriate and unlawful processing and storing of data by companies.

POPIA provides conditions for how organisations should access, store and process personal information in South Africa. Banks as well as third parties will need to consider the following principles when operating in any open banking initiative:

Protection of Personal Information Act Principle	Open Banking Consideration
Accountability – Parties need to act responsibly to ensure conditions for lawful processing are met and upheld.	The POPIA has legal requirements for responsible parties such as banks and third-party providers to ensure the security and confidentiality of personal data. POPIA requires the responsible party to establish written data processing agreement with their operators (third parties used to process data on behalf or outside of the responsible party) to manage any processing between them. Responsible parties should perform due diligence on operators to determine whether adequate security and governance measures are in place that meet POPIA requirements.
Processing and Purpose Limitations – Personal information must be processed in a lawful and fair manner that does not infringe on the privacy of the data subject	The purpose of processing data must remain in line with what the data subject consented to and should only be performed in the legitimate interest of the data subject. Banks and third parties will need to ensure that their customers are well informed of how their data will be processed.
Security Safeguards – Parties must ensure that the proper security measures to safeguard integrity and confidentiality are in place.	Banks and authorised third parties need to ensure that they have the necessary technical and organisational measures in place to protect the personal data they are processing. Banks and third parties will need to look at meeting industry best practise standards such as ISO 27001/2, COBIT or ISF.

Complying with data privacy regulations such as GDPR and POPIA has been a significant concern for companies, not only because of the potential reputational damage that can result from a privacy breach, but also due to the financial burden of non-compliance penalties.

Consumer sentiment regarding data privacy will also be a concern for banks as South African consumers feel uneasy about sharing their data. A South African survey into data privacy found that as many as 83% were concerned about the protection of their data, whilst 92% expressed concerns about the security of their financial data, and 80% about their health-related data. For open banking to take off effectively in South Africa, a key focus will need to be changing consumer perceptions regarding data security and privacy.



> **A South African survey into data privacy found that as many as 83% were concerned about the protection of their data...**

HOW CAN MONOCLE HELP?

As open banking gains momentum, banks will look to assess their current data, system and process architectures and to determine their readiness for open banking development. This will require project teams to unpack the intended product and service offering into specific, executable project steps. Monocle is able to assist clients in translating these business imperatives into the following actionable IT and operational change requirements:

1. API Architecture and Framework

Design the specifications for open banking APIs as well as design the system and data architectures that form the open banking program throughout the enterprise.

2. Data Models and Taxonomies

Analyse, define and establish data models and taxonomies while considering data lineage, timing, definitions and metadata for all required open banking datasets.

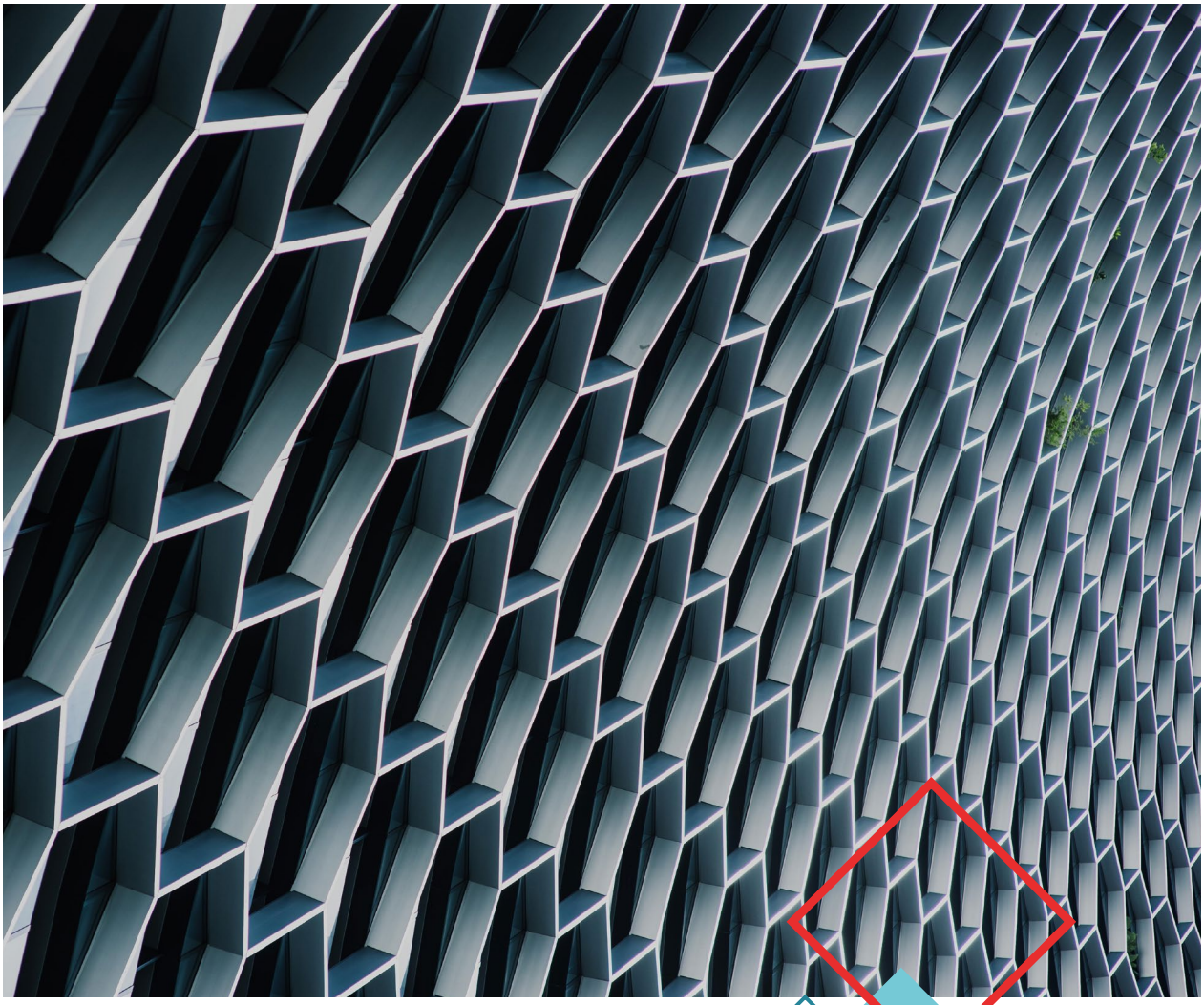
3. Data Classification

Classify and catalogue all data sets at the required granularity and detail to enable regulatory compliance relating to privacy, consent and security.

4. Operating Models and Third Party Provider Collaboration

Design and implement updated operating models with consideration to third-party processes, service level agreements and open banking governance frameworks.

Monocle has extensive experience in digital enterprise transformations and designing fit-for-purpose and regulatory-compliant digital solutions. With deep industry knowledge and strong technical skills, we are well positioned to support banks with their forthcoming open banking initiatives.



ABOUT MONOCLE

Monocle is an independent, results-focused management consulting firm specialising in banking and insurance with almost two decades of experience working alongside industry leading banks and insurance companies around the world. With offices in London, Amsterdam and Johannesburg we service our clients across the United Kingdom, Europe, Scandinavia, Asia, South Africa and much of Sub – Saharan Africa.

We design and execute bespoke change projects, from start to finish, bridging the divide between business stakeholders' needs and the complex systems, processes and data that sit under the hood. We offer several unique capabilities to our clients, which have been forged over time through the combination of a highly specialised skillset and extensive experience working with the systems, processes and people that are at the heart of the financial services industry.

JOHANNESBURG

13th Floor, Greenpark Corner,
3 Lower Road, Morningside,
Sandton, South Africa

Phone: +27 (0) 11 263 5800
Fax: +27 (0) 11 263 5811
Website: www.monocle.co.za

CAPE TOWN

301 New Cumberland,
163 Beach Road, Mouille Point,
Cape Town, South Africa

Phone: +27 (0) 82 952 1415
Website: www.monocle.co.za

UNITED KINGDOM

4 Lombard Street,
London,
EC3V 9HD, England

Phone: +44 (0) 2071 902 990
Website: www.monocle.co.uk

AMSTERDAM

Weteringschans 165,
1017 XD Amsterdam,
Netherlands

Open Banking: Disruption or Distraction?

MONOCLE