Open Banking and Open Data: Ready to Cross Borders?

July 29, 2022
Version: 1st Editor's Draft
Lead Editor: Dima Postnikov

Introduction

Would you like to be able to aggregate your data across your bank accounts? Enable your tax accountant to see your financial information? Enable the App of your choice to make a payment on your behalf? Or perhaps you would like to enable your residents or customers to perform these tasks in a low cost, secure and interoperable way? There is a global movement towards “Open Banking/Open Data” the paradigm shift where a user authorizes the release of their data from one entity (a data holder like a bank) to an entity where they would like it to go (a relying party like a FinTech). This is also known as “user-consent based data sharing.” Although this movement started with banking use cases and gaining access to data held by banks, it is now expanding to a range of other verticals including brokerage and mutual fund services, insurance, telecommunications, utilities, health and more.

One of the major complications is that each market has implemented their own version of Open Banking/ Open Data, so users or businesses cannot conduct these transactions across jurisdictions.

The next big challenge is how and when to enable global interoperability and unlock these cross-border use cases. This paper explores global relying party demand and outlines what “good might look like” and how to get there.

Readers of this whitepaper are encouraged to read this proceeding paper (“Open Banking, Open Data, and the Financial-Grade API”), since it more fully covers the origins of the Open Banking/ Open Data, market status including legal mandates, key standards, implementation considerations and recommendations for ecosystem participants. This paper will only cover some of the key themes of the preceding paper, and then picks up on the barriers to enabling Global Open Banking, and the driving forces likely to make this the next phase in this global trend. We will explore the use cases, market participants, standards, and mechanisms that can make Global Open Banking a reality.

The intended audiences for this paper are government and private sector thought leaders working on domestic open banking open data implementations, as well as thought leaders working on the adjacent areas of cross-border payments, cross-border identity, and international trade. Readers interested in Open Health and its linkages to Open Banking/Open Data should refer to the “The Global ‘Open Health’ Movement: Empowering people and saving lives by unlocking data” whitepaper published by the OpenID Foundation.

Comments

Comments on this 1st Editor’s Draft are welcome, and the deadline for comments is **August 26th 2022**. Comments will then be consolidated into a final draft of this paper, with a target for publication in September 2022. **Please send comments to director@oidf.org.**

Open Data Ecosystem Evolution

Although the Open Banking / Open Data movement is still relatively new in terms of domestic, ecosystem-wide scale, the need to expose customer data to external parties is not new. It has existed for a long time with legacy solutions using files, batch processing and message queuing to get data from the source to its destination.

Unfortunately, customers often were unaware that their data had been shared between different parties. Sometimes the user had granted indirect permission via product or website Terms & Conditions or other legal disclaimers, sometimes the user's permission was just implied. In some early use cases, third party access to data relied on "screen scraping," where a user gave their username and password to the third-party, and that third party used the login information as if they were the customer to download the information. Screen-scraping is now widely perceived as an insecure practice, creates risks to user privacy, and is progressively difficult to achieve as phishing-resistant authentication capabilities are scaled.

Changes to privacy expectations and regulations have introduced a requirement of user control of their data. It is becoming a norm that an end-user needs (and expects) to provide an 'informed consent' for their data to be shared with external parties. At the start of this movement, it was unclear how to enable such use cases and policies in practice, at scale.

With the development of secure API frameworks, it is now possible to share customer data securely with explicit consent enforcement. Open data ecosystems are essentially API-based access frameworks that expose a user's data to trusted parties with the user's consent, and they do so in a consistent way for all participants in an ecosystem. Over the last few years, we have seen these API-based access frameworks go through 3 phases of evolution:

Phase 1: Private ecosystems exposing public APIs.

Phase 2: Open banking ecosystems.

Phase 3. Cross industry ecosystems

This paper only focuses on API based integrations, and the opportunities to enable cross-jurisdiction use cases via APIs (and not other methods like screen-scraping).

Phase 1: Private API ecosystems

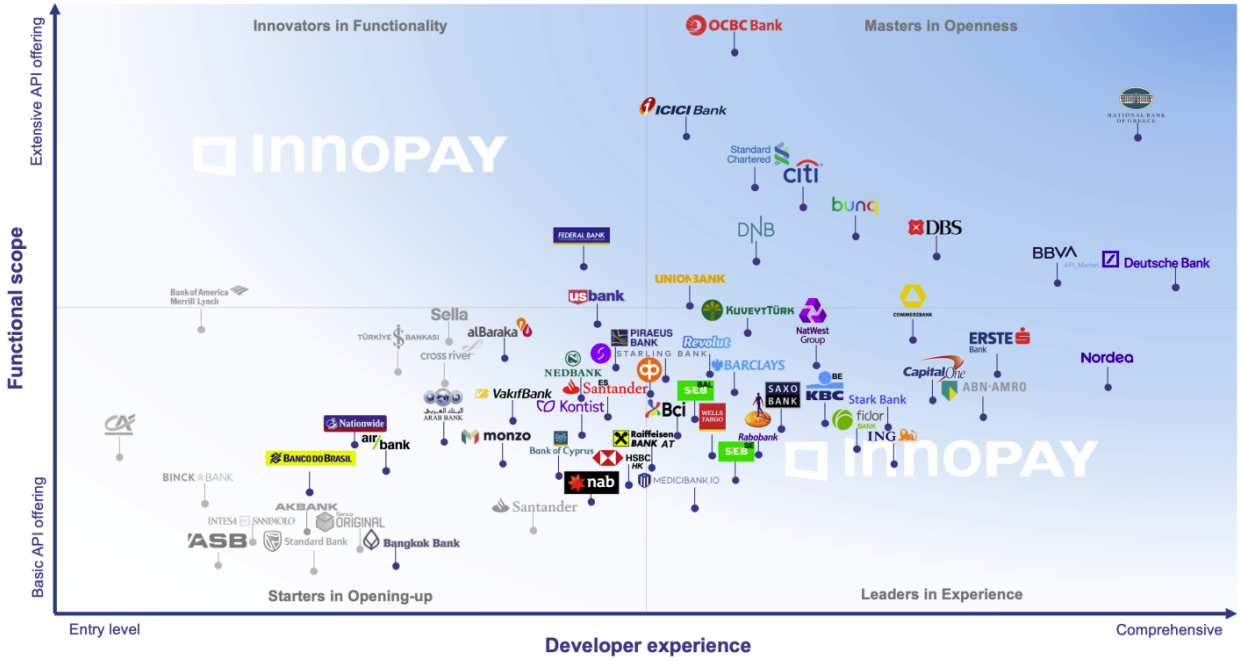
Many digitally savvy industry leaders began exploring internal and external API integrations well ahead of regulation, roughly a decade ago.

For example, a number of leading banks and telcos attempted to set up their own API programs to provide access to customer data and banking functionality to external developers. Banks recognised that external API ecosystems could unlock partner integration, client connectivity, banking-as-a-service/-platform and ultimately increase innovation and established private API programs. A few examples of these early bank implementations were Barclays API exchange, BBVA API Market, Deutsche Bank API program, and Santander's Payments Hub[1]. These programs were are unregulated and typically centered around one company, controlled by one entity, and were not mandated through government regulation.

[1] https://dzone.com/articles/top-10-banking-apis-how-to-make-your-app-and-trans

The benefits of APIs were manifold, as summarized in the chart below. They helped the bank surface capabilities from their legacy systems to their own front-end channels and across divisions within the bank, they future-proofed their platforms, simplified integrations with external vendors and partners, and facilitated innovation.

Going forward, the number and reach of API adoption is likely to continue scaling. According to a 2020 McKinsey global survey on APIs in banking, banks have plans to double the number of these APIs by 2025[2], and nearly 20 percent of banking APIs are used externally to support integration with business partners and suppliers. Similarly, Innopay reported a 17% increase of APIs in 2022 per bank in year since 2021[3], and much more room to grow. The chart below maps bank API deployments by their functional scope (basic to extensive) and developer experience (entry level to comprehensive). Over the next few years, we can anticipate most financial institutions migrating to the top right corner of this chart.



* Grey logo indicates limited portal accessibility, thereby complicating full assessment

APIs are firmly established as the “go-to” method for enabling services both inside the banks and outside the bank, and unsurprisingly, they proved to be the natural starting point to enable the “Open Banking/ Open Data” movement.

Phase 2: Open Banking Ecosystems

As the private ecosystem started delivering significant benefits for the bank's customers and partners, the obvious questions arose: What if a fintech company needs access to more than one bank? What if a customer has accounts in more than one bank?

[2] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/whats-new-in-banking-api-programs

[3] https://www.innopay.com/sites/default/files/media-files/Open%20Banking%20Monitor%202022.pdf

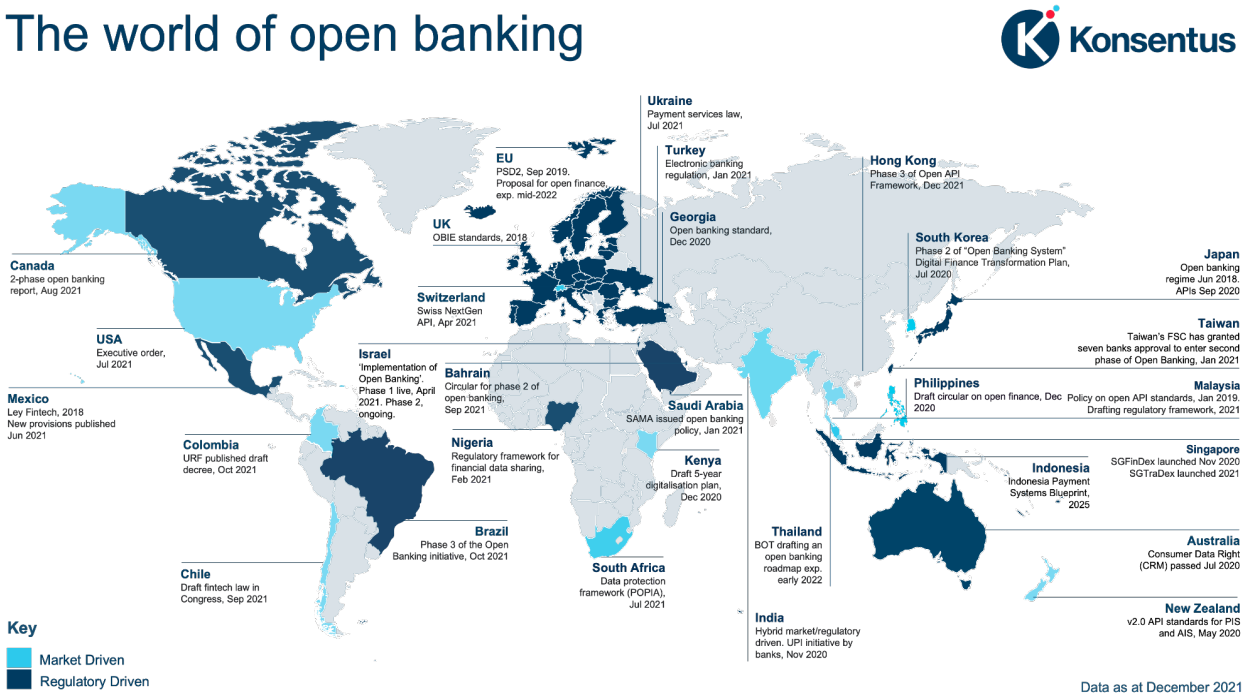
Regulators and private industry bodies in different countries across the world understood the value of using a common API access framework for an entire ecosystem. Open Banking brought the following benefits to consumers and fintechs:

- Consistent way of accessing data across the whole industry.
- Secure data transfer
- Mandated user control (explicit consent)
- New features previously not possible
- More competitive market

The elegance of a common framework, together with the user-consent based control it enabled, has led to rapid market adoption. Starting with the UK and PSD2 countries, followed by Australia, US, Brasil, New Zealand, Canada, Saudi Arabia, Nigeria, Bahrain, UAE and Israel and 10+ additional countries in review now. These open banking ecosystems can be market driven (US or NZ), partially regulated (UK for CMA9 banks only), or fully regulated (Australia, Brasil, Saudi Arabia).

There are also hybrid scenarios, where the regulators, like in Japan or in Europe (raw PSD2 regulation), mandated APIs to be provided without a standardized API contract. While this model provides full coverage of the Data Providers, it still carries significant complexity for Data Consumers.

This chart from Konsentus show the global status of Open Banking, with an overlay of which markets are regulatory versus market driven. In a few years' time we expect that most developed markets will have started or completed their own banking implementations, and emerging markets will continue the global rollout[4].



[4] https://www.konsentus.com/resources/the-world-of-open-banking/

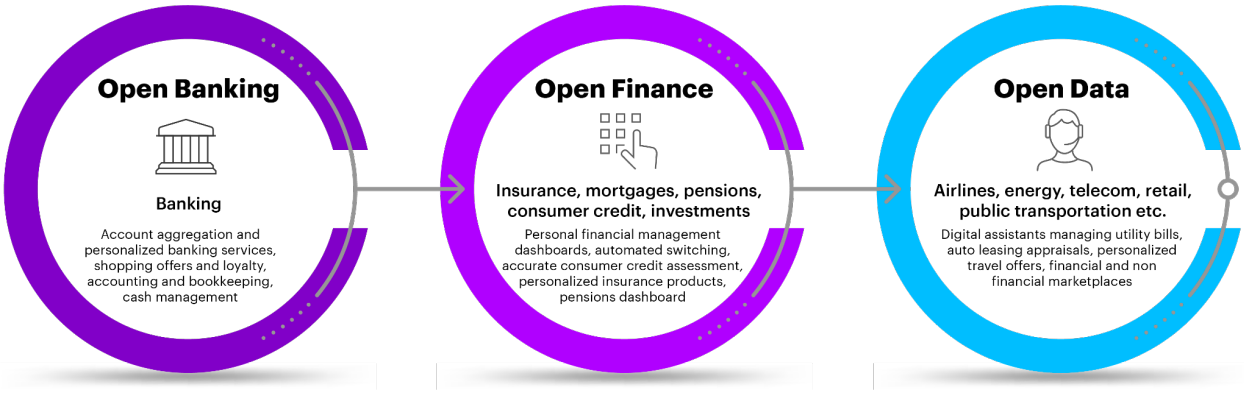
For more detail on local regulation and implementation status, standards selected by market, and implementation considerations, refer to the OpenID Foundation's March 2022 Whitepaper on "Open Banking, Open Data, and the Financial-Grade API"[5].

Phase 3: Cross-Industry Open Data Ecosystems

Once Open Banking is implemented in a region, it's only natural for a consumer, government official, or technologist to ask: why can't we use the same access mechanism to get my data from investment managers, insurance companies, telecommunication, health, and energy providers as well?

This simple question is driving the move from Open Banking to Open Finance and Open Data. While Open Finance has the ability to interlink multiple use cases in the finance industry, open data extends the model even further by enabling use cases in other industry verticals.

According to Forester, Open Finance will be a continuous process, "marking a fundamental shift in how customers access financial services and how firms deliver them"[6].



The momentum towards Open Finance and Open Data is currently driven by domestic markets, and usually ones that are government controlled:

- Brasil also has aggressive plans to scale its Open Banking (live from 2021) to Open Insurance in 2022, and they are exploring a move to Open Health as well.
- In 2022, Australia is going live with the Open Energy sector to complement its Open Banking ecosystem (Consumer Data Right) live from 2021. Open Telecommunications is the next sector to go live in 2023.
- The UK is considering expanding Open Banking (live from 2018) to Open Finance to take care of a wider range of use cases.
- The New Zealand government is considering Consumer Data Right legislation to come into effect this year, which may see it follow a multi-vertical approach similar to Australia.

[5] https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

[6] https://www.forrester.com/blogs/open-finance-will-reshape-the-relationship-between-banks-and-their-customers

- Berlin Group also extended their PSD2 API framework in the direction of Open Finance[7].

It is reasonable to believe that other countries will move towards Open Data as well. However, we may see some markets move more slowly into Open Data, especially if the governing entity does not have authority over new verticals, or if the market is “private sector led” and the Board of the entity is composed only of financial institutions.

What Have We Learned from Implementations to Date?

Leading Use Cases

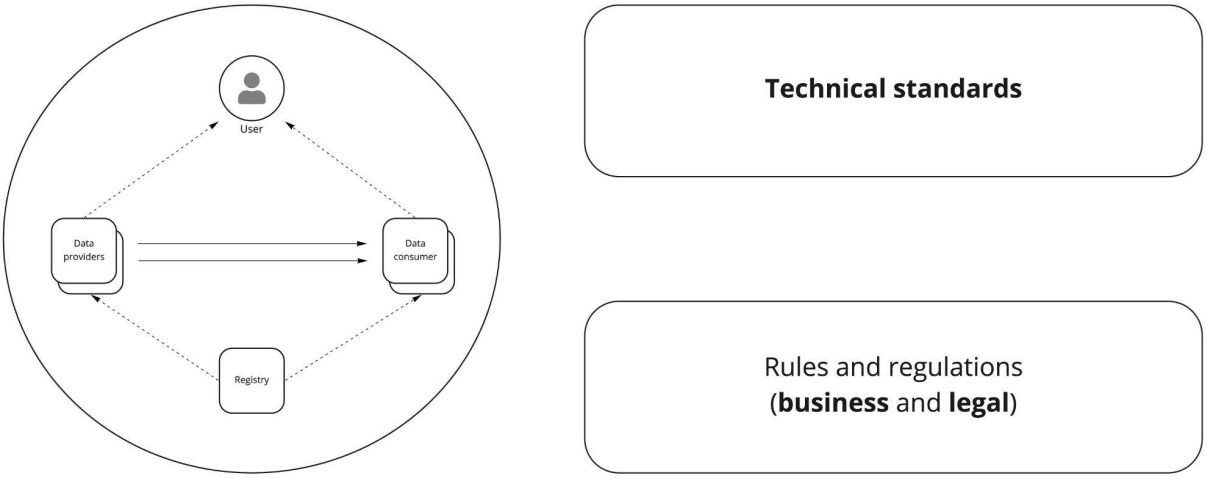
Around the world, there are three sets of use cases that most open banking or open finance ecosystem deliver:

- Consumer identity data
- Consumer Account information data
- Payment initiation

There are more similarities than there are differences in the use cases each ecosystem seeks to enable.

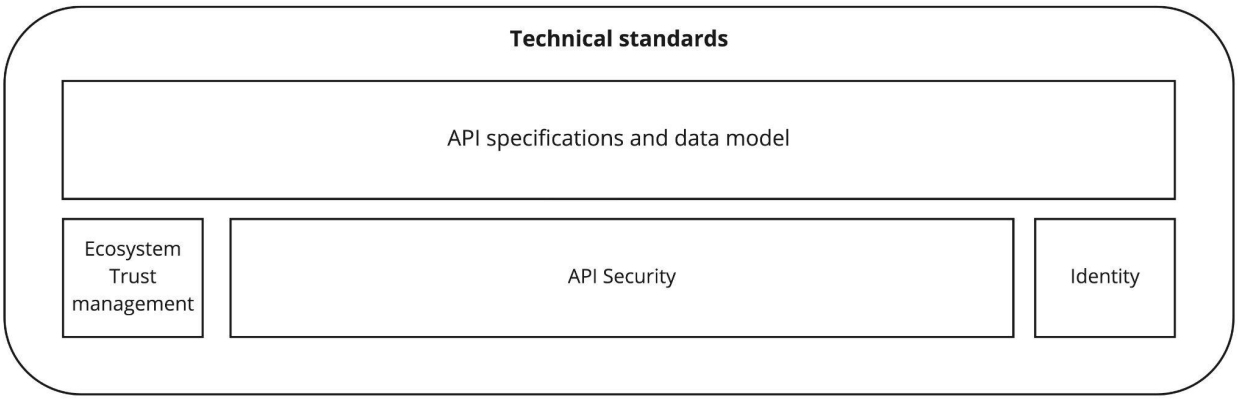
Open Data / API Ecosystem Building Blocks

In order to set up any API ecosystem, you need to select technical standards, and define business and legal rules to ensure a common, interoperable and secure process for all participants.



[7] https://www.berlin-group.org/open-finance

The typical API ecosystem setup requires the same technical building blocks as shown below:



The components of the API system are defined as follows:

Identity protocol defines how you transfer identity information from a Data Provider to a Data Consumer with End-User consent. Most ecosystems across the globe have adopted OpenID Connect 1.0**.** This end-user authentication OAuth 2 extension has been a de facto industry standard with broad vendor support.

Security profile defines how parties are authenticated, how the authorisation and the data request and response are secured, and how message integrity is preserved. One key decision the governing entity must determine is the standard for the API security profile.

While each ecosystem is still local/regional and specific to its jurisdiction, the majority of Open Banking / Open Finance / Open Data ecosystems have chosen OAuth-based FAPI as their API security profile. In addition, in some countries, FAPI CIBA (client-initiated backchannel authentication) is used for decoupled authentication across channels., This global adoption allowed multiple vendors to provide support for FAPI and reduce the costs of adoption.

While most live ecosystems (e.g.: Brazil, UK) are running on FAPI 1.0, some others (e.g.: Norway, Australia) started implementing FAPI 2. FAPI 2 simplifies the security profile, especially for Data Consumers (clients), and adds additional common building blocks (Grant Management, Pushed Authorisation Request and Rich Authorisation Request) to improve functionality and increase interoperability in the area of fine-grained consent capture and management.

For more context on FAPI, refer to the Foundation's "Open Banking, Open Data and the Financial-Grade API" whitepaper[8].

Trust management framework is required to establish a minimum trust level between different participants. How do I know who to trust and who is allowed to do what? There is almost no standardization in this area. To date, every jurisdiction has had to develop a trust management framework on their own, and determine key issues like what data holders and relying parties merit access to the ecosystem, how to ensure their conformance, and maintain the registry of participants.

In private ecosystems, trust establishment between the participants is simple, custom and controlled by one entity, usually the private entity itself or their delegated service provider. In Open Banking and Open Finance, trust management is usually done through the central registry typically managed

[8] https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

by the regulator, or an entity authorized by the regulator. In some cases, especially in Open Finance and Open Data, there are multiple ecosystem regulators involved.

Given that setting up an Open Banking framework across the globe is a repetitive task, a new breed of vendors has appeared on the market - ecosystem providers. For example, companies like Raidiam are industrializing the Open Banking ecosystem setup based on their experience in the UK, Brazil and other countries.

Functional API specifications and data models provide a common understanding of the data moving between the Data Providers and Data Consumers. In regards to API data models, there is some standardization as some ecosystems like OBIE and the Berlin Group have opted for data models based on ISO 20022 (where available), although some implementations deployed custom data models. When looking at variances between Open Banking implementations, the area of the greatest divergence is custom, functional API specifications controlled by a local governing body.

There are only a couple efforts to develop API specifications and data models ecosystems such as the Berlin Group (10 European countries) and FDX (US and Canada). Every other jurisdiction had to produce their own API blueprints.

In summary, across the three main implementation types, and the key components of those ecosystem, there are a few consistent configurations we gathered from our survey of markets:

	Private API ecosystems	**Open Banking ecosystems**	**Cross industry open data ecosystems**
Identity protocol	OpenID Connect	OpenID Connect	OpenID Connect
Security profile	Custom, usually OAuth based, can be FAPI	Dominated by FAPI	Dominated by FAPI
Trust management	Custom	Regional Central register	Regional Central register
Functional API specifications and data model	Custom with minimal ISO2022 usage	Regional with some ISO2022 usage	Regional
Trust management	Custom	Regional Central register	Regional Central register

Privacy Considerations

One potential privacy risk in any Open Banking, Open Data implementation is whether the relying party is asking for more information than is reasonable from the consumer, or whether the relying party is retaining or continuing to collect information without the user's awareness.

Currently each jurisdiction, be it government led or private sector led is defining the expectations for user privacy. It will be important for each individual jurisdiction to have appropriate privacy practices in place, and to ensure that cross-border use cases have suitable user transparency.

It is considered to be a best practice for an Open Banking ecosystem to unlock user's data and, at the same time, to encourage data minimisation, user control and transparency.

Challenges to Global Standardization

The OpenID Foundation "Open Banking, Open Data" paper mentioned above covers the reasons why standardization is important:

- Proven technology
- Secure
- Cost savings and vendor support
- Conformance testing and certifications[9]

These are several of the reasons most markets select global open standards like OpenID Connect and FAPI as part of their go to market approach. There are also many markets with market-led standards (e.g. India, Singapore, Berlin Group), which can also serve to deliver Open Banking use cases, but which adds to the complexity of enabling cross-border use cases.

The Berlin Group is one initiative working on standardization across multiple jurisdictions in Europe (Germany, France, Italy, Macedonia, Netherlands, Portugal, Austria, Slovakia, Serbia and etc.).

More information on leading standards bodies could be found in the Annex C.

Achieving a single global standard that would underpin Open Banking and Open Data for cross border use cases is particularly challenging for a few reasons:

- Open Banking and Open Data efforts to date have mostly been "jurisdiction led," and domestic use cases are prioritized over cross-border use cases.
- There is no "global" governance authority, and additional resources are required to coordinate with other jurisdictions
- and additional effort is required to coordinate with other authorities.
- Local markets tend to have a bias towards 'made here' design, such as standards developed by local experts, to services provided by local vendors.
- Local decision makers may not know about the benefits of global standards, and the ability to leverage global standards while retaining local governance and control.
- It is hard to standardize functional API specifications and data models due to local differences, and even large global banks like HSBC, Standard Chartered, Santander, and Citibank and payment providers like PayPal have challenges building platform services.

[9] https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

- Middleware providers like True Layer or Tink offer cross-border solutions for relying parties that need it.

Despite these challenges, users and businesses do conduct their personal affairs and business across jurisdictions, and it is inevitable that cross-border use cases will need to be supported to meet their requirements. It's a question of when, and how.

Phase 4: Is Open Data Crossing Orders Next?

Just as proprietary API services transitioned to Open Banking, and Open Banking moved to Open Finance and Open Data…. could the next stage be cross border transactions? Can all the challenges be overcome to enable global interoperability across domestic Open Banking and Open Data networks?

What if a UK-based fintech could help a customer with bank accounts in multiple jurisdictions with Personalized Financial Management? Or a car rental company in Norway can verify customer identity in Australia and accept a payment directly from an Australian bank? What are the use cases that could drive the adoption of Global Open Banking, Open Finance and Open Data? Who are the entities with the motivation to mobilize adoption, and is there sufficient appetite (commercial or regulatory) to overcome the friction, resource costs, and alternatives available today?

The next section will assess the relying parties and use cases most likely to drive the momentum, and make cross-border Open Banking and Open Data transaction a reality for people.

Global Relying Parties & Use Cases

Digital Platforms / Consumer FinTechs

The rise of the internet, mobile, apps and services have enabled new digital platforms to thrive, and start building out financial services of their own. Digital platforms could be some of the greatest beneficiaries of Open Banking, and Open Data "going global" given the lower cost to deliver and ease of scaling cross border. That said, many regulations have actively excluded Digital platforms from participation in Open Banking ecosystems to date. An article in PYMNTS.com (Jan 2022) indicates banks and FinTechs, although previously rivals in the early days of Open Banking, may now align to pressure governments /regulators to keep Digital Platforms out of Open Banking markets.[10]

Apple - Wallet for Payments, installments, P2P, Identity

In March 2022, Apple acquired UK Open Banking startup Credit Kudos[11], and it was the first public foray by Apple into services with an Open Banking dependency. This open banking startup is focusing on a specific use case: credit decisioning. The acquisition could be another stepping stone

[10] Open Banking and the Constant Threat of BigTech," Jan 13, 2022, PAYMTS.com. https://www.pymnts.com/digital-first-banking/2022/open-banking-the-constant-threat-big-tech/

[11] https://www.theblockcrypto.com/post/138898/apple-acquires-uk-open-banking-startup-credit-kudos

for Apple to become a fintech company and start offering lending services. Open Banking unlocks customer's data held at their existing banking institutions.

In June 2022, Apple announced a new service to make Apple Pay payments in 4 installments over a few months for no interest, without the Apple Pay merchant making any changes[12]. While the economics of this model is not clear yet, it is clear that Apple continues to expand their financial service offerings from Apple Pay, to Apple Card, to ID in Wallet, to credit decisioning (Kudos acquisition) and installments.

Apple has rolled out their Wallet products at different paces across the world, services like Apple Pay are available in 40+ countries while Apple Card and ID in Wallet is (currently) only available in the US. Given its track record to offer products and services to its customers globally, it's reasonable to assume Apple will be interested in offering Open Banking-linked services in other markets.

Block - P2P Payments & Installments

Block, formerly known as Square, has two cross border products and services. The first is Afterpay, a global fintech company operating “buy now, pay later (BNPL)” service in Australia, the United Kingdom, Canada, the United States, and New Zealand with 16m+ users[13]. The second is the Cash App is a highly successful service developed by Block that allows it to make peer-to-peer money transfers in multiple jurisdictions. Currently, this service is available in the United States and United Kingdom and it has grown from 3m to 44m+ plus users in ~5 years[14].

Google - Open Banking APIs, P2P Payments, Wallet

In 2021, Google acquired Japanese payment service startup Pring[15].This fintech company focuses on P2P payment in Japan and it is licensed. Any Open Banking obligations on payment providers in Japan would likely apply to Google as well.

Google also offers Google Pay, Google Wallet and a range of payment and identity services globally.

PayPal - P2P Payments, Merchant Acquiring, & More

PayPal is a fintech operating global payment that can be used in 200+ countries, with over 200 ways to enable payments, both credit and debit, and a wide range of alternative methods.

Since PayPal is a regulated payment services provider in some jurisdictions, they are obliged to enable Open Banking to conform to regulation. To achieve this, PayPal’s team has to support a variety of API and security standards in each country.

Global companies like PayPal, could benefit from having a consistent, global approach to Open Banking standards and market requirements.

---

12 https://developer.apple.com/apple-pay/whats-new/

13 https://en.wikipedia.org/wiki/Afterpay

14 https://www.businessofapps.com/data/cash-app-statistics/

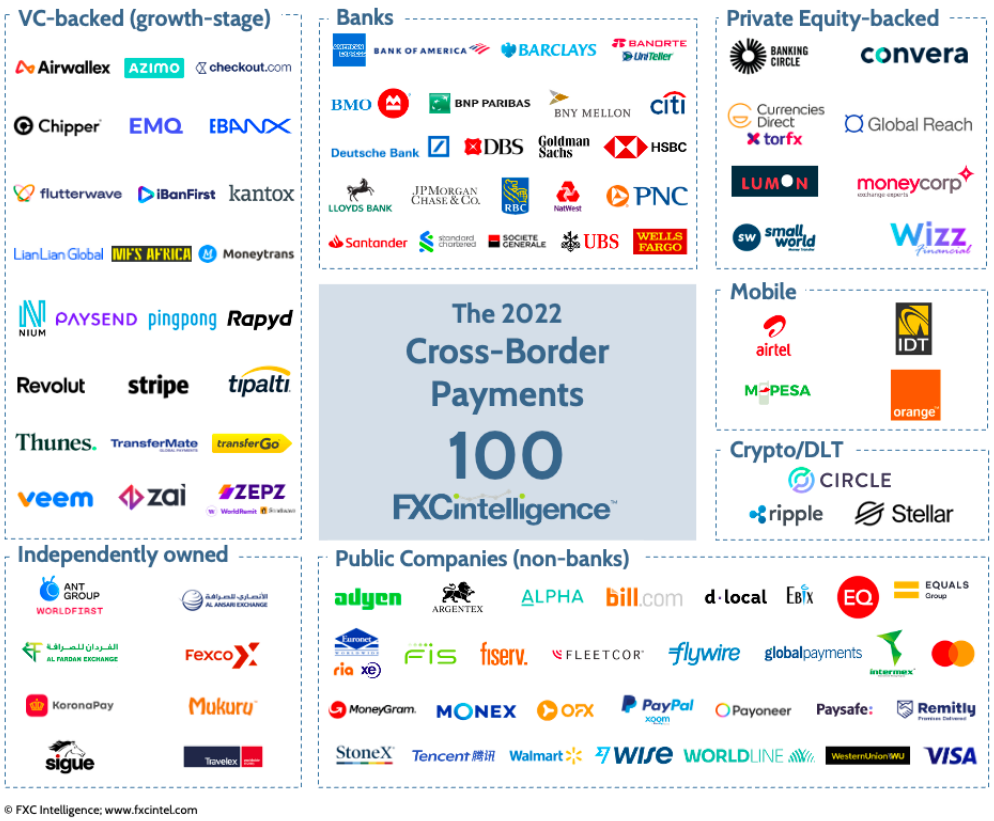
15 https://www.pring.jp/news_info/227

Cross Border Payments Sector

A wide range of financial service and payment providers are in the lucrative cross-border payments sector. The Digital platforms mentioned in the prior section all participate in cross-border payments as do traditional banks and money service companies (Western Union) and FinTechs (Wise).

SWIFT gpi (Global Payment Initiative) a new standard for handling cross-border payments that was created as a result of collaboration between SWIFT and the global banking community.

FXC Intelligence has published The Top 100 Cross-Border Payment Companies report in 2020, 2021 and in 2022[16]. According to his report, the cross-border payments sector continues to grow, and investors continue to back a range of different business models and technologies. This demonstrates the unfulfilled need in the market, especially in the fragmented B2B payments space.



© FXC Intelligence; www.fxcintel.com

Beyond private markets' appetite to deliver compelling cross-border payment services, we are also seeing governments set goals to scale cross border payments as well. More below in the Government section.

International Payment Networks

Mastercard

As a strategic initiative, Mastercard has been making significant investments in its open banking platform over the last few years, giving them reach across several jurisdictions. In their own words, “Open banking is democratizing financial services by putting consumers at the center of where and

[16] https://www.fxcintel.com/research/reports/the-top-100-cross-border-payment-companies

how their data is used to provide the services they want and need."[17]. Their investments show their commitment to this strategy:

- February 2019, Mastercard announced its partnership with Token, an open banking platform provider that operates in 13 countries in Europe[18].
- June 2020, Mastercard has made a significant investment by purchasing Finicity for US$825m[19], a service operating primarily in North America.
- September 2021, MasterCard acquired European open banking platform Aiia.

In parallel, Mastercard has been investing in its cross-border digital identity solution and has discussions in multiple markets like Egypt, Montenegro, Australia.

Visa

Visa appears to have a similar strategy. In 2020 they sought to buy US financial service aggregation company Plaid for $5.3B before the Department of Justice filed in November 2020 to block the deal, and Visa ultimately walked away from the deal in 2021. Shortly after in June 2021, Visa acquired European open banking platform Tink for EUR1.8b, giving them access to "more than 3,400 banks and financial institutions, reaching millions of bank customers across Europe"[20]. In November 2021, Visa invested in Australian open banking platform Basiq, expanding their global coverage.[21]

Payment Network Summary

Both Visa and Mastercard have consistently demonstrated their keen interest in global open banking solutions by investing significant amounts of funds over the last few years. To date, the acquired solutions operate in one region where they originated (e.g.: EU and US / Canada), the only option these credit cards schemes had being to acquire intermediaries that would simplify integrations per region and speed their time to market.

While credit card schemes themselves are not subject to Open Banking regulatory mandate, their ecosystem of merchants and fintechs could benefit from open banking data becoming more accessible in many jurisdictions.

However, it is reasonable to believe that payment networks that are inherently global, and benefit from economies of scale, will benefit from global interoperability standards that lower costs, simplify market expansion, and open up new product and service offerings.

The Sharing Economy

To improve rider safety, drivers need to perform identity verification and to improve payment experience, providers like Uber and Lyft needs to connect to different payment schemes available in the supported areas.

---

17 https://investor.mastercard.com/investor-news/investor-news-details/2021/Mastercard-Expands-Open-Banking-Reach-with-Acquisition-of-Aiia/

18 https://token.io/press/mastercard-selects-token-io-as-a-partner-for-its-new-open-banking-hub-1

19 https://investor.mastercard.com/investor-news/investor-news-details/2020/Mastercard-to-Acquire-Finicity-to-Advance-Open-Banking-Strategy

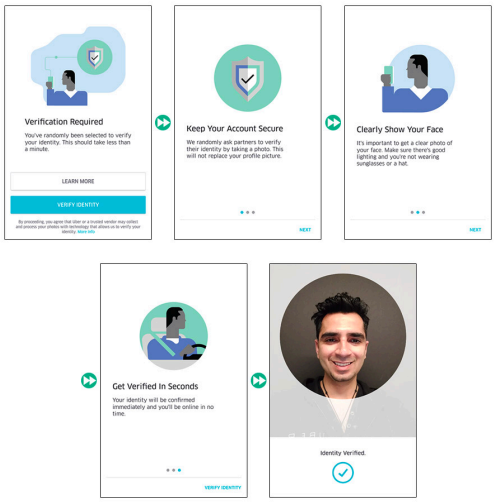
20 https://www.businesswire.com/news/home/20210623006027/en/Visa-To-Acquire-European-Open-Banking-Platform-Tink

21 https://www.pymnts.com/news/investment-tracker/2021/visa-invests-in-open-banking-platform-basiq/

Currently, these companies have to access identity and financial services differently in each country (if such services are available at all) and they will significantly benefit if this access could be standardized, lowering their development and maintenance costs, and potentially their transaction costs as well.

Sharing economy sector is dominated by global companies operating in different countries across the world: Airbnb, Uber, Taskrabbit and similar companies.

Uber alone is now operating in 72 countries. The scale of the financial opportunity is already material, as PWC predicted back in 2015 that sharing economy revenue will grow from $15 to $335 billion dollars[22]. Even modest cost savings or easier market entry can translate to meaningful margin improvements and growth.



[23]

Social Networks - Identity & Payments

Global social media networks, like Facebook (~3b users) or Twitter (200m+ users), have been under pressure by the public and legislators to better verify their users to prevent anonymised, harmful activity and to provide traceability if an offense occurs (e.g. scams, cyberbullying)[24]. Proper identity verification could reduce occurrences of fake users, fake news and false influencers. Twitter reports that fewer than 5% of accounts are fakes or scammers, commonly referred to as “bots”[25], but even a small number of fake accounts can be harmful to the online community. Today, Twitter provides an ability for users (usually higher profile individuals) to verify their identity to let the audience know that their account is authentic, the well-known “blue checkmark” for verified accounts. The opportunity to scale this “Twitter Blue” service with a blue checkmark should expand to a wider audience of users (e.g. those willing to pay $3/month). This topic is widely discussed in traditional and social media given the advocacy of this by Elon Musk as part of his Twitter takeover bid.[26]

---

[22] https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/sharing-economy-en.pdf

[23] https://timeattackmanila.com/news/generalnews/ubers-new-safety-feature-now-require-drivers-take-selfies/

[24] https://petition.parliament.uk/petitions/575833

[25] https://theconversation.com/how-many-bots-are-on-twitter-the-question-is-difficult-to-answer-and-misses-the-point-183425

[26] https://outsider.com/news/elon-musk-says-everyone-who-signs-up-for-paid-twitter-service-should-get-blue-check-mark/

Facebook launched a 'Page Publishing Authorization' for some Facebook pages, with Instagram (1b+ users) implementing a system to verify some suspicious pages.

Some networks, like Facebook and TikTok (~700m+ users), perform some form of age verification to prevent users under the age of 13 from accessing their app. While initially they relied on users' self-attestation, now they are increasingly employing AI algorithms to determine the age of its users, given the lack of other authoritative digital identities (e.g. government issued digital IDs).

TikTok is also planning to test ways to age-restrict some types of content in its app[27]. This is not possible without identifying the users and/or their guardians.

Entities like Google are also obliged to comply with regulation on age and content restrictions for their platforms (e.g. YouTube). Two key pieces of EU legislation:

- Age Appropriate Design Code **(AADC):** If you are not compliant with the Code, you are likely to be considered in breach of the GDPR and the Data Protection Act 2018, and be exposed to fines of up to €20 million or 4% of your annual worldwide turnover, whichever is higher.
- **Audiovisual Media Services Directive (AVMS):** to protect minors from harmful content, and to protect the general public from incitement to violence or hatred and content constituting criminal offenses.

It's worth noting that most social media businesses rely on advertising, so they have a need to be able to accept and route payments across borders to fund their business.

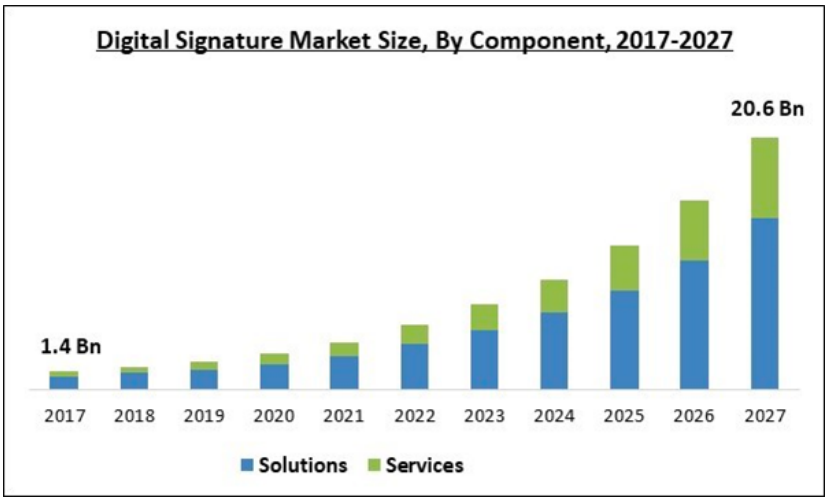
Other types of global services, like dating and gaming are either regulated or choose to perform age verification. For example, in Japan dating services have to rely on mobile network operators' (MNO) verification services in the absence of other widely accepted options. MNOs themselves are required to perform KYC checks for all subscriptions.

Given the global nature of these social media businesses, creating a global service would require local market specific integrations… unless a global, consistent and interoperable approach to identity and payment can be achieved.

[27] https://www.engadget.com/tik-tok-is-testing-ways-to-age-restrict-content-for-teens-100010082.html?src=rss

Global Digital Signing Providers

COVID-19 pandemic drove the adoption of digital signing across the globe. According to Research and Markets, digital signing market is expected to continue to grow to US$ 20+ billion by 2027:



Global providers like Adobe and DocuSign specialize in providing core document signing capabilities. In order for a user to sign a document, then need to be authenticated. This means that document signing solutions need to integrate with authentication providers.

eIDAS regulation standardized the process of electronic singing and its authentication requirements in Europe, but, unfortunately, it only works in Europe[28].

Global Assured Identity Network (GAIN) initiative is working on defining a consistent approach for Relying Parties to integrate with different Identity Information providers across the globe. Digital signing is one of the key use cases pursued by the GAIN community[29].

Government Strategy

The Government strategy that underpinned Open Banking and Open Data regulations started with user-consent based data sharing, enabling competition, and stimulating innovation. Those motivations are still driving 20+ markets to expand or initiative Open Banking and Open Data implementations.

But now Governments want to do even more, and Open Banking and Open Data implementations and ecosystems offer a useful playbook to inform health, identity, cybercrime, and cross-border payments.

“Open Health” is gaining traction with a similar goal of enabling people to move medical records between providers, and provide consent for a wide range of use cases. Covid-19 laid bare the problems in most jurisdictions with poor identity infrastructure that undermined the ability to coordinate testing, vaccine distribution, and balance user privacy with data. In 2021, Digital

[28] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+-+Get+started

[29] https://gainforum.org/GAINWhitePaper.pdf

Government Exchange report “Digital Identity in Response to Covid19” was released with contributions from Australia, Canada, Finland, Israel, New Zealand, Singapore, the Netherlands, the United Kingdom, and the World Bank (as an observer). The paper offers pathways to mutual recognition and/or interoperability between existing digital identity schemes.[30] In the same spirit, but at a more tactical protocol level, the OpenID Foundation is publishing a whitepaper “The Global Open Health Movement: Empowering People and Savings Lives by Unlocking Data”[31], to look at the identity and health standards landscape, current policies and regulations, and outline key recommendations to close gaps in standards.

Government has also recognized the potential for government issued digital IDs, and a wide range of initiatives are underway globally now ranging from the EU Digital Wallet efforts, the Arizona, Maryland, and Transportation Service Authority (TSA) partnerships with Apple to enable ID in Wallet (with many other US states in the pipeline), and similar efforts globally to leverage the ISO 18013-5 Mobile Driving License, W3C Verifiable Credential standards, and enable relying party acceptance both online and in person. Similar to Open Banking initiatives that start domestic led, so are government issued identity credential programs often jurisdiction led. That said, government officials have a strong appreciation of the need for their residents and business to travel and conduct business outside of their jurisdictions, and recognize the value of international standards, collaborations, and forums that will facilitate global interoperability of identity capabilities.

Cybercrime, borne of illicit activities with unquantifiable human impact, costs the global economy up to 5% of GDP per year. Despite the sums spend on anti-money laundering and anti-terrorist financing, so far it has not been effective. For every $1,000 of 'illegal funds' in the financial system, $100 is spent on compliance, but only $1 is intercepted or merely 0.1%. Building robust government issued digital identity capabilities and pairing them with globally interoperable digital identity schemes is a viable solution towards countering cybercrime at scale. This concept is being progressed by the open source, non-profit efforts of the Global Assured Identity Network participants.[32]

Last but not least, the G20 has made cross-border payments a key priority, and a framework program to realize the potential[33]. The Financial stability Board (FSB) together with the Committee on Payments and Market infrastructures developed a roadmap to address cost, speed, transparency and access to cross-border payments by consumers and businesses.

[30] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

[31] https://openid.net/wordpress-content/uploads/2022/07/OIDF-Whitepaper_The-Global-Open-Health-Movement_1st-Editors-Draft_2022-07-21.pdf

[32] https://nat.sakimura.org/2021/09/14/announcing-gain/ and the openid.net/gainpoc

[33] https://www.fsb.org/2021/10/g20-roadmap-for-enhancing-cross-border-payments-first-consolidated-progress-report/

The G20 roadmap consists of 19 building blocks, as seen in the diagram below:

Source: CPMI: Enhancing cross-border payments: building blocks of a global roadmap - Stage 2 report to the G20 (July 2020)

If a path for Open Banking, Open Data to “Go Global” is achievable, it could address 6 of the 19 building blocks:

- **Block 5: Applying AML/CFT** rules consistently and comprehensively, which can be facilitated with protocols like OpenID Connect for IDA that includes reference to the policy that was followed in the originating jurisdiction so the relying party can simplify their own policy assessment.
- **Block 8: Fostering KYC and identity sharing**. Consistently identifying customer customers and beneficiaries is required to make cross border payments, identity and data sharing work. A mechanism to use international open source standards like FAPI can help with cross jurisdiction security profile, and standards like OpenID Connect can enable KYC and identity data sharing.
- **Block 6: Reviewing the interaction between data frameworks** and cross-border payments. Cross border data sharing might be impacted by national privacy and data protection legislation. Efforts like the Open Identity Exchange trust framework mapping can help relying parties make informed policy decisions on data they receive using open standards.
- **Block 14 - Adopting a Harmonized ISO 20022** version for message formats (including rules for conversion/mapping). Open data technologists are already exploring how they can distill requirements for key use cases to the minimum data sets required to simplify the functional requirements layer of cross border transactions.

- **Block 15 - Harmonizing API protocols** for data exchange. Non-standardised data formats create additional complexity, unnecessary transformation, delays and potentially manual processing. This also adds risk of misinterpretation and data loss, lowers data quality. Adoption of common message formats and standardized APIs *"can lead to additional efficiency gains by avoiding workarounds and translation from one implementation to another during integration of systems, thus facilitating interoperability and reducing the implementation costs for new providers and enhancing the ability to achieve fully automated straight through processing functionalities*"[34].
    - The BIS Innovation Hub, SWIFT ran ISO 20022 hackathon in March 2021 to highlight the potential of cross-border payments standardisation. 60 teams from payments and technology market participants demonstrated high interest and high potential of using common message standards and standardized API specifications[35]. Mojaloop built one of the winning entries with ISO2022 format payments via SWIFT routing to Mojaloop for last mile delivery (via an adapter).
- **Block 16: Establishing unique identifiers with proxy registries.** FSB is conducting analysis of developments in the use of Digital IDs in the financial sector to uniquely identify organizations and individuals participating in financial transactions. The Global Legal Entity Identifier Foundation developed a path after the Financial Crisis of 2007-8 to define a common approach to financial service legal entities, to help with transparency on linkages between people and entities. There is a need to extend this type of model further to include all types of relying parties, and to improve the binding between the natural person, their identity, and the digital services (and things) with which they are interacting.

[34] https://www.fsb.org/wp-content/uploads/P131021-1.pdf

[35] https://www.bis.org/press/p210325.htm

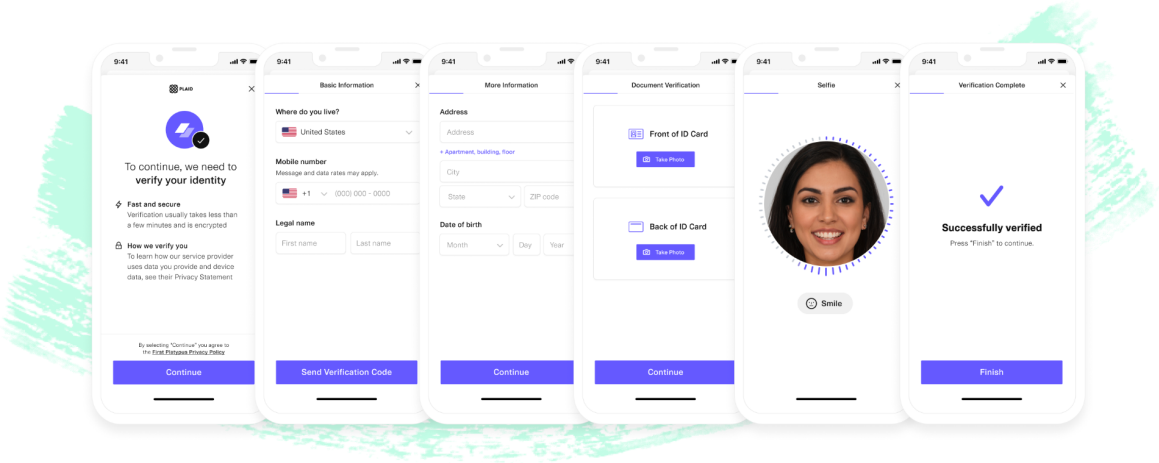
Solution

Option 1: Intermediary Providers

There are a number of technology providers in the market that are in a position to help Open Banking implementations integrate across borders.

Providers like TrueLayer and Moneyhub allow their global clients to abstract complexities of each individual jurisdiction with a simplified set of APIs for account information and payment initiation.

Plaid focuses on global account aggregation use cases, helping to connect apps with customer accounts in different financial institutions, which is a classic open banking use case. Recently, with the purchase of Cognito, Plaid expanded their offering into identity and KYC space[36]. By doing identity verification in-house, adding income verification and payments, Plaid can now provide end-to-end flow for their customers.



Stripe, on the other hand, started with payments, with a focus on making it easy for developers to accept payments in their digital platforms and apps. In 2021, Stripe expanded into identity with the product called Stripe Identity,[37] which sought to make it easy for developers to identify consumers. Recently, in May 2022, Stripe has announced further expansion into bank connectivity with Stripe Financial Connections[38]. Now their customers have fewer systems to connect to and manage, they can utilize the same platform for payments, subscriptions, payouts, ID and income verification.

In short, these and other intermediary providers specialize in providing developer friendly, global APIs for:

- Identity verification
- Account information
- Payments

36 https://plaid.com/blog/introducing-identity-verification/

37 https://techcrunch.com/2021/06/14/stripe-goes-beyond-payments-with-stripe-identity-to-provide-ai-based-id-verification-for-transactions-and-more

38 https://stripe.com/newsroom/news/financial-connections

They usually seek to use open banking APIs where available, with fallback to screen scraping and direct integrations.

Some of the providers are pure connectivity providers and some others are providing value add services on top of the base connectivity.

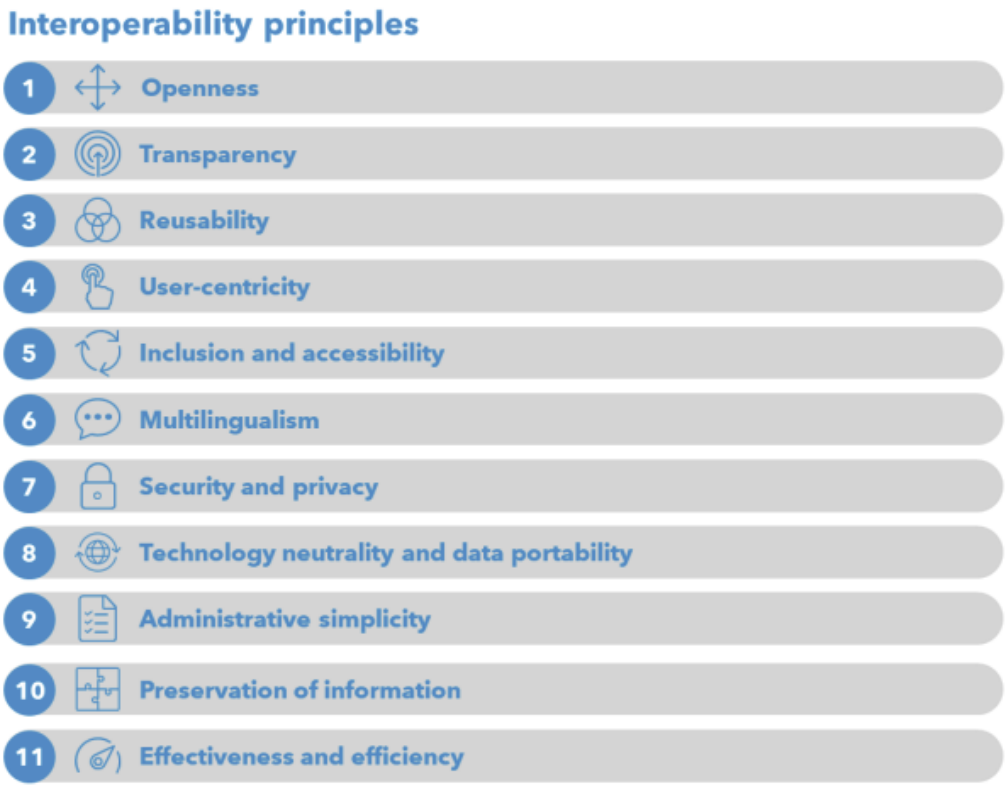
The downsides to these intermediary solutions are:

- Custom (non-standard) API and security profile specifications.
- Reliance on a vendor to support additional jurisdictions.
- Additional entity processing and storing end-user data, complicating privacy/ compliance requirements
- Switching friction and costs to change suppliers

Option 2: Direct Integration Between Participants of Different Schemes

Just as Open Banking in a single jurisdiction can offer economies of scale to domestic participants that benefit end consumers, so too can linking up Open Banking implementations or “networks of networks” also benefit end consumers.

The Digital Government Exchange defined a generic set of principles for cross border identity ecosystems that can equally apply as principles for cross-border Open Banking & Open Data, and is summarized in the chart below[39]:



[39] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

Global Open Banking Standards

To enable interoperability at the key layers of the ecosystem architecture, selection of the standards is the fundamental activity that will enable interoperability. It's best not to invent new standards where possible.

Identity Protocol

Use OpenID Connect to carry identity information between the participants. OpenID Connect is a common language already understood by many private and open API ecosystems[40]. Minimize the effort for participants to implement (minimally invasive structure)

Security Profile

Use FAPI security profile to protect APIs. This OAuth 2 based profile is used by the growing majority of the schemes. Use version 2 of FAPI framework (FAPI 2) because it delivers a simplified security profile and additional building blocks for interoperability.

Trust Management

In order to achieve global trust management, the following principles should be considered:

1) Trust establishment is done on a scheme-to-scheme level
2) Data transfer is peer to peer,
3) Select standards to enable interoperability between the schemes. (No participating scheme is obliged to change the standards they use internally.)
4) Minimize central infrastructure and governance, no central point of failure or control. No central decision making on what's allowed and what's not, no scheme can decide on behalf of the other scheme.
5) Participant on-boarding, vetting and integration is to be done at a local scheme level (by scheme operator). Ideal outcome for relying parties would be if they can "register once and use it everywhere".
6) Encapsulate "local" in the local scheme (e.g. delegate translation to the schemes and not the RP, such as via a shared or entity service, an SDK or another solution.)
7) Compliance with local regulation is the local's scheme responsibility.
8) Consumer/ business on-boarding is done at a local scheme level (vetting and integration by local, originating scheme operator)

Functional API specifications & data model

A practical approach to achieve interoperability at the API level between different markets could include the following:

- Deliver simplified APIs using that can be used across the globe.
- Optimize APIs for global RP consumption

[40] https://openid.net/specs/openid-connect-core-1_0.html

Delivery and Operational Considerations

- Autonomy of local networks is preserved (be it government led or private sector led).
- Start simple, keep it simple, iterate on demand.
- Start with enabling account information use cases cross border, then progress to more complicated use cases, like payments later. For example, a minimum viable product roadmap could consist of:
    - Use cases that only require account details
    - Use cases that only require Transactions information
    - Use cases that only require confirmation of Payee
    - Payment initiation use cases, e.g. simple immediate payments within the local ecosystem. Potentially could use v1 of OBIE Payment initiation API specification as a starting point. Payment initiation APIs should be payment scheme agnostic. Local schemes could decide what existing “payment rails” are used for payment execution.

Summary

Customer-consent based data sharing has moved through multiple phases already from Private APIs, to Open Banking, and Open Banking to Open Data and Open Health. We have seen 20+ markets move into implementing these programs, and building out scale in individual markets.

The next big horizon is Open Banking and Open Data Going Global, however, there will be new challenges to overcome. Unlike domestic Open Banking and Open Data initiatives, domestic governments will have limited influence on how the Open Baking and Open Data will materialize cross-borders.

The momentum to enable cross border Open Banking and Open Data will probably be driven by private entities, although governments are interested and may help nudge adoption where there is a credible path. In this context, private entities will need to see direct or indirect benefits for developing the capabilities required and interoperating with their peers.

The good news is that many Open Banking and Open Data technologists already see the cross-border potential, and are working actively to chart a course forward. A list of organizations on the “leading edge,” informally exploring this topic are noted in the Annex B. As noted in the use cases above, there are essentially three sources of benefit that might motivate a company to engage and invest:

- Cost savings from building a single global platform that can serve multiple jurisdictions with limited local integration
- Compelling products and services that unlock compelling cross border “open data” and identity, services that are not viable today
- Cost, time or other savings from payment initiation that are not served by existing technologies and networks (e.g. payment networks, SWIFT etc.)

Technologists that are already working on the cross border challenges see two paths forward, one driven by intermediaries and the other driven by direct network integrations or “network to network” interoperability. Advocates of the latter option are already working through standards selection, use cases, roadmap discussions, and stakeholder alignment to bring the next phase in Open Banking, Open Data to life.

Next Steps

We encourage the global community to comment on this whitepaper and to take part in the conversations below to help progress the cross border, open banking and open data path to market.

Comments on this Paper

Comments on this paper are warmly welcomed by August 26, 2022 to **director@oidf.org**. We welcome your thoughts and suggestions to ensure we accurately reflect the marketplace, key stakeholders, use cases, and options to enable cross-border Open Banking/ Open Data. We target publication of a final paper in September 2022.

Contribute to Organizations

OpenID Foundation

Working Groups such as FAPI and OIDC for Identity Assurance are progressing standards that may be selected for the interfaces to enable global interoperability. Any individual or entity can join the Foundation's working groups, at no cost, by signing the contribution agreement. More information at https://openid.net/wg/fapi/ and https://openid.net/wg/ekyc-ida/

The Global Assured Identity Network Proof of Concept Community Group is working on trust management and global identity scheme interoperability, global account scheme interoperability, and providing a safe space for interoperable testing of the same. More information at http://openid.net/gainpoc

Open Identity Exchange (OIX)

OIX Established an Interoperability Working Group working on scheme governance, and business level interoperability and liability.

Annex A: Acknowledgement

Lead Editor: Dima Postnikov

Contributors: Gail Hodges, Nat Sakimura, Daniel Goldscheider, Michael Richards, Kosuke Koiwai, Max Geerling, and Ralph Bragg.

Annex B: What is the OpenID Foundation?

The OpenID Foundation is a non-profit, open standards body specializing in identity standards. The Foundation's standards are currently used by over 3 billion people globally, and underpin millions of applications. The OpenID Foundation is truly open source, and standards and tests can be used by any entity at no cost.

The Open ID Foundation's vision is to help people assert their identity wherever they choose, and to deliver on that vision by leading the global community in creating identity standards that are secure, interoperable, and privacy preserving. In the case of Open Banking and Open Data, the Financial Grade API family of specifications are the most relevant, although other standards like OpenID Connect for Identity Assurance may play a role in the future.

The OpenID Foundation does not think any one standards body/non-profit, government, or private company will move the whole market to enable Open Banking, Open Data globally. The Foundation anticipates that many different organizations (public-led and private led) will need to collaborate to enable cross-border transactions. The OpenID Foundation offers its open standards for the Open Banking and Open Data community to consider both at a market level, and to enable cross border transactions. The Foundation also offers itself as a "safe space" for the community to convene, to interoperably test, and to develop tests that enable interoperability.

Membership in the foundation is not required to contribute, contributors only need to sign up to the Contribution Agreement of each (or all) Working Groups in which an individual or an entity would like to contribute. Nonprofit and government entities may become members for $250, individuals may join for $50, and private entities may join on a sliding scale based on number of employees. With this structure, the Foundation seeks to ensure a sustainable, and accessible model for the global community. For noting, the Foundation is funded roughly ⅓ by membership, ⅓ by certification fees, and ⅓ by directed funding projects requested by members.

The Board of the OpenID Foundation is keen to ensure that efforts like this whitepaper serve to synthesize the community's collective view on the landscape, and offer pragmatic recommendations that will facilitate the global conversation. For more information on the Foundation, see **openid.net** or contact **director@oidf.org**.

Annex C: Standards Bodies and Non-Profits

Role of Standards Bodies

Beyond the OpenID Foundation noted in Annex B, many other domestic, regional and global standards bodies are likely to make meaningful contributions to the approach for cross-border payments. As described in the Open Banking, Open Data and the Financial Grade API paper, there are a range of reasons and trade-offs between domestic-led and global-led standards.

Below are a few of the standards bodies active in the global discourse on Open Banking and Open Data, many of whom are already engaged in the cross-border transaction challenge. Comments from the global community to add to this listing are welcome.

Berlin Group (Germany, Europe)

The Berlin Group pursued standards to support local Open Data requirements. The Berlin Group standards have been implemented across the EU and are being extended to cover Open Finance. Berlin Group opted for data models based on ISO20022. The Berlin Group has been the primary driver of standards within the EU, along with PolishAPI in Poland and STET in France.

Banco Central do Brasil (Brazil)

The Brazilian central bank has taken a government-led, regulatory approach and went live in 2021, with a mandate for most data holders (banks) and relying parties to comply with its API standards. The Brazilian government selected FAPI as the security profile, and mandated certification by the OpenID Foundation for all Data Holders and relying parties. Open Insurance (OPIN) is expected to follow later in 2022, and Open Health may follow.

Data Standards Body (Australia)

In Australia, the Consumer Data Right went live in July 2020 granting consumers access to their banking data. Eventually, the Consumer Data Right is intended to extend across the wider Australian economy including Energy, Telecommunications and financial services such as insurance and investment providers.

Financial Data Exchange (US, Canada)

In the US and Canada there is a market-driven approach, spearheaded by the Financial Data Exchange. This non-profit entity is *"dedicated to unifying the financial services ecosystem around a common, interoperable and royalty-free technical standard for user-permissioned financial data sharing."*[41] There are currently over 200 participants, both data providers and data consumers. The market-driven approach may be supplemented by some level of regulation, both in the US and Canada.

[41] https://financialdataexchange.org/FDX/About/FDX/About/About-FDX.aspx

Financial Stability Board (G20)

This G20 entity is working on common building blocks for cross-border payment initiation.

Open Banking Implementation Entity (UK)

In 2016 the Competition & Monetary Authority (CMA) published a report on the UK's retail banking market found that older, larger banks did not have to compete as much to gain customer business while newer banks found it difficult, one solution was Open Banking. Since 2018, customers and SME ca share their current account information with third party entities who use that data to tailor apps and services.[42] The 9 largest banks are required to conform to regulation, and the UK government selected FAPI as the security profile to underpin this government-led implementation. The UK's selection of FAPI nudged many other markets to follow suit, opening the path for other markets to implement more swiftly, and potentially to interoperate more easily in the future. Now the UK is focused on expanding into Open Data, across other verticals like energy, telecommunications and pensions.[43]

Open Banking Nigeria

In Nigeria, Open Banking Nigeria led the effort, working with the Central Bank of Nigeria (CBN) and other stakeholders in a "hybrid" market and regulatory approach. Much of the standard was written by the market, with the Central Bank providing guidance. Notably one key goal is to enable financial inclusion, which is manifested in their efforts to enable users with "feature phones" as well as "smart phones", a capability that could benefit multiple markets. The Nigerian implementation is due to go live in 2022,[44] and they have selected FAPI as the security profile.

Payments New Zealand

A private sector-led Open Banking initiative, which selected and implemented FAPI as the security profile. The New Zealand Government is currently expected to publish a "Consumer Data Right" legislation (similar to the Australian government's approach) later this year.

Other Non-Profits

A range of other non-profits play an important role working on advocacy, best practices, and trust framework development. They also offer a vital "safe space" for the public and private sectors to convene, and work through shared problems and approaches. A few of the organizations active in the Open Banking/ Open Data domain are:

- Emerging Payments Asia
- FDATA
- iSprit
- International Institute of Finance
- Open Identity Exchange

---

[42] https://www.openbanking.org.uk/about-us/

[43] https://www.openbanking.org.uk/news/open-banking-and-obie-highlights-may-2022/

[44] https://openbanking.ng and https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf

Annex D: Bibliography

1. OpenID Foundation: Open Banking, Open Data, and the Financial Grade API (2022). <https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf>

2. OpenID Foundation: The Global “Open Health” Movement: Empowering people and saving lives by unlocking data (2022).

3. OpenID Foundation: OpenID for Verifiable Credentials (2022). <https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf>

4. GAIN: GAIN Digital Trust (2021) <https://gainforum.org/GAINWhitePaper.pdf>

5. Innopay: The current status of Open Banking and a glimpse into the future of Open Finance (2022), <https://www.innopay.com/sites/default/files/media-files/Open%20Banking%20Monitor%202022.pdf>

6. McKinsey Digital: What’s new in banking API programs (2022), <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/whats-new-in-banking-api-programs>

7. Australian Payment Network: TrustID Framework (2022), <https://www.auspaynet.com.au/insights/Trust-ID>

8. DGX Digital Identity Working Group: Digital Identity in response to COVID-19 ver.04 (2022), <https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf>

9. G20: G20 Roadmap for Enhancing Cross-border Payments (2021) <https://www.fsb.org/wp-content/uploads/P131021-1.pdf>

10. PWC: Sharing or paring? Growth of the sharing economy (2015) <https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/sharing-economy-en.pdf>