GPay perspective: Open banking system design

G Pay

Contents

Executive Summary

What is Open Banking?

Open Banking is the use of open APIs that enable consumers to use third-party products and services that communicate with financial institutions to manage their finances. So far, Open Banking APIs allow consumers to securely:

1. Share their financial data with non-bank third parties of their choosing (Account Information Services, or AIS).

2. Initiate payments from their bank accounts via third parties of their choosing (Payment Initiation Services, or PIS)

Open Banking holds the potential to drive innovation and spur competition across digital ecosystems, with user consent and high consumer protection standards. In the countries where it has been implemented, Open Banking is driving the creation of innovative products and services, which are enabling more choice and better financial options for consumers and small businesses.

Executive Summary

Open Banking models across the world

To date, a number of Open Banking models have been used in various markets. Two key examples are:

- **India's Unified Payments Interface (UPI)**, which enables third-party initiated payments (PIS) through a centralized API framework, has been used to drive the digitisation of payments and movement of money with phenomenal success. As of November 2020, UPI transaction volume had reached the 2 billion mark, representing 10% of India's GDP.

- **EU and the UK:** Open Banking has been implemented via decentralized API standards, spurring competition and innovation within the region's financial services sector. To date, over 500 entities have registered as third party providers (TPPs). Open Banking has not only led to rapid TPP growth but also catalysed consumer-focused innovation by incumbents, with 45% of financial institutions investing over 100M euros in Open Banking and 44% of financial executives quoting "Customer Experience" as the top driver for investment.[1]

---

[1] The investments and returns of Open Banking., Tink, 2020,
https://resources.tink.com/hubfs/05%20Resources/Tink%20survey%20report%20-%20The%20investments%20and%20returns%20of%20open%20banking.pdf

Executive Summary

Google's Open Banking recommendations

Alongside policymakers and industry partners, we share the belief that robust participation of the fintech ecosystem is essential for Open Banking to achieve its stated goals of innovation, competition and financial inclusion. This participation should ensure that the regulations and technical standards underpinning Open Banking reflect the practical needs of technology developers and avoid creating unintended barriers to participation.

As both a third party provider (TPP) and a partner to financial institutions, Google places a strong emphasis on solutions that reduce friction, both for our users and other developers that wish to connect into common infrastructure. In this white paper, we outline recommendations in four critical areas where we believe central banks, regulators and market participants should focus their attention.

Our recommendations are drawn from first-hand experience launching and scaling Google Pay (formerly known as Tez) across a wide range of ecosystems with diverse regulatory frameworks: in India with UPI; enabling first-party payments via local real-time payment rails in several markets (e.g. SEPA in Europe); integrating with banks via API aggregators in the US; digitising payments with PayNow in Singapore; and through active engagement with regulators and Central Banks around the world (e.g. UK, Europe, Brazil, Mexico, Canada, and more).

Executive Summary

Google's Open Banking recommendations (cont.)

The four areas on which we focus are:

API scope - this directly impacts the level of innovation and competition that will be enabled across the ecosystem. We recommend implementing both account information services (AIS) and Payment initiation services (PIS) from day one. This will provide the framework and foundation that will maximise participation, innovation and competition across the financial services ecosystem. AIS enables parties to innovate and provide services that can improve consumers' understanding of their financial position, while PIS allows users to take immediate action on the insights and helps improve their financial health.

API framework - this has a direct, practical impact on the cost to new providers of participating in the Open Banking ecosystem and therefore impacts the level of new competition and innovation. We recommend the use of a Centralized Nodal API framework with a defined API standard to minimise implementation fragmentation and the need for additional layers and associated costs in the payment stack, ensuring equal access to the real-time payment rails for FSPs and TPPs of all sizes. The API framework needs to be considered from both a technical and a functional lens and should be secure, reliable, inclusive, efficient and scalable.

Simple authentication - this defines the ease with which consumers and developers can engage with the benefits of Open Banking. Thus, it should be at the forefront of system design, with consistent standards enforced across all licensed participants. We recommend a model of embedded trust, whereby third-party providers (TPPs) manage user consent directly through their interfaces once trust is established between User, financial service provider (FSP), TPP and device.

Commercial Model - this needs to ensure that the right financial incentives are in place to encourage adoption, investment and maintenance of best practices by all market participants. We recommend an ecosystem-wide principles-based approach to allow sustainable commercial models to emerge. This approach is compatible with fee discounts for micro transactions and SMEs. We also recommend clear standards for liability, fraud responsibility, and dispute resolution between FSPs, TPPs and users.

Executive Summary

What is out of scope?

This paper does not attempt to cover the following topics:

- **Governance model:** We do not provide an opinion on governance policy as each market tends to have their own provisions for overseeing Open Banking with each involving costs and benefits. We do not provide details on the accreditation process for the participants mentioned in this paper.

- **Technical standard:** We do not outline a template for API specifications, business rules or a detailed system architecture. Instead, our goal is to suggest a high-level framework and address common concerns.

- **Benefits of Open Banking and third-party initiated payments:** We do not attempt to quantify the benefits of these systems and APIs for innovation and competition, which are widely recognized by policymakers and other experts.

Relevant documents

For other Google white papers related to payments please see:

- Real Time Payments Systems and Third Party Access

- Design principles for Third-party Initiation in Real-time Payment Systems white paper

Glossary
of terms

Glossary

Account Information Services (AIS):
An online service which provides consolidated information on payment accounts held by a payment service user with financial service providers.

Application Programming Interface (API):
A computing interface that defines interactions between multiple software intermediaries.

Competition and Markets Authority (CMA):
The UK's competition and consumer authority, with responsibility for carrying out investigations into mergers, markets and the regulated industries and enforcing competition and consumer law.

Financial Conduct Authority (FCA):
The conduct regulator for financial services firms and financial markets in the UK.

Financial service provider (FSP):
An entity that provides financial services to consumers and other businesses.

Identification and Verification (ID&V):
A process to check and confirm the identity of a person or entity.

National Competition Authority (NCA): One or more entities designated by a Member State as having the necessary powers and allocated responsibilities for performing the tasks related to certification, oversight and enforcement in accordance with this Regulation and the delegated and implementing acts adopted on the basis thereof.

OAuth2: An authorization framework that enables applications to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account.

Open Banking: The use of open APIs that enable third-party developers to build applications and services around the financial institution.

Open Banking Implementation Entity (OBIE):
The delivery organisation working to define and develop the required APIs, security, and messaging standards that underpin Open Banking in the UK.

Payment initiation service (PIS):
An online service which accesses a user's payment account to initiate the transfer of funds on their behalf with the user's consent and authentication.

Payment Service Providers (PSP):
A certified and trusted entity that connects third party providers to a centrally managed service.

Payment Services User (PSU):
A natural or legal person making use of a payment service as a payee, payer or both.

Glossary

Strong Customer Authentication (SCA): Authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is).

Third party provider (TPP): Organisations or natural persons that use APIs developed to standards to access customer's accounts, in order to provide account information services and/or to initiate payments.

Unified Payments Interface (UPI): The real-time payment system developed by the National Payments Corporation of India (NPCI) facilitating inter-bank transactions in India.

Section 1:
API scope

G Pay

API scope

There are 2 types of API service covered within Open banking; Account information Services (AIS) and Payment initiation services (PIS).

Some Regulators and/or Central banks have stopped short of implementing Payment Initiation Services (PIS) as part of their first phase of Open Banking e.g. Australia[2] and Canada. Others have focused on enabling third-party initiated payments only e.g. India. We believe the full value of Open Banking can only be achieved by offering BOTH AIS and PIS as complementary functionality. While AIS enables TPPs to innovate and provide services that can improve consumers' understanding of their financial position, PIS allows users to take immediate action on the insights and help improve their financial health.

Account Information Services (AIS): Provide TPPs access through user consent to banking, transaction, and other financial data.

Allowing user controlled access to this data will drive innovation and spur competition across digital ecosystems, creating new innovative products and services. An example of this can be seen in the UK market, which launched AIS APIs in January 2018. Since launch, a large array of new products and services have been created, from; personal finance management, subscription management, KYC process automation, credit scoring, multi-banking, and many more[34]. The impact can be seen in the number of third parties licensed to access AIS APIs, 219 as of February 2021 and the number of monthly API calls, over 631M in the same month[5].

---

[2] It is worth noting that the AU regulator eventually decided to include payment initiation in their roadmap as of January 2020, as they have found it to be "the functionality most frequently asked for by fintechs and the market"
[3] OBIE, THE OBIE'S 2020 ROUND UP
[4] Tink, The most popular Open Banking use cases in the UK, Tink, 2020
[5] OBIE, Open Banking APIs Performance

Recommendation

The scope of AIS should allow TPPs to provide financial services based on a comprehensive view of users' daily financial activity.

- **Account types** should include, at a minimum, current, savings accounts and credit cards

- **Scope of data and availability** should at a minimum match what is accessible from the financial service provider's (FSP) online channels (website and mobile application), or via incumbent screen scraping based-solutions.

Payment Initiation Services (PIS):

Enable TPPs to initiate payments with user consent from accounts held at financial institutions.

Like AIS, enabling users to initiate payments from third party services will drive innovation and spur competition across digital ecosystems, creating new innovative products, services and experiences within the payment space. An example of this can be seen in India, where UPI[6] launched in 2016 and has spurred a variety of new products and services from third party providers. UPI now accounts for 22% of all payments[7] and represents 10% of India's overall GDP.

---

[6] NPCI, Unified Payments Interface (UPI)
[7] Statista, Share of payment systems across India in FY 2019

Recommendation

The scope of Payment Initiation Services (PIS) should allow TPPs to provide native payment experiences that support a users' everyday needs.
We recommend PIS APIs should include the following capabilities:

Payment types (all domestic)	Key TPP use cases enabled (non-exhaustive)
Single immediate payments (including scheduled payments), typically submitted by the payer's PSP/FSP on local payment rails	• Online / offline merchant payments • P2P
Request-to-pay, allows a payee to request funds from a payer	Pull payments (payee-requested) including: • Online / offline merchant payments • P2P
Funds reversal, critical to track link with a previous payment order	• Customer disputes and refunds
Recurring payments with fixed beneficiary, but variable time and amount (i.e. mandate)	• Utility payments • Round-up savings
Recurring payments, with fixed time, beneficiary and amount (aka standing order)	• Utility payments • Subscriptions
Payment cancellation	• Scheduled and recurring payments

Section 2:
API framework

G Pay

API framework

The choice of API framework has a direct impact on the cost of fintech participation in Open Banking, which subsequently impacts the levels of new competition and innovation. One example of this can be observed in the UK, where a decentralized model has led to fragmentation of API implementations across FSPs - necessitating the creation of third party API aggregators to simplify connectivity for new participants. Smaller fintechs face the choice of navigating this fragmentation themselves, supporting only a subset of FSPs, or paying aggregators for access. These challenges create an unintended barrier to entry and thus reduce competition and innovation at the ecosystem level.
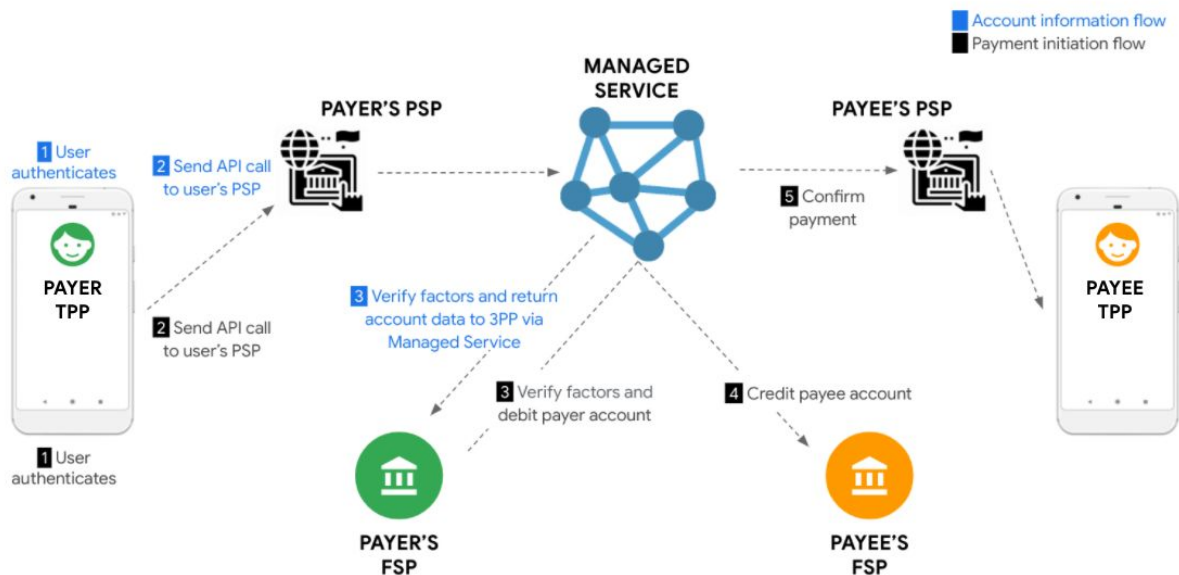
Types of API framework

There are two API frameworks that have been used for open banking systems around the world:

1. **Centralized** - all participants (PSPs, FSPs, TPPs, etc) connect to a single system

2. **Decentralized** - all FSPs are responsible for providing a standard set of APIs and PSPs connect to each FSP individually.
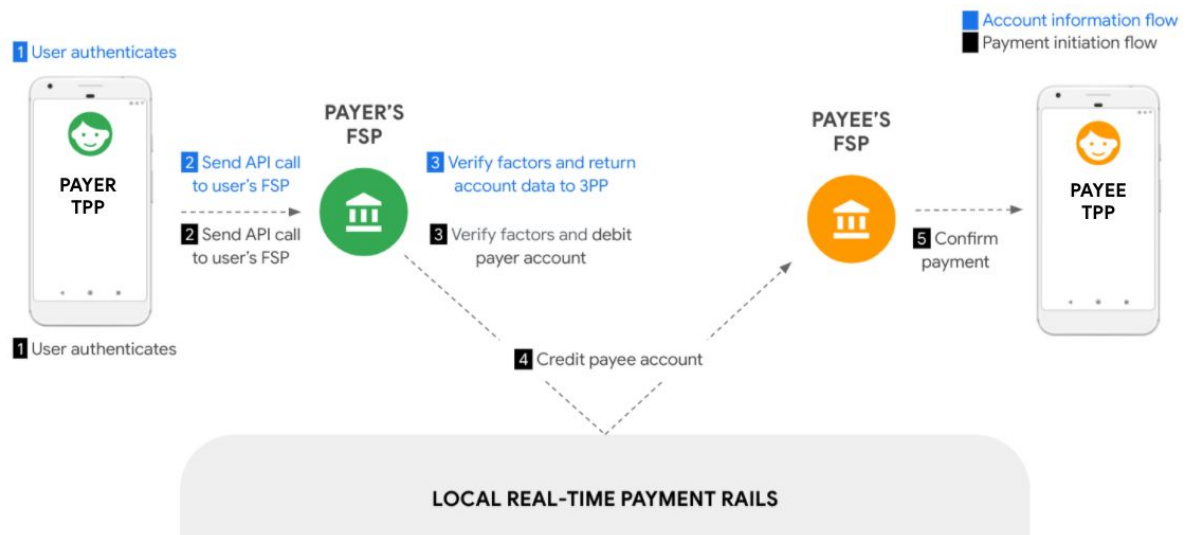
API framework

In centralized systems

In centralized systems (e.g., India's UPI or Australia's NPP) a single API endpoint to a managed service acts as a central switch, shuttling requests and responses between participants (e.g., from PSPs to FSPs, and from TPPs to PSPs). This ensures that each participant needs no more than exactly one API integration. In addition, centralized systems provide the ability to more easily enforce at scale other system-wide policies such as those for security, billing, rate limits, and other request quotas.

API framework

In decentralized systems

(e.g., UK's Open Banking), a central regulatory body defines a set of API standards to be implemented individually by each FSP. This removes the need for centrally-run infrastructure. However, each TPP and/or PSP must then integrate directly with each of the FSPs via the API specification, which may itself have practical implementation differences from FSP to FSP.

API framework

The following table summarizes the key differences between centralized and decentralized systems.

	Centralized	Decentralized
Central Infrastructure	Required	None required
Policy enforcement	Handled centrally, full control	Handled by FSPs, audit only
Integrations for TPPs	1 per TPP	1 per FSP per TPP
Guaranteed consistency for all integrations	Yes, one implementation means no variation whatsoever for API clients	No, different implementations may have subtle differences in behavior (even with same API)
Leads to aggregators	No, central system is already an aggregator	Yes, aggregators have a viable business model which may create costs for TPPs
Allows competition on API specifications	Yes, new API methods can be routed through extensions in the central switch	Yes, FSPs can support additional API methods
Version fragmentation	No, single deployment means all bug fixes and new versions are fully controlled	Yes, changes rolled out across all FSPs on varying timeframes

_ Color key:_* _Green indicated that the rated model fares well on a topic, red indicated that it fares poorly, amber indicates it's good enough but less than ideal._

API framework

Setting mandate vs standards

An NCA will need to consider whether to:

1. Set the mandate and objectives but refrain from setting the actual technical standards for implementation of Open Banking. In this scenario the NCA would expect market participants to come together to define standards and specifications for the implementation of the mandate. This was the approach taken by PSD2 in Europe.

2. Define the technical standards, albeit in an inclusive process involving all potential market participants. This was the case in the UK and Australia, where a designated implementation entity set the API specifications and Customer Experience guidelines, in consultation with market participants throughout.

Recommendation

We recommend the use of a Centralized API framework with a defined API standard. This:

- Prevents the API standard and implementation fragmentation observed in decentralized models

- Eliminates the need for API aggregators for TPP access (reducing ecosystem cost)

- Ensures equal access to connectivity for participating TPPs

- Enables TPPs to focus on building products/services, not account access (which Open Banking should guarantee)

- Provides transparency and oversight into API compliance and performance, as well as faster identification and deployment of debug fixes

- Leverages existing investments in real time payment (RTP rails) infrastructure and security protocols

While a centralized model requires an entity to oversee the development of the framework and enforce compliance to the standard, we believe the long-term benefits outweigh the additional cost. Furthermore, even jurisdictions using decentralized models usually require a standalone entity to govern access to the payments infrastructure (e.g. Pay.UK in the UK) and set API standards (e.g. the OBIE in the UK).

Section 3:
Simple
authentication

G Pay

Simple authentication

Creating a low-friction and secure user experience is crucial to the adoption of Open Banking for both consumers and developers. This is particularly true in the authentication of a user in both AIS and PIS.

Open Banking systems that have developed high-friction user experiences have experienced slower adoption. For example, in the UK:

- **User adoption PIS remains low**. Authentication of the user is supported via a redirect to the FSP. At launch the design of these experiences was left to each individual FSP, resulting in many high friction flows. Since launch, the Open Banking Implementation Entity (OBIE) has issued UX implementation guidelines and legal mandates to address these problems. Despite these efforts, a recent OBIE report shows only 0.55% of API calls to FSPs were for payment initiation services[8].

- **There have also been problems in the AIS authentication experience, particularly the requirement to re-authenticate the user every 90 days**. Third party providers (TPP) have reported 3**0% user drop-off at this point**[9], and cited it as a significant barrier to product innovation, and ultimately their viability and ability to operate. The Financial Conduct Authority (FCA) has recently proposed a change to its regulatory technical standards[10] that would remove the 90-day re-authentication via redirect, replacing it with a consent extension flow surfaced within the TPP experience.

---

[8] Source: openbanking.org.uk monthly API performance statistics, accessed February 2nd, 2021.
[9] Source: Openbanking.org.uk: Options paper - reducing the negative impact of 90 days re-authentication
[10] Source: FCA consultation, https://www.fca.org.uk/publication/consultation/cp21-3.pdf

Recommendation

Authentication should be built around the concept of delegated trust. This means that once trust is established between the user, TPP and FSP, subsequent user consent and authentication actions can be obtained and managed by the TPP, removing the need to redirect the user back to the FSP every time. These requirements should be specified within the system design and mandated across all participants.

Account Information Services (AIS)

- **Initial access consent:** The user, TPP and FSP establish trust via an Identification and Verification (ID&V) process performed by a redirect to the FSP surface. On completion, an access token is created (e.g., OAuth2) giving the TPP ongoing access to the user's account data. Strict technical standards should be mandated for this flow.

- **Consent management:** The user should be able to remove or extend access consent at any point, directly from the TPP or FSP surface. Defined user actions such as signing in to the TPP service or App should enable automatic consent extension. Users should be prompted to review and revoke or extend their consent on an ongoing time bound basis, e.g. annually.

Payment initiation Services (PIS)

- Initial consent (first payment setup): The User, TPP and FSP establish trust via an ID&V process performed by a redirect to the FSP surface. (As in the case of AIS).

- Transaction time: The TPP uses the trust established to perform authentication of the user using Strong Customer Authentication (SCA) principles at transaction time. There is no ongoing requirement to redirect to the FSP for every subsequent transaction. For technical details see our 'Design Principles for Third-party Initiation in Real-time Payment Systems' whitepaper[11].

---

[11] Design Principles for Third-party Initiation in Real-time Payment Systems, https://research.google/pubs/pub50087/
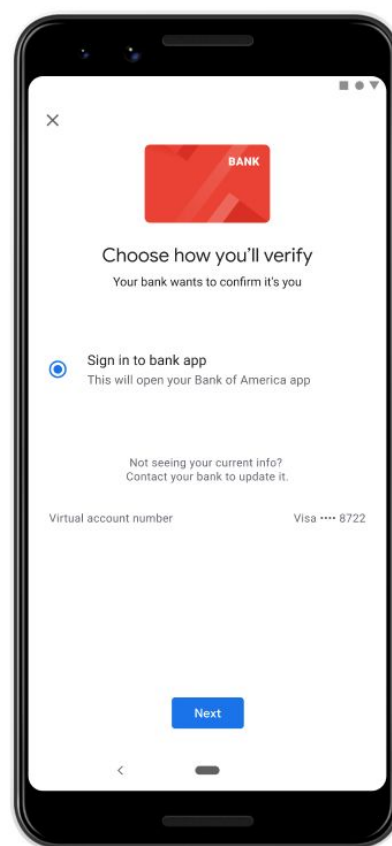
Recommendation

The recommended user authentication experience at time of payment with no redirect is already in place for tokenized card payments with mobile wallets such as Google Pay and Apple Pay.
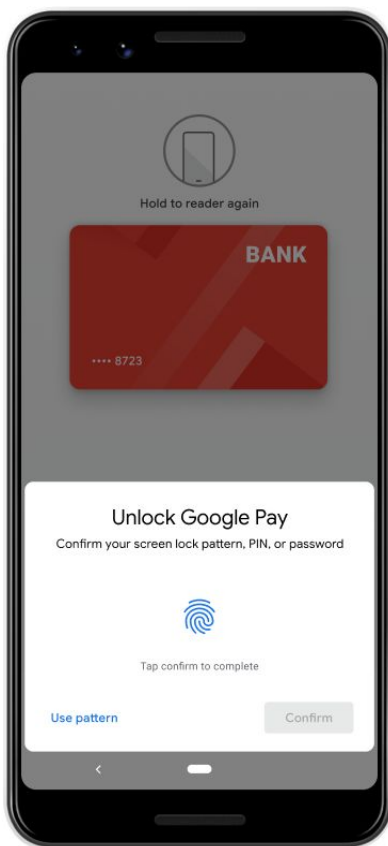
Initial binding (Google Pay)

User performs one-time ID&V with the FSP, creating a key on the device

Time of transaction (Google Pay)

User re-authenticates via biometric or PIN/password; low friction and in-context

Section 4: Commercial model

Commercial model

Open Banking systems promise great benefits to consumers, merchants, financial providers, and the broader economy. However, they also entail costs to FSPs, namely:

- **Direct investment** to develop and maintain new technical infrastructure
- **Ongoing operational costs**, such as local real-time payment rail settlement fees, dispute management, and regulatory compliance
- **Opportunity costs** from the impact of Open Banking on existing business models - for example, growth in local real-time payment rails payments vs. network card transactions

A careful balance must be struck to ensure that Open Banking systems support the attractive end-user economics necessary for consumer and merchant adoption, while also providing an economic incentive for FSPs to continue investing in critical infrastructure. This will be required to encourage the growth of alternative payment solutions for end-users to compete with existing payment methods (e.g. cards).

Examples from existing Open Banking implementations can be instructive. In the UK, EU, and India, regulators have mandated that PIS services be provided free to users, merchants, and TPPs - exposing FSPs to both development and ongoing operational costs.

Commercial model

This has led to two undesired outcomes:

- FSPs have largely operated slowly and only invested to meet the mandated requirements[12]. For example:

  Several large UK banks implemented Open Banking with overly complex user-facing flows, such that the OBIE was forced to issue minimum Customer Experience Guidelines[13].

  Also in the UK, the Competition and Markets Authority (CMA) was required to issue direction[14] to five banks who were found in breach of deadlines for app-to-app redirection functionality. This breach forced users to rely on cumbersome browser data sharing.

  The UK[15] (and the EU) has found the pace of Open Banking adoption and innovation (particularly PIS) disappointing, and is currently reviewing the Open Banking frameworks to try and accelerate adoption[16]. However, their proposals to date have focused on creating additional protections for consumers that would bring Open Banking payments closer to card payments (e.g. a chargeback equivalent), rather than on incentivising FSPs to actively promote the use of Open Banking.

- Reliability at scale is impacted. For example:

  Users in India are experiencing increased rates of transaction decline and failure when paying through UPI[17], as PSP investment in tech infrastructure has not kept pace with the rapid growth in UPI adoption.

---

[12] Source: https://www.thebanker.com/Editor-s-Blog/Has-open-banking-reached-maturity, Has Open Banking reached maturity
[13] Source: www.openbanking.org.uk, Open Banking Customer experience guidelines, https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf
[14] Source: Competition Market Authority, https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#retail-banking-market-investigation-order-2017
[15] Quote; Throughout the study, we have been surprised at the lack of innovation in this space, OBIE Report, A7 Root Cause Analysis on Consent Success
[16] Sources: UK Payments Landscape Review: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/904140/2020_template_PLR_CfE_27072020_final.pdf, pp. 16-19; European Commission Retail Payments Strategy: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN, pp. 6-9.
[17] Source: www.moneycontrol.com, As UPI grows leaps and bounds, transaction failures increase, too. October 29, 2020.

Recommendation

We encourage the adoption of an ecosystem-wide principles-based approach to allow sustainable commercial models to emerge. This means recognizing that PSPs need to cover at least their direct costs by allowing room for ecosystem fees, as well as innovation in business models and service delivery. At the same time, the approach must also respect policymakers' goals for Open Banking by ensuring that ecosystem-level costs remain low to stimulate adoption and drive innovation in other areas of financial and commercial service provision.

These principles should include:

- **Competitiveness:** Overall system fees should hew close to actual costs and remain competitive with existing solutions
- **Financial scalability:** Fees to individual participants should reflect the actual incurred cost of provision - not scale linearly with payment volume
- **Value for processing:** FSPs should be incentivized to invest in lowering costs and improving service levels, and to compete for greater processing volumes.
- **Fee parity:** No user or merchant should face different charges for payments made via a TPP vs. a direct open banking participant. Rather, fees should primarily be borne by TPPs and payer FSPs
- **Protected thresholds and classes:** Fees should not be levied on TPPs and FSPs below a minimum volume threshold, so as to support new entrants. Additionally, fee exemptions should be considered for low-value micro-transactions, and transactions with qualifying small enterprises and social entities, e.g. charities
- **Clear standards on limits of liability, fraud responsibility, and dispute resolution** should be set between FSPs and TPPs, ideally by an appointed third-party body.

Appendix

Learn more about Google Pay

Questions?
Contact us at:

Google

Stephen Ratcliffe (sratcliffe@google.com)

Mounir Mouawad (mounirm@google.com)

JJ Geewax (jjg@google.com)

G Pay