

WHITEPAPER



macro global®
creating value through innovation



Open Banking: A Strategic Change to Banks - The Playoffs



Foreword

The European payments market has been modernised and reformed several times in the recent past and this situation had an adverse effect on European financial institutions. Ten years after the introduction of the Payments Services Directive (PSD), the European payments ecosystem procured the next step in its regulatory evolution in the shape of PSD2. On 12 January 2016, the revised Payment Services Directive (EU) entered into force in the European Union and the Payment Services Directive Two (PSD2) is one the most radical pieces of legislation aimed at the payments industry and the banking sector. PSD2/Open Banking alarms the payments landscape in a far more revolutionary way than its predecessor.

“Open Banking is about making everything for sale. It provides a new way to increase digital revenue for the banks that are willing to think differently. Open Banks and FinTechs will continue to erode margins and customer relationships for those banks that don't.”

-- Kristin Moyer Research Vice President and Distinguished Analyst at Gartner

With the transition to the new open ecosystem, Open Banking poses a regulatory challenge for banks and builds a profound opportunity to create new business models for financial services and new value for customers. The adoption of Open Banking formalises the relationship between Banks and FinTechs by establishing the Open Banking framework. An immutable shift to Open Banking has become inevitable which provides open access to customer account data and the payments infrastructure speeds up the FinTech market players to develop new integrated service models. The second iteration of the Directive is driven by the same objective and ambition i.e., to lead payments innovation and data security by reducing competitive barriers mandating new security practices.

In this white paper, we will highlight the key considerations for Open Banking implementations and explore how banks can go beyond OB compliance to create a simplified experience for end-users with increased efficiencies using Macro Global's Open Banking solution-Tavas as a strategic partner.

Open Banking World – The Players and Drivers

Open Banking introduces a host of new roles for different organisations to play in the payments process. The most important part is the introduction of two new roles as Third-Party Providers (TPPs) in the banking ecosystem: Payment Initiation Service Providers (PISP) and Account Information Service Providers (AISP). Both roles are open to current and new players and banks, or Account Servicing Payment Service Providers (ASPSPs) will be required to support these new service providers if their customers want to grant them access to their account (either for information purposes or to initiate a payment).

Credit Institutions

An undertaking whose business is to receive deposits or other repayable funds from the public and to grant credit for its own account. On the flip side, credit institutions are referred as bank and their activities are broader and not limited only within payments.

Payment Institutions

Enacting Open Banking, Payment Institutions are referred to a category of payment service providers offering services supporting payments.

Third-Party Provider (TPP)

Third-party providers are organisations accessing customer's accounts by enabling services to provide account information and/or to initiate payments.

Payment Service Users (PSU)

A Payment Service User is an authorised person making use of a payment service as a payee, payer, or both. i.e., they make and/or receive payments.

Account Information Service Provider (AISP)

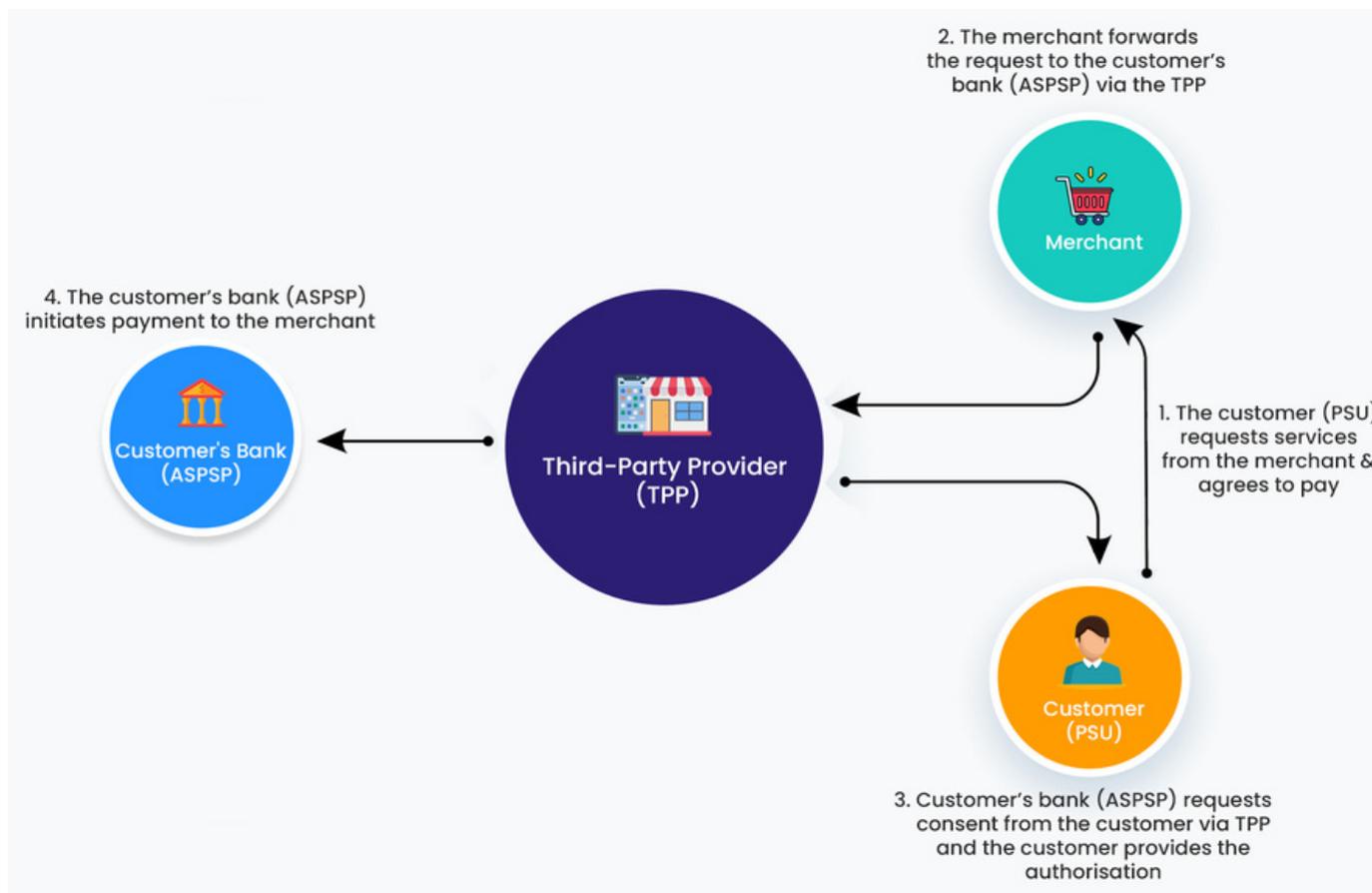
AISPs provides aggregated information of PSUs finances and also to manage account services held with multiple payment service provider(s).

Payment Initiation Service Provider (PISP)

PISPs are regulated entities like retail banks or third parties enabling online services to initiate a payment order upon PSU request to a payment account held with multiple payment service provider(s).

Account Servicing Payment Service Provider (ASPSP)

The role of ASPSP is namely covered by banks and are responsible for maintaining the customer's payment account(s). And enable services to PISPs and AISPs to access the authorised account(s) upon the account holder's consent.



Journey towards Open Banking Implementation – An Insight

Encouraging boundless choice and more pioneering services for both individuals and entities, Open Banking aims to strike the right chord for a new era of banking innovation within the competitive digitised business positioning. The progressive banks are in the midst of digital transformation and whilst the Directive exhibits an array of challenges for the players involved complying as a whole with the regulations – the Regulatory Technical Standards (RTS).

1. An opportunity to invest on compliance

“63% of banks see Open Banking as an opportunity, but there is widespread acknowledgement that Open Banking is also a potential threat and that in order to be able to fulfil the opportunity organisations must prepare and react appropriately”.

Strategically, Open Banking raises a number of key problems that banks have to address before implementing it. Banks are mandated to provide appropriate authentication & authorisation for TPPs and the ability to access their customer account data and process their payments and transactions using bank APIs.

A well-defined Open Banking framework extends beyond the API scope and calls for more re-engineering on the bank's portfolio and business model to accelerate into new market space.

Banks choose Open Banking as a stage of progression towards building a business model by providing Open Banking services integrating with the third-party provider as mandated by the new regulation to ensure compliance. Under the directive, banks are obliged to provide an open interface for authorised TPP as a value-added service handholding the opportunity to design the new ecosystem for customers.

2. TPP – The initiator

Banks are mandated to expose the payment initiation and account information services to regulated third parties and broaden their services and approach. TPPs are considered to be an entirely new customer for banks as they do service for the bank's end customer. Banks must offer 24/7 inclusive support to every TPP and additional domain services ranging from onboarding of third parties, certification validation, a sandbox environment and developer community management.

3. Mandated Contingency and voided Fallback exemption

Banks providing a dedicated interface (API) to third-party Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP) can apply for a fallback exemption to avoid third-party providers (TPPs) from accessing the bank's standard internet banking interface. If the bank proves to be robust in terms of availability and reliability of its dedicated interface for the specified timelines, then the bank can exempt from fallback measures with approval from the Open Banking regulators.

The Open Banking framework lays down the banks to have a contingency mechanism ensuring the payment service user (PSU) access the service in case of a fallback in the dedicated API interface. The fallback solution enables to access customer transaction data through the online or mobile banking interface.

4. The BEST FIT – Open APIs Vs Legacy System

The dependency on legacy infrastructure is common for any bank, the challenge is that the legacy system deeply ties between operational data and processes. In the last 10 years, technologies supporting API management and integration have taken a bigger picture and effect on banks to innovate and rationalise both product and service efficiency. To stay competitive rather than just compliant, banks need to extend the legacy system with an integration layer and open up their APIs to enable services in a secured and resilient platform. The new directive digitally transforms the bank's architecture and infrastructure to build an enhanced experience and adhere to today's open world.

5. Open Banking – The banking services redefined

It's unlikely that banks build Open Banking without any kind of external support particularly when it comes to infrastructure and software requirements. Any bank complying with the Open Banking agenda prefer to work with technology that doesn't require reinventing the wheel. In order to facilitate an infrastructure that enables third-party providers (TPPs) to obtain standardised access to requested data, banks must engage with providers underlying the Open Banking solution with data protection and security measures thereby reducing the compliance burden.

Macro Global's Open Banking Services for Banks

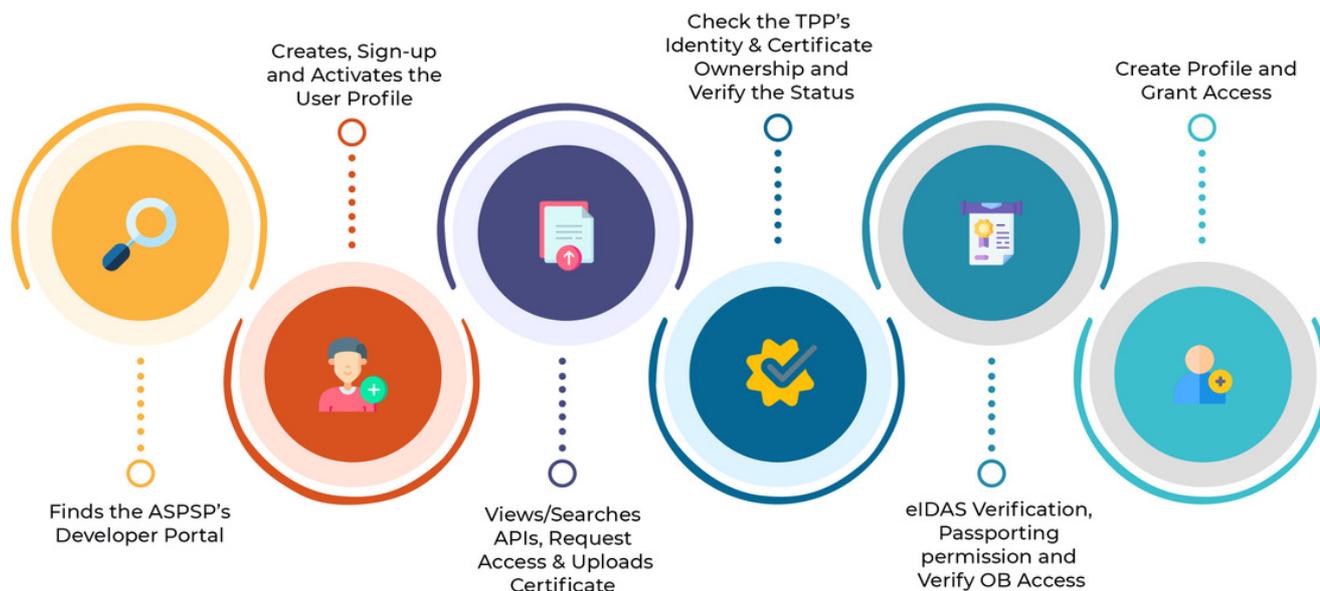
Secure Open APIs are transforming financial services in the new digital economy providing innovations for competitive differentiation. To thrive and to capitalise on the business opportunities, banks (ASPSPs) must focus on their infrastructure, re-engineer their business model and open up their systems for third-party providers (TPPs) to provide a consolidated view of account information.

"Tavas – Open Banking Product Suite and Solutions" empowers the bank to build a connected experience and provides the flexibility to adapt to the emerging opportunities to position themselves in the new era of consumer-centric banking. Banks are mandated to implement a series of technical specifications and its standard including Strong Customer Authentication (SCA), secure Application Programming Interface (APIs) and consent mechanisms to adapt the digital transformation and create a strategy through innovation. Macro Global's expertise help banks to achieve OB compliance through our unified solution and persuade their vision. Tavas enables banks to create a seamless customer experience by addressing the key challenges around customer authentication, secure APIs, consent management and maximise the value of customers with a flexible solution.

Tavas – Integrated Services

Third-Party Onboarding:

To oblige the Open Banking framework, banks should check their internal guidelines on whether to grant permission for third-party providers (TPPs). Banks need to procure customer consent to permit the TPPs to access Account Information Services (AIS), Payment Initiation Services (PIS) and access information on the availability of funds (COF) in the payment account. TPPs play a vital role within the new Open Banking ecosystem and must integrate their services with banks' Open Banking APIs. As a value proposition with our Tavas, Macro Global furnish a dedicated developer portal where API documentation is published which can be used by the third-party providers for the onboarding registration processes with the bank. Third-party providers must provide the mandatory information and specify the Open Banking roles authorised by the Competent Authority (CA). The developer portal enables to access the Sandbox environment enabling TPPs to perform tests and checks on APIs.



Exposing Open Banking APIs:

Subject to the regulatory requirement, Tavas provides banks to extend and integrate their services (Account Information Service, Payment Initiation Service, Card-Based Payment Instrument Issuer) with third-party providers by offering a common REST API and also enables the banks to deploy pre-configured APIs. APIs can be customised to the bank's specific needs and requirements. Our solution supports the regulated third-party providers (TPPs) with READ/WRITE APIs to consume the subjected services.

Identity Server:

Tavas's OAuth 2.0 Server is aligned with the Open Banking compliance requirements considering both technical and business industry-standard protocol for authorisation and the server can operate in any on-premises or cloud environment with seamless integration. It offers enterprise-grade capabilities with strong and adaptive authorisation, validating the access token based on background factors (e.g., TPP validation, SCA Authorisation). Macro Global services make it feasible for banks to adopt the evolving opportunities with a high level of security policies through the OAuth 2.0 Server providing personalised service to build a strong, enhanced customer experience.

Mutual TLS (mTLS) – Tavas Gatekeeper:

The Open Banking specification mandates the banks to apply mutual TLS (mTLS) in order to manage and validate the third-party provider (TPP) which requires integration between the banks' login component and Identify Server to support the OpenID Connect. Tavas solution enables subjected integrations to bridge identity services with security protocols and optimised for securing APIs and microservices.

Certificate Verification – Tavas's Flag off:

Certificates are the key security component specified by the Regional Banking Authority which empowers the banks to become OB compliant and authenticate third-party providers (TPP). Macro Global services verify the validity of TPP's licence and validate the certificate signature, eIDAS certification and passporting permission on daily basis. An additional validation will be processed to ensure whether the third-party providers' role affirmed corresponds to the service requested to ensure integrity of the transmitted data.

OpenID Connect – Tavas Data Privacy Vault:

The Open Banking mandate demands secure access to customers sensitive and PII (Personal Identifiable Information) data and to uphold the mandate, Tavas supports common API security standards such as OpenID Connect (OIDC) standard protocol built on top of OAuth 2.0 used for Identity and Access Management to face off the data privacy challenge. Tavas's stringent data security approach across the platform simplifies the integration and is compatible with industry practices such as Financial-grade API (FAPI) and Mutual TLS (mTLS).

Strong Customer Authentication (SCA) – Tavas Authentication Readiness & Adoption:

The new directive is governed by Strong Customer Authentication empowering improved protection for online transactions. The subjected authentication method is incorporated in Tavas as a security layer to authenticate a payment initiation and ensure secured payment processing via something the user knows (password) and something the user possesses (One-time password sent to a phone) in order to comply with multi-factor authentication requirements. Tavas's Strong Customer Authentication service strengthens and speed up the payment transaction in a secured manner and provide reliable authentication for web and mobile banking applications.

Tavas Administration Portal:

The web-based back-office administration portal supports the banks' verification and authorisation process (Four eye principle) for the TPP onboarding. The administration portal provides exclusive information for the bank to track, monitor and manage the services including TPP Onboarding, Regulatory Reporting, API Health Check, Tracking the transactions (both success and Failure), Revoke Consent, etc.



Tavas Administration Portal – The Standout Features:

Dashboard

A centralised dashboard to manage the payment and account consent management for well-informed business decision making. Display below metrics & KPIs (Key Performance Indicators)

- 💡 How many TPP's have been onboarded?
- 💡 How many AISP and PISP requests have been initiated?
- 💡 Total number of Account and Payment transaction count
- 💡 Is there any TPP registration pending for review or approval?

TPP Management

Provides the list of TPP's onboarded and allows the user to Approve or Reject the access.

Account Consent Management

Provides the details of Account Consent Information and provides the option for the user to either Authorise/Revoke or Reject the consent.

Payment Consent Management

Provides the details of Payment Consent Information and provides the option for the user to either Authorise/Consume or Reject the consent.

API Health Check

Proactively monitor the API health status to stay ahead of failures or major issues.

Regulatory Reporting

Regulatory reports designed based on the mandates established by the regulators (FCA and other regional regulators) indicating the quarterly statistics on the availability (as a percentage of uptime and downtime) and performance (based on daily average time in milliseconds) of the dedicated interface.

Solution and Business Benefits

Macro Global's vision is to empower financial institutions with Open Banking API services creating a unique opportunity in the digital world and deliver real value. Macro Global has the proficiency to act as a Technical Service Provider as well as an entrusted strategic expert in Open Banking Implementation. Tavas enables the organisations to manage the business workflow by offering dedicated API services through a one-stop-shop solution that enfolds Regulatory development.

Tavas enables strong compliance through a reliable solution.

- Tavas complies with the Open Banking conformance test suite and is compliant with UK Open Banking Specification Version 3.1 and other regional OB specifications.
- Integrated developer portal and API sandbox to enable third-party provider (TPP) to build and develop Open APIs.
- Ensures compliance with strict regulations to achieve interoperability and stay in control of the endlessly changing payments ecosystem.
- Resilient service to handle massive account and payment requests and ensure the integrity and validity of every transaction.
- Strong technological solution with a flexible and streamlined process and secure authentications with multi-factor authentication.
- Enable payment service users to securely initiate payments and transfers from the financial account directly from ASPSPs mobile app or internet banking website.
- Limit fraudulent risk with secure, real-time data access from payment services user's bank account.
- Responsive, round-the-clock security controls to verify the identity access.

We are here to help you

If you want to learn more about our products or services or just have a question?

If you need advise from our expert team who understand your business better than our peers?

If you want to know how we transformed businesses using our unparalleled industry and domain expertise?

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

<https://www.macroglobal.co.uk/contact-us/>

