



Open Banking and Open Data: Ready to Cross Borders?

January 31, 2023

Version: Final

Lead Editor: Dima Postnikov

Contents

Introduction	4
Open Data Ecosystem Evolution	6
Phase 1: Private API Ecosystems	7
Phase 2: Open Banking Ecosystems.....	8
Phase 3: Cross-industry Open Data Ecosystems.....	10
What Have We Learned from Implementations to Date?	11
Leading Use Cases	11
Open Data API Ecosystem Building Blocks	11
Existing Ecosystem Analysis	13
Privacy Considerations.....	17
Challenges to Global Standardization	18
New Open Data Ecosystems	19
Monetization of Open Data?	20
Is Open Data Crossing Borders Next?	22
Global Relying Parties & Use Cases	23
Digital Platforms & Fintechs.....	23
Cross-border Payments Sector	25
International Payment Networks	26
The Sharing Economy	27
Social Networks & Content Providers.....	28
Global Digital Signing Providers	30
Government Strategy.....	30
Solutions	34
Currently Available Solutions	34

Proposed Open Standards Based Cross-Border Solution	36
Summary	41
Next Steps.....	43
Annex A: Acknowledgement.....	44
Annex B: What is the OpenID Foundation?.....	45
Annex C: Standards Bodies and Non-Profits	46
Annex D: Analysis of the G20 Roadmap for Enhancing Cross-Border Payments	48
Annex E: Bibliography.....	50

Introduction

Would you like to be able to see data across your bank accounts? Enable your tax advisor to see your financial information? Enable the App of your choice to make a payment or access transaction information? How about enabling those use cases across countries?

There is a global movement towards Open Banking and Open Data where a user authorizes the release of their data from one entity (a “Data Providers” like a bank or a utility provider) to an entity where they would like it to go (a “relying party” like a Fintech), and a user can enable this transaction across any Data Providers and any relying party in a market. Although this movement started with banking, it is now expanding to other verticals including user consent-based movement of information for investments, insurance, telecommunications, utilities and more.

The next big challenge is how and when to enable cross-border use cases, removing transaction friction from the millions of people and businesses that operate or would like to start operating across borders. However, there are two major complications:

Firstly, many markets impose regulatory limits around what personal data can be transferred or stored in other markets, not to mention whether or not financial services can be offered to their citizens by firms who are not licensed in that market.

Secondly, each market has their own version of Open Banking and Open Data, so users or businesses cannot leverage these emerging ecosystems to conduct Open Banking and Open Data transactions across borders.

Thus, users either cannot enable cross-border use cases at all, or they must use proprietary solutions. This paper explores what “good might look like” to remove this friction.

The intended audiences for this paper are government officials, ecosystem implementers of open banking open data, and experts in the adjacent fields of cross-border payments, data privacy, international trade and digital identity. Readers are encouraged to first read “Open Banking, Open Data, and the Financial-Grade API”¹, since it more fully covers the origins of this movement as well as the consumer and economic benefits, legal mandates, standards, and recommendations for domestic implementations.

This second paper focuses on the path to global interoperability including the benefits, market participants, standards, barriers and solutions.

We will start with consumer use cases and benefits. People and businesses are progressively global with each passing year. Here are three key facts:

- The global digital economy is estimated to be equivalent to a G7 country, and it is estimated to be growing 6 times faster than emerging markets (as of May 2020, World Economic Forum).²
- \$3.7 trillion world exports of “digitally delivered services” including financial services, insurance, information services, and others have tripled since 2005 (as of 2021, World Trade Organization).³

¹ Tonge, Dave. “Open Banking and Open Data and the Financial Grade API,” FAPI WG, OpenID Foundation: https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

² https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf

³ https://www.wto.org/english/res_e/booksp_e/wtsr_2022_c2_e.pdf

- 281M migrants living outside the country of their birth, or 3.6% of the global population, have tripled since 1970 (as of 2020, United Nations).⁴
- \$6.7 trillion or 9.4% of the global GDP is contributed by migrants (as of 2015, McKinsey).⁵

This means that the global digital economy and digital exports are growing exceptionally fast which impacts almost everyone, especially those with access to an internet connected device. Furthermore, migrants may be a modest share of the global population but they have a disproportionately high contribution to global GDP. It is reasonable to conclude that countries and businesses that best serve these consumers and businesses will be disproportionately successful as well.

Historically, global services have been the provenance of a few global entities (global banks, global digital platforms, global accountancy firms, etc.). These entities usually developed their own proprietary solutions, scaling staff to not only to ensure conformance to local laws, but to ensure market conditions remained favorable to their growth. The movement to enable cross-border open banking and open data will allow more people access to lower-cost, global services via local service providers.

Just as governments have played a central role in enabling domestic open banking and open data ecosystems, we anticipate these same governments will seek first mover advantages in enabling global interoperability as the “next step” in their domestic roadmaps.

There are several key benefits to governments that make this jump:

- Competitiveness of their domestic businesses abroad
- Competition and innovation in their domestic market
- Privacy and data protections for consumers and businesses
- Global financial stability.

Proactive government policies can influence the distribution of these gains, and mitigate the externalities of global market forces. As policy makers gain comfort in the operation of domestic open banking and open data platforms, we anticipate their desire to extend domestic “fair playing fields” to global trade, rather than prioritizing the protection of a few large firms. Many policy makers are already familiar with the premise that equal access to data empowers consumers to benefit from lower cost and friction, and smaller firms can more easily enter the marketplace and become competitive.

The whitepaper offers pragmatic recommendations on how to enable global interoperability:

- **Architecture based on “Networks of Networks”:** Connecting domestic ecosystems using a “networks of networks” approach allows “domestic sovereignty” (local governments exerting their natural authority over domestic networks), adding only minimal central infrastructure and governance.
- **Global standards:** Where possible, use global standards which unlock low-cost, secure connectivity between global market participants, such as the de-facto standards used in open data across the world like OpenID Connect, OAuth and FAPI.

⁴ <https://worldmigrationreport.iom.int/wmr-2020-interactive/>

⁵

<https://www.mckinsey.com/~media/mckinsey/industries/public%20and%20social%20sector/our%20insights/global%20migrations%20impact%20and%20opportunity/mgi-people-on-the-move-in-brief-december-2016.pdf>

- **Simplified API specifications and rules:** Global use cases merit simple APIs and rules. The next step is evaluating the optimal “home” for the working group(s) to (1) review existing standards against global requirements, (2) evaluate the optimal governance rules that best serve people and domestic network participants.

The final section of this paper will review solutions and detailed recommendations, the result of a year of deliberation by technologists fluent with open banking and open data implementations.

Another way to look at this paper is a technologist’s response to the World Economic Forum’s 2020 whitepaper on “Data Free Flow with Trust: Paths Towards Free and Trusted Data Flows,” (DFFT) albeit more narrowly on a “bottom’s up” approach on how we can achieve some of the DFFT global policy goals by building on existing networks of Open Banking and Open Data.⁶

Open Data Ecosystem Evolution

Although the Open Banking and 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, often depending on bespoke bilateral solutions between entities.

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 it is progressively difficult to achieve as phishing-resistant authentication capabilities are scaled.

Changes to the privacy and customer experience expectations, regulations, and pressure from fintechs have created a need to enable users to have ultimate control over their data (or “user consent-based data sharing”). It is becoming a norm that people need (and expect) 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 at scale.

With the development of secure API frameworks, it is now possible to share customer data securely and give customers the data-sharing control they expect. 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. API-based interoperability allows for a simple ecosystem scale instead of the historical need for point-to-point integrations. Over the past decade or so, we have seen these API-based access frameworks go through three phases of evolution: first private

⁶ https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf

ecosystems are established, then open banking ecosystems, and then cross-industry ecosystems.⁷ We are now seeing a fourth phase emerge, cross-jurisdiction data sharing:

Phase 1: Private API ecosystems.

Phase 2: Open banking ecosystems.

Phase 3. Cross-industry ecosystems

Phase 4: Cross-jurisdiction data sharing

APIs in this Phase 4 of cross-jurisdiction data sharing seek to address the following:

- Simplify existing cross-jurisdiction operations (e.g. international payments);
- Enable new data sharing use cases;
- Expand options for interoperation, whether as an addition to existing connectivity “rails” (e.g. global payment networks, SWIFT, etc.) or emerging “rails” such as decentralized finance models.

Today, a few major entities and standards bodies dominate the cross-border financial services landscape. However, there are new challenges to these traditional models from those who favor decentralized solutions and / or lower barriers to entry for new entrants. As calls to achieve global, regional and domestic sustainability of trade and trust persist (e.g. World Economic Forum’s Data Free-Flow with Trust, GDPR, and Consumer Data Rights) we will need to consider both existing and emerging models to achieve benefits for people at scale. One viable path is to leverage the API standards and domestic Open Banking and Open Data implementations (such as FAPI, UPI, the Berlin Group, etc.) to help realize these goals in practice using existing networks. Furthermore, if we consider the coexistence of multiple standards inevitable, then the emphasis shifts to how standards can best achieve interoperability to balance domestic sovereignty with the benefits of global scale, interoperability and security.

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. Prior to that, to get customer data, the fintechs used screen scraping, and unsolicited use of APIs exposed for internal clients. Privacy and security issues and also increasing API development maturity causes large Data Providers to start thinking about alternative approaches.

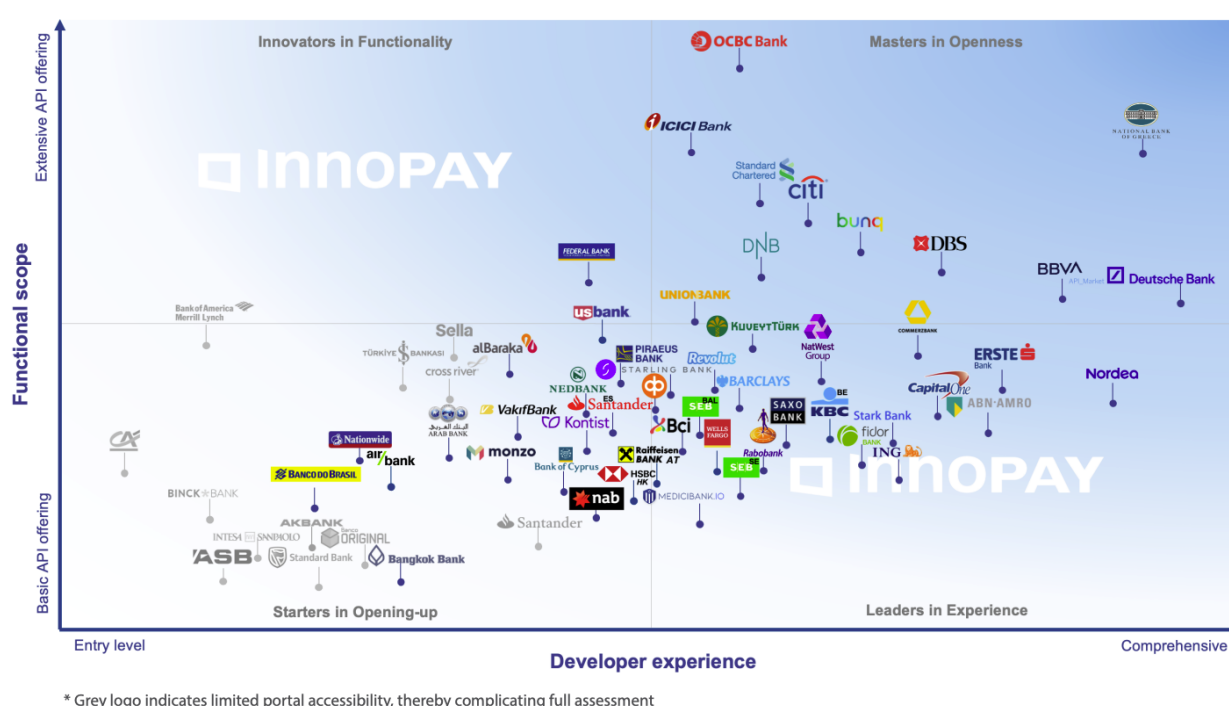
A number of leading banks and telecommunication companies attempted to set up their own API programs to provide access to customer data and banking functionality to external developers. Banks recognized that external API ecosystems could unlock partner integration, client connectivity, banking-as-a-service/-platform and ultimately increase innovation and establish 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 Hub⁸. These programs were unregulated and typically centered around one company, controlled by one entity, and were not mandated through government regulation.

⁷ Tong, Dave. “Open Banking and Open Data and the Financial Grade API,” FAPI WG, OpenID Foundation.https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

⁸ <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 are 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 2025⁹, 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 a year from 2021, and much more room to grow. Innopay's 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.¹⁰



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 and 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?

⁹ <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/whats-new-in-banking-api-programs>

¹⁰ <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:

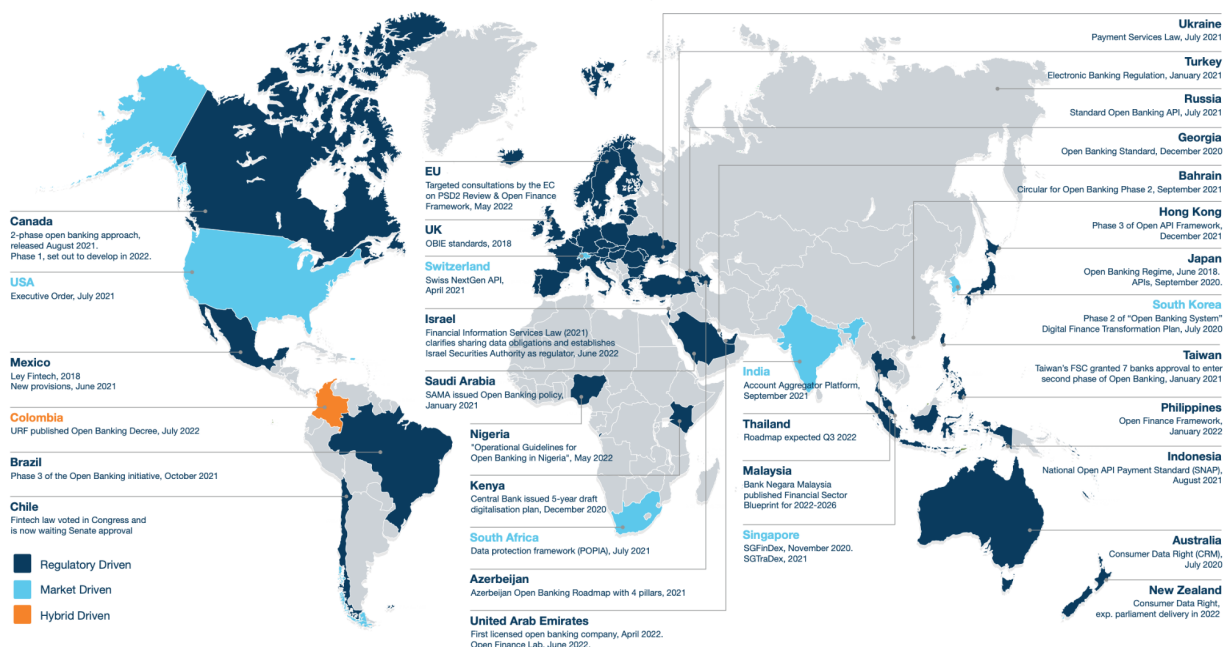
- Consistent way of accessing data across the whole industry
- Secure and customer-controlled data sharing
- Mandated user control (explicit consent)
- New features previously not possible
- More competitive marketplaces.

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, Brazil, 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, Brazil, Saudi Arabia). There are also hybrid scenarios where the regulators, like in Japan or in Europe (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 shows 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 rollout¹¹.

The World of OPEN BANKING

Data as at September 2022



¹¹ <https://www.konsentus.com/wp-content/uploads/The-World-of-Open-Banking-Sep-2022-1.pdf>

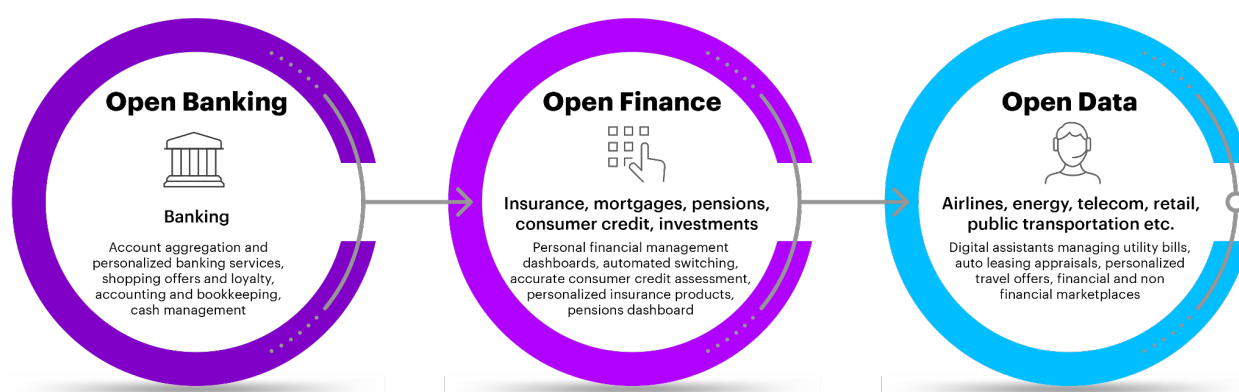
For more detail on local regulation and implementation status, standards selected by market, implementation considerations and best practices, refer to the OpenID Foundation's March 2022 White Paper on "Open Banking, Open Data, and the Financial-Grade API."¹²

Phase 3: Cross-industry Open Data Ecosystems

Once Open Banking and Open Data are 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 then to 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 Forrester, Open Finance will be a continuous process, "marking a fundamental shift in how customers access financial services and how firms deliver them," as demonstrated in the diagram below.¹³



The momentum to date towards Open Finance and Open Data has been driven by domestic markets, and usually, ones that are government controlled:

- Brazil launched Open Banking in 2021 and they have started implementing Open Insurance in 2022.
- In 2023, Australia is going live with the Open Energy sector expanding on its Open Banking ecosystem (Consumer Data Right) with telecommunications to follow.
- The UK is considering expanding Open Banking (live from 2018) to Open Finance to take care of a wider range of use cases, and or, to enable "smart data" as mentioned in the Queen's speech. The UK takes credit for exporting a "vibrant" open banking ecosystem to 80 countries.¹⁴

¹² https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

¹³ <https://www.forrester.com/blogs/open-finance-will-reshape-the-relationship-between-banks-and-their-customers>

¹⁴ <https://www.openbanking.org.uk/news/what-the-future-holds-for-open-banking/>

- The New Zealand government announced in November 2022 that their Consumer Data Right legislation will start with banking and extend to other verticals, similar to Australia's approach, and they noted that industry-led efforts have already started.¹⁵
- Berlin Group also extended their PSD2 API framework in the direction of Open Finance¹⁶.

Australia and Brazil, which at the moment of writing this whitepaper are expanding Open Banking to new verticals, decided to use the same API access framework for all verticals and participant types. By doing so, they are de facto creating national cross-industry ecosystems that will result in new use cases for the next generation of consumer applications. Other countries may not be able to move with the same speed to encompass new verticals, as not all government entities governing Open Banking will also have authority in other industry verticals. It is worth remembering that the global evolution of Open Banking into Open Data was not pre-planned. It happened slowly over the last decade in many jurisdictions and in many different ways. It's only now we can step back and appreciate what happened, look at the patterns and best practices, and think about the future directions.

What Have We Learned from Implementations to Date?

Leading Use Cases

Around the world, there are three sets of use cases that most if not all open banking or open finance ecosystems deliver as a priority:

- Consumer identity data
- Consumer account information data
- Payment initiation

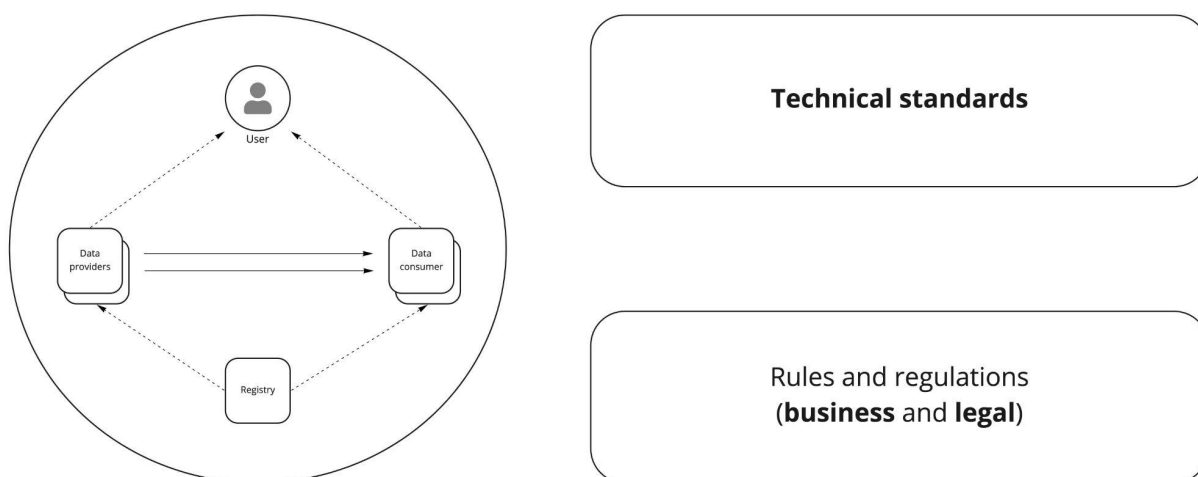
There are more similarities than there are differences in the use cases each ecosystem seeks to enable.

Open Data API Ecosystem Building Blocks

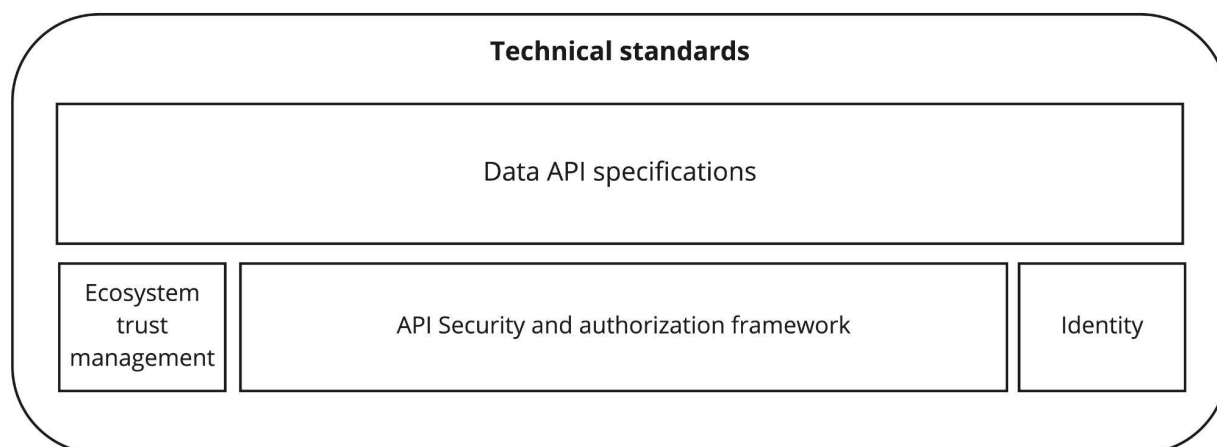
In order to set up any API ecosystem, you need to select technical standards, and define business and legal rules to ensure a common, interoperable and secure process for all participants.

¹⁵ <https://www.beehive.govt.nz/release/govt-moves-introduce-open-banking-give-customers-better-deal#:~:text=Open%20banking%20ensures%20banks%20must,banks%2C%20David%20Clark%20said>

¹⁶ <https://www.berlin-group.org/open-finance>



The typical API ecosystem that involves customer data sharing between participants requires the same technical building blocks as shown below:



The components of the API ecosystem are defined as follows:

Identity is a protocol that 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.

Data Functional API specifications are functional **and data models to provide** a common understanding of the data moving between the Data Providers and Data Consumers.

API Security and authorization framework is a profile that defines how parties are authenticated, how the authorisation and the data request and response are secured, how consent is captured and how message integrity is preserved. Determining the API security profile is one of the key decisions that have to be made, and it has a significant impact on security and interoperability.

Ecosystem Trust management is a framework required to establish a minimum trust level between different participants. How do I know who to trust and who is allowed to do what?

Existing Ecosystem Analysis

The independent Open Banking Global Interoperability working group performed a detailed analysis of existing Open Banking ecosystems across these four key dimensions. The systems analyzed included:

- Open Banking (OB UK)
- Financial Data Exchange (FDX US)
- Consumer Data Right (CDR Australia)
- Open Banking (OB Brazil)
- Payments Services Directive 2 (PSD2 EU)
- Data Empowerment and Protection Architecture (DEPA India)

Their findings are as follows:

Component / Ecosystem	Open Banking UK	FDX	CDR	Open Banking Brazil	NextGenPSD 2 / Berlin Group	DEPA (AA + UPI)
Jurisdiction	UK	US	Australia	Brazil	EU	India
Model	P2P	P2P	P2P	P2P	P2P	vi hub / broker
Identity						
Framework	OpenID Connect	OpenID Connect	OpenID Connect	OpenID Connect	N/A	Proprietary (based on a mobile number)
Data API Specifications						
API specifications	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary
Data model	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary

Account information API	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary	Proprietary
Payment initiation API	Proprietary	Proprietary	No (planned)	Proprietary	Proprietary	Proprietary
Functional API certification	Full proprietary (mandatory for CMA9)	Partial proprietary (optional)	Partial proprietary (optional)	Full proprietary (mandatory)	N/A	Proprietary
API Security and Authorization framework						
Base security profile	FAPI	FAPI	FAPI	FAPI	Proprietary OAuth2 profile	Proprietary
Security profile certification	OIDF (mandatory for CMA9)	OIDF (optional)	OIDF (optional)	OIDF (mandatory)	Proprietary	Proprietary (mandatory)
Consent capture, management and enforcement						
Authorization framework	OAuth 2	OAuth 2	OAuth 2	OAuth 2	OAuth 2 and other modes	Proprietary
Redirect authorization flow	Y	Y	Y	Y	Y	Y
Decoupled authorization flow	CIBA	CIBA	N	CIBA	Proprietary	Proprietary
Authorization request delivery	Signed request object via front channel	Signed request object via PAR	Signed request object via PAR	Signed request object via PAR	Unsigned request object via front channel	Request object via PAR
Fine grained consent	Custom lodging intent	RAR	N	Custom lodging intent	Custom lodging intent	Custom consent

						handled by trust anchor
Ecosystem trust management						
Trust anchor	Proprietary central registry	Proprietary distributed registries	Proprietary central registry	Proprietary central registry	Certificates under PSD2 and eIDAS	Proprietary distributed registries (regulated non-bank finance companies)
RP registration	Customized dynamic client registration	Customized dynamic client registration	Customized dynamic client registration	Customized dynamic client registration	N/A (pre-registered with trust registries)	N/A (pre-registered with trust registries)

* P2P - Direct Data Provider to Data Consumer.

Most ecosystems across the globe have adopted OpenID Connect 1.0 for their Identity protocol. As noted above, this end-user authentication OAuth 2 extension has been a de facto industry standard with broad vendor support.

While each ecosystem is still local or regional and specific to its jurisdiction, the majority of Open Banking and Open Data ecosystems have chosen the OAuth-based FAPI as their API security profile. FAPI 1.0 benefits from being a standard proven now across multiple jurisdictions, and both FAPI 1.0 and FAPI 2.0 have had formal security analysis conducted by the University of Stuttgart.¹⁷¹⁸ Many markets like the fact they can maintain domestic sovereignty of their ecosystem design while also benefiting from proven security profiles that reduce risks while ensuring ecosystem interoperability. In addition, in some countries, FAPI CIBA (client-initiated backchannel authentication) is used for decoupled authentication across channels. The fact that multiple markets selected the same standards had a material secondary benefit, as global adoption has allowed multiple vendors to provide support for FAPI and reduce adoption costs for both data providers and data recipients.

While most live ecosystems (e.g.: Brazil, UK) are running on FAPI 1.0, some others (e.g.: Norway, Australia, Saudi Arabia) started implementing or building towards FAPI 2.0. The second version of FAPI not only simplifies the security profile, especially for Data Consumers (clients), but also has a much broader interoperability scope. Unlike FAPI 1.0, FAPI 2.0 standardizes the way authorization requests are included in the authorization flow, and the way grants (authorizations) are managed with Grant Management APIs. The introduction of Grant Management, Pushed Authorisation Request (PAR), and Rich Authorisation Request (RAR) in FAPI 2.0 will strengthen interoperability in the area of fine-grained consent capture and management. For more context on FAPI, refer to the

¹⁷ Daniel Fett, Pedram Hosseini, and Ralf Küsters, An Extensive Formal Security Analysis of the OpenID Financial-grade API. 2019 IEEE Symposium on Security and Privacy (S&P 2019). <https://ieeexplore.ieee.org/document/8835218>

¹⁸ "FAPI 2.0 - Announcing New Drafts and Security Analysis." OpenID Foundation blog. <https://openid.net/2022/12/19/fapi-2-0-announcement/>

Foundation's "Open Banking, Open Data and the Financial-Grade API" whitepaper or the FAPI working group homepage at <https://openid.net/wg/fapi/>.¹⁹

There is almost no standardization in ecosystem trust management. To date, every jurisdiction has had to develop a trust management framework on their own and determine key issues like which Data Providers and relying parties merit access to the ecosystem, how to ensure their conformance, how to maintain the registry of participants, and what governance binds ecosystem 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 Data, trust management is usually done through the central registry, typically managed by the regulator or an entity authorized by the regulator. In some cases, especially in Open Finance and Open Data, there may be multiple ecosystem regulators involved. Although the core components may be the same of any Open Data implementation, regulator span of control can complicate the governance and implementation due process.

With the rising global adoption of Open Data, setting up trust ecosystems has become a repetitive task. The similarity of these ecosystems (same or similar security profiles, consent requesting flow, consent management APIs) has triggered an ecosystem of its own to emerge: new types of vendors. Some vendors specialize in providing end-to-end Open Banking or Open Data enablement platforms for data providers or relying parties, while a new breed of vendors has appeared - trust 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. Other companies like Ozone API offer sandboxes (or reference implementations) to further accelerate market adoption. These vendors serve the public or private entities that govern Open Banking or Open Data implementations, allowing these "managing entities" to outsource select technical functions and "fast track" ecosystem launches. In contrast, markets that have taken a bespoke approach require each jurisdiction to produce its own API blueprints, with homegrown end-to-end security and interoperability dependencies.

Standardization of security profiles and consent flows triggered the emergence of a new type of vendors assisting clients with different components of identity and access management. Companies, like Cloudentity and Authlete, specialize in providing compliance with the selection of security profiles, consent flows and consent management APIs while giving Data Providers the freedom of bringing their own data APIs. Other companies, like Ozone API and FinansysTech, go a step further by offering a complete turnkey 'open finance in a box' solution designed to meet all functional API requirements of defined standards in a number of markets globally. The unique quality of these companies is a rapid adoption of modern industry standards which is extremely important in a constantly changing world of identity.

The standardization of security profiles, consent flows, and consent management APIs also has a notable impact on the design of private ecosystems. In the regions where there is no open banking regulation and framework in place, pioneer banks willing to expose their proprietary data APIs to fintech also need security and consent profiles. These organizations often leverage existing security and consent profiles defined in one of the jurisdictions where open banking regulation and framework are in place. This phenomenon makes these private ecosystems almost and de facto an extension of certain jurisdictions at the consent and security profile level. While it is not a true cross-border interoperability it will likely have a positive impact on future cross-border data sharing. Standardization of security and consent profiles and vendor support enables quick implementation of secure private ecosystems. For

¹⁹ https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

example, if a bank (anywhere in the world) would like to start new API program for their partners and customers, there are proven building blocks that it could use to achieve quick time-to-market.

There are only a couple of cross-jurisdictional efforts to develop API specifications and data models, such as the Berlin Group (10 European countries) and Financial Data Exchange (FDX) (US and Canada). 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.

In summary, this is a current level of standardization across different ecosystem components as gathered from our survey of markets:

	Standards
Identity protocol	OpenID Connect
API security profile and authorization framework	Dominated by FAPI (OAuth2)
Trust management	Regional, central register
Functional API specifications and data model	Regional, no standard

Privacy Considerations

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 minimization, user control and transparency.

Many countries have existing privacy laws in place like General Data Protection Regulation in Europe (GDPR), Brazil's Data Protection Bill of Law (LGPD), the Australian Privacy Act and the California Consumer Privacy Act (CCPA).

One potential privacy risk in any Open Banking and 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. There might be additional complications with cross-jurisdiction data sharing if local regulations prevent this from happening.

Some markets, like Open Banking Brazil, already take user privacy regulation into account. However, the interoperability of these regulations needs to cover subjects like storing users' data cross-border, managing the users' authorisation, access revocation and expiration.

Challenges to Global Standardization

The OpenID Foundation “Open Banking, Open Data” whitepaper referenced earlier explains in depth why standardization is important, including:

- Proven technology
- Secure
- Cost savings and vendor support
- Conformance testing and certifications²⁰.

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 actively deliver Open Banking use cases. The Berlin Group is one initiative working on standardization across multiple jurisdictions in Europe (e.g. Germany, France, Italy, Macedonia, Netherlands, Portugal, Austria, Slovakia, Serbia and etc.) and India is working on cross-border implementations of the UPI standard, with neighboring markets. More information on leading standards bodies can be found in Annex C and the “Open Banking, Open Data” whitepaper.

The complication is that each instance of a market or region-specific standard adds complexity to the global journey to enabling cross-border use cases. 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:

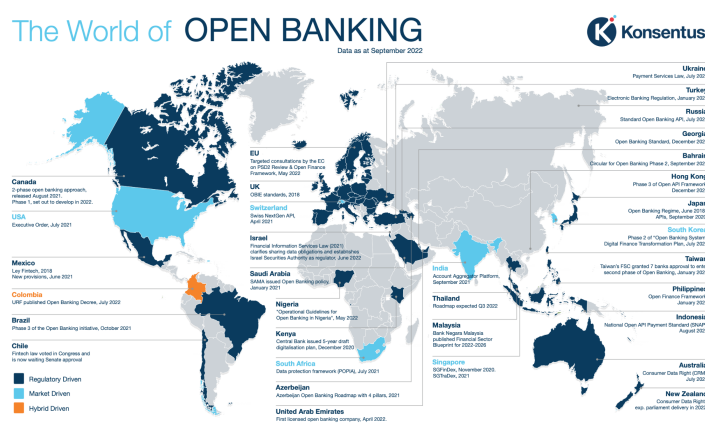
- Open Banking and Open Data efforts to date have mostly been “market led,” and domestic use cases are prioritized over cross-border use cases.
- There is no “global” governance authority, and additional resources are required to coordinate with other countries and regions.
- Local markets tend to have a bias towards ‘made here’ design, such as standards developed by local experts and services 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.
- Privacy and data policies continue to evolve and cascade across countries, making compliance an evolving target.
- It is hard to standardize functional API specifications and data models due to local differences even large global banks and digital platforms like HSBC, Standard Chartered, Santander, Citibank, PayPal, Google and Apple are likely to have challenges building platform services.
- Middleware providers like True Layer or Tink offer cross-border solutions for relying parties that need it, introducing substitution business risk.

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 and reap the benefits the DFFT seeks to realize. It’s a question of when and how.

²⁰ https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

New Open Data Ecosystems

First, we must acknowledge that there are still parts of the world that don't have live Open Data and Open Banking started much less on an implementation path or well adopted. This chart from Konsentus from September 2022 shows in gray the large number of markets that had not started implementing open banking a year ago, and the dark blue shows those markets with regulatory driven approaches versus market driven approaches in light blue.²¹ Strong progress has been made in the past 10 years, but we must note that the distribution of deployment and expertise is mixed. However, this global movement still offers a running start to achieve some of the goals of the DFFT whitepaper.



It's worth noting that momentum continues in 2022, a few examples below:

- The Saudi Arabian Monetary Authority (SAMA) is moving at pace to enable Open Banking in Q1 2023, an effort that is of considerable interest to other authorities in the Middle Eastern Region.
- Canada's Ministry of Finance is about halfway through their Open Banking due process, a deep dive consultation, policy and development process between the public and private sector expected to conclude in 2023.²²
- The US CFPB Director Chopra announced October 2022 its intent to develop rules that will enable competition to benefit consumers and new entrants, with comment period open now, and a timeline for rules by the end of November 2023 ahead of implementation in 2024.²³
- New Zealand's government has announced in November 2022 its plans to introduce a Consumer Data Right regime, starting with banking and expanding to other verticals following the Australian model.²⁴

²¹ <https://www.konsentus.com/wp-content/uploads/The-World-of-Open-Banking-Sep-2022-1.pdf>

²² <https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation.html>

²³ <https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/>

²⁴ <https://www.beehive.govt.nz/release/govt-moves-introduce-open-banking-give-customers-better-deal>

- The Nigerian government and local Open Banking Nigeria continue to make steps towards Open Banking in the country.
- The South African government continues its diligence on a cross-agency policy for Open Banking.
- The Colombian government announced its plans to enable Open Banking, and other countries in Latin America are expected to follow in the footsteps of Brazil and Mexico as 2023 progresses.
- Asian markets are very active in Open Banking and Open Data, led by Singapore, India, Australia, and Japan with activity in many more markets underway. Like Latin America, more news of implementations and regulations are expected throughout 2023.

While many countries and regions are only starting their Open Banking and Open Data journey, they are in a great position to benefit from all the latest standardization efforts, global learnings, and mistakes. We may see some markets that are particularly agile moving from policy to scale implementations in as little as 18 months. As long as each market does not try to “reinvent the wheel,” their consumers, fintechs and data providers will be able to reduce the time and cost required to go live.

Monetization of Open Data?

In the first phase of Open Banking and Open Data, the impression was that some Data Providers like banks were exceptionally unwilling to enable the new regulation. However, some Open Data providers took a different view, exploring how they can leverage their brand and customer base to create new innovative offerings. For example, in Brazil we observe banks acting as both data providers and relying parties from the start of the ecosystem launch. This model is particularly useful for consumers in Brazil that typically have current accounts and credit cards with multiple banks.

As Accenture points out in “Power plays for monetizing Open Banking APIs” report²⁵ innovative banking institutions will choose between Banking-as-a-Platform and Banking-as-a-Service models.

In the **Banking-as-a-Platform** model, banks will complement their offering in their channels with additional services from third parties. There are plenty of existing examples using this model worldwide²⁶:

- DBS partnering with Expedia and Singapore Airlines to improve travel booking experience²⁷.
- Monzo partnering with flux to enhance transaction experience by adding receipts and loyalty functionality to its online banking²⁸.

In the **Banking-as-a-Service** model, banks will provide banking services via third parties’ channels. Some of the examples of BaaS are:

²⁵ <https://www.accenture.com/au-en/insights/banking/monetizing-open-banking-apis>

²⁶ <https://bankingblog.accenture.com/how-to-guide-for-monetizing-open-banking>

²⁷ <https://www.techinasia.com/dbs-singapore-airlines-expedia-chubb-insurance-launch-travel-marketplace>

²⁸ <https://techcrunch.com/2019/01/28/monzo-teams-up-with-flux-to-add-itemised-receipts-and-loyalty-points/>

- Mexican Uber app providing financial products (bank account and bank card) for its drivers within their app by partnering with BBVA²⁹.
- Cash App by Square provides some financial services by partnering with Sutton Bank and Lincoln Savings Bank³⁰.

Both models will deliver additional value and monetization opportunities for these providers. Whichever model is chosen, the bank needs a mature API infrastructure to implement it.

We also will have to observe the degree to which “data for money” models persist in the next wave of regulatory reviews. The regulation-led models evaluated for this paper do not have payment mechanisms where relying parties pay compensation to Data Providers for access to data, however some proprietary models have mechanisms to allow for compensation. Will compensation models persist, or will regulation limit the ability for these models to persist? What about when transactions move across borders? Like the Accenture models, will Data Providers have to rely on adjacent strategies for top line growth to offset (or exceed) compliance costs?

Monetization strategies by market participants are not a core focus of this paper, but regulators will need to reflect on the motivations of market participants and ensure any rules incentivize the desired outcomes and mitigate externalities.

²⁹ <https://tipalti.com/banking-as-a-service/>

³⁰ <https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/blog/offering-20210727-blog-baas.pdf>

Is Open Data Crossing Borders Next?

The transition from proprietary API services to Open Banking, from Open Banking to Open Finance, and from Open Finance to Open Data happened rapidly over the past 10 years and continue at pace now. Yet it was not long ago that the challenges for enabling Open Banking seemed daunting to the first movers. The challenges of enabling Open Banking and Open Data seem similarly daunting now. Can all the challenges be overcome to enable global interoperability?

The first question is, what are the use cases that could drive the adoption of Global Open Banking, Open Finance and Open Data? What if a UK-based fintech could help a customer with bank accounts in multiple jurisdictions with Personalized Financial Management, competing on par with a global bank, global investment firm or global accountancy firm? Or a car rental company in Norway can verify customer identity in Australia and accept payments directly from an Australian bank?

Equally pressing, which entities have 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 transactions a reality for people and businesses.

Global Relying Parties & Use Cases

Digital Platforms & Fintechs

The rise of the internet, mobile phones and apps, and cloud-based 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 across borders. 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 government regulators to keep Digital Platforms out of Open Banking markets.³¹

Apple

In March 2022, Apple acquired UK Open Banking startup Credit Kudos, and it was the first public foray by Apple into a business with an inherent Open Banking dependency. A few months later at WWDC in June 2022, Apple announced a new service in partnership with MasterCard to allow users to initiate installment payments in 4 installments over a few months for no interest, without the Apple Pay merchant making any changes.³² In theory, the Credit Kudos acquisition helps Apple offer installments to consumers typically declined by credit agencies. While Apple’s global market deployment plans for this Buy Now Pay Later model is not clear yet, it is another step on Apple’s roadmap to offer progressively more financial services. Since 2014, notable additions to Apple’s financial service offerings include Apple Pay, Apple Cash, Apple Card, Apple Tap to Pay, Apple ID in Wallet, and now, Buy Now Pay Later and installments.

An area to watch out for, is that Credit Kudos is also a UK Financial Conduct Authority authorized entity and credit bureau, and an active participant in the UK Open Banking scheme with access to banking data from all large UK banking institutions which helps underpin its predictive scoring. This is the first example of how Apple is (potentially) leveraging Open Banking information to underpin a competitive new offering (installments or Buy Now Pay Later). Apple may not be obliged to conform to Open Banking and Open Data regulation in markets for some time, however, they are already on the front foot acting as a relying party to realize new products and services.

There are many who conjecture on Apple’s potential future financial services roadmap, with one such article by the Financial Brand in August 2022, exploring various paths Apple might choose to take.³³ To realize new features like financial planning, Apple may turn again to Open Banking and Open Data to realize their strategy, and offer consumers visibility outside Apple controlled products and services. Their acquisition of Credit Kudos also demonstrates that even overt regulatory blocks of Apple and other tech firms may not be an impediment if their market scale offers them the option to “buy” their way into access to Open Banking and Open Data information. Of course, as and when payment service providers are obliged to conform to regulation as Data Providers, Apple (or its enabling bank partners like Goldman Sachs and Green Dot Bank) will also have to comply.

³¹ Open Banking and the Constant Threat of BigTech,” Jan 13, 2022, PAYMNTS.com. <https://www.pymnts.com/digital-first-banking/2022/open-banking-the-constant-threat-big-tech/>

³² <https://developer.apple.com/apple-pay/whats-new/>

³³ <https://thefinancialbrand.com/news/fintech-banking/understanding-the-retail-bank-that-apple-has-quietly-built-150546/>

Block

Block, formerly known as Square, has two notable 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.³⁴ The second is Cash App, a highly successful service developed by Block that allows its customers to make peer-to-peer money transfers in multiple jurisdictions. Currently, this service is available in the United States and the United Kingdom, and it has grown from 3m to 44m+ plus users in ~5 years.³⁵ With global offerings like these, Block is likely to be active in Open Banking and Open Data initiatives in multiple markets.

Furthermore, as of March 1, 2021 Block began operating as a bank, so it will be obliged to conform to any US rules on Open Banking applicable to all US banking entities, however it is not (yet) known to be active in the Financial Data Exchange.³⁶

Similar to Apple, Block may become more active on the relying party side of the Open Banking and Open Data ecosystems, ahead of any obligations to conform to regulations as a bank or payment service provider.

Google

In November 2021 Google ceased its efforts to offer checking accounts to its customers, a service called Plex developed in partnership with Citibank and several other financial service partners.³⁷ This change of approach likely limits the “Data Providers” obligations might have in many markets in which it is currently operating.

Similar to Apple and Block, we may well see Google more active on the relying party side of the Open Banking and Open Data ecosystems, ahead of any obligations to conform to regulations as a Data Providers.

PayPal

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 will be obliged to enable Open Banking to conform to regulation as payment service providers are included in the scope. To support local law PayPal is likely to need to support a variety of API and security standards in each country, which implies entities like PayPal and other cross-border service providers and banks are likely to favor global standards. The more consistent implementations are between markets, the less complexity to maintain and operate services across markets.

³⁴ <https://en.wikipedia.org/wiki/Afterpay>

³⁵ <https://www.businessofapps.com/data/cash-app-statistics/>

³⁶ <https://investors.block.xyz/news/news-details/2021/Square-Financial-Services-Begins-Banking-Operations/default.aspx>

³⁷ <https://www.wsj.com/articles/google-is-scrapping-its-plan-to-offer-bank-accounts-to-users-11633104001>

Cross-border Payments Sector

Given one of the first use cases enabled by Open Banking is payment initiation, one of the first use cases of interest for cross-border transactions is... cross-border payment initiation.

Of course, today the cross-border payment market is crowded and complex, so it is unclear if and when Open Banking enabled cross-border payments would gain material traction. Market participants serving this use case today include Digital platforms, traditional banks, money service companies (e.g. Western Union, Money Gram), and Fintechs (e.g. Wise). Even with all this competition, mechanisms to enable cross-border payments tend to be high cost and can take days to settle. The marketplace is even more complex when you consider not just consumer payments, but corporate payments as well.

SWIFT is the dominant mechanism for global cross-border payments and SWIFT gpi (Global Payment Initiative) is a new standard for handling cross-border payments that was created as a result of collaboration between SWIFT and the global banking community.³⁸ SWIFT gpi has 4000+ participating financial institutions, \$300B in payments a day in 150+ currencies. This has substantially reduced time to send and receive, “nearly 50% of gpi payments are credited to end beneficiaries within 30 minutes, 40% in under 5 minutes, and almost 100% of gpi payments are credited within 24 hours.”³⁹ However, the time savings are not equally distributed as noted by the Bank of International Settlements in their report of data in 2020, which indicated that mature markets and routes could be in minutes or even seconds, while lower and medium income markets and some trade routes could still take days to settle.⁴⁰ In this context, Open Banking and Open Data implementations could enable faster transaction settlement on some payment “routes” albeit dependent on Open Banking being live on each “route.” It would take time to replicate SWIFT coverage, but once in place, the Open Banking and Open Data “rails” could expedite payments and SWIFT functional specifications can be used on Open Banking “rails” like the FAPI security profile. It is worth noting that SWIFT is already active in some areas of Open Banking and Open Data, such as the Preauthorization API published in 2019 which facilitates Buy Now Pay Later services.⁴¹

FXC Intelligence has published The Top 100 Cross-Border Payment Companies report in 2020, 2021 and in 2022.⁴² According to this report, the cross-border payments sector continues to grow at pace, 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.

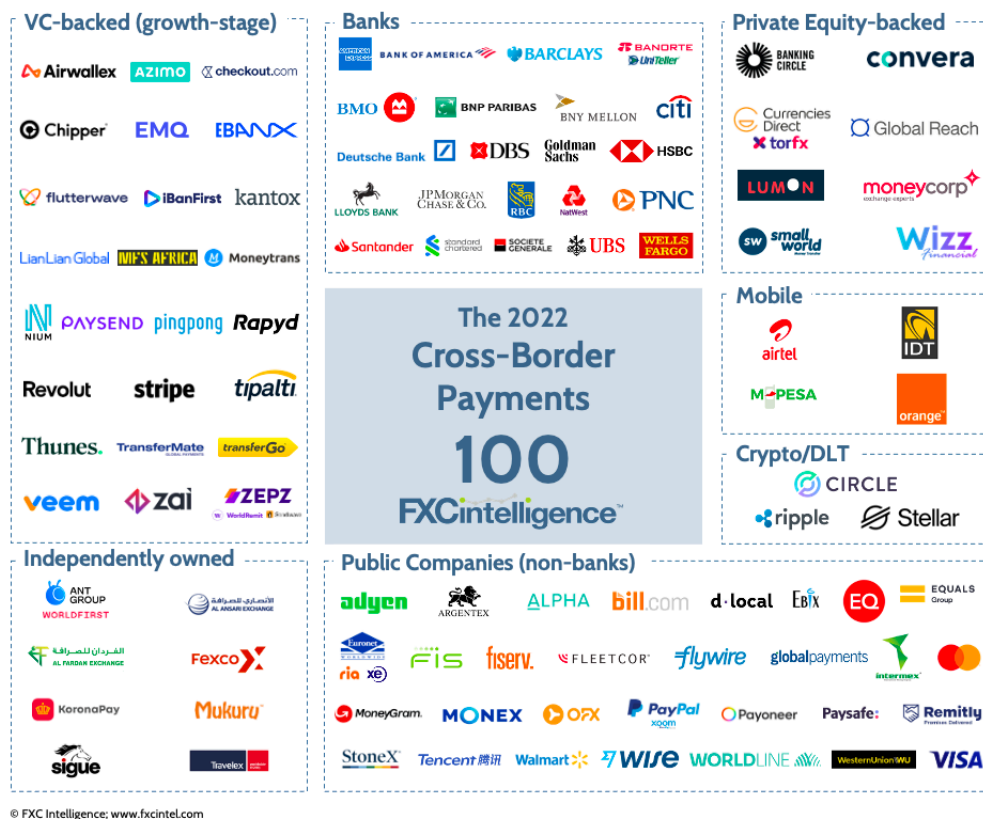
³⁸ <https://www.swift.com/our-solutions/swift-gpi>

³⁹ <https://www.swift.com/our-solutions/swift-gpi/about-swift-gpi/fast-transparent-and-trackable-payments#:~:text=Swift%20gpi%20lets%20you%20make,are%20credited%20within%2024%20hours>

⁴⁰ https://www.bis.org/cpmi/publ/swift_gpi.pdf

⁴¹ <https://www.swift.com/news-events/press-releases/swift-leads-industry-open-banking-library-api-standards>

⁴² <https://www.fxcintel.com/research/reports/the-top-100-cross-border-payment-companies>



Beyond private markets' appetite to deliver compelling cross-border payment services, we also see governments setting 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 how their data is used to provide the services they want and need."⁴³ Their investments show their commitment to this strategy:

- In February 2019, Mastercard announced its partnership with Token, an open banking platform provider that operates in 13 countries in Europe⁴⁴.
- In June 2020, Mastercard has made a significant investment by purchasing Fincity for US\$825m⁴⁵, a service operating primarily in North America.
- In September 2021, MasterCard acquired the European open banking platform AiiA.

⁴³ <https://investor.mastercard.com/investor-news/investor-news-details/2021/Mastercard-Expands-Open-Banking-Reach-with-Acquisition-of-AiiA/>

⁴⁴ <https://token.io/press/mastercard-selects-token-io-as-a-partner-for-its-new-open-banking-hub-1>

⁴⁵ <https://investor.mastercard.com/investor-news/investor-news-details/2020/Mastercard-to-Acquire-Fincity-to-Advance-Open-Banking-Strategy>

MasterCard is also a member of the US based Financial Data Exchange, an industry led effort to enable open banking in the US market.

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”⁴⁶. In November 2021, Visa invested in Australian open banking platform Basiq, expanding their global coverage.⁴⁷ Visa is also a member of the Financial Data Exchange, a US based industry organization working to enable Open Banking in the US market.

Payment Network Summary

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.

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), however they signal the payment schemes desire to acquire businesses that would simplify integrations per region and speed their time to market.

It is reasonable to believe that these global payment networks also seek to benefit from economies of scale, and as scale relying parties, they will prefer governments that select global open standards that simplify their ability to launch competitive new product and service offerings.

The Sharing Economy

The sharing economy is dominated by global companies such as Uber, Airbnb, Didi Chuxin (China), Lime, Zipcar, TaskRabbit. Use cases may vary, but the common theme is the need to ensure trust between the end payer and the end provider of the service or lender of the asset.

For example, to improve rider safety, drivers need to perform identity verification. Providers like Uber and Lyft need to connect to different identity schemes in each market in which they operate, and ensure consistent payment is available from end consumer to the end service provider.

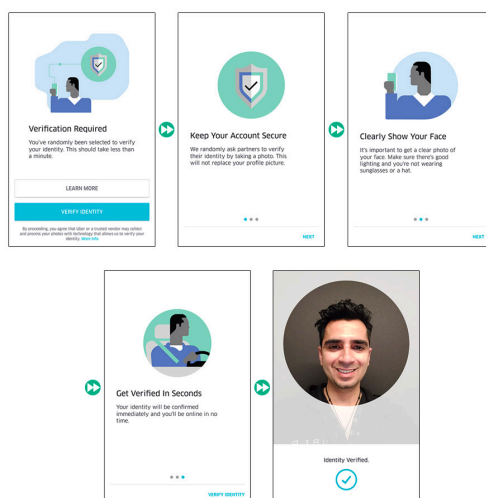
These companies often have to access identity and financial services differently in each country (if such services are available at all), and Uber alone operates in 72 countries. Sharing economy providers will significantly benefit if this access could be standardized, lowering their development and maintenance costs, reduce their transaction costs, and most importantly, ensure their networks are trusted and payments flow as expected in their networks.

Even modest cost savings or easier market entry can translate to meaningful margin improvements and growth, and the scale keeps growing. The Sharing Economy Market

⁴⁶ <https://www.businesswire.com/news/home/20210623006027/en/Visa-To-Acquire-European-Open-Banking-Platform-Tink>

⁴⁷ <https://www.pymnts.com/news/investment-tracker/2021/visa-invests-in-open-banking-platform-basiq/>

Research Report estimates the market size in 2021 at \$113B on track to grow 32% to \$600B by 2027.⁴⁸



49

Social Networks & Content Providers

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 anonymized, harmful activity and to provide traceability if an offense occurs (e.g. scams, cyberbullying).⁵⁰ Proper identity verification could reduce occurrences of fake users, fake news and false influencers.

Twitter reported in 2022 that fewer than 5% of accounts are fakes or scammers, commonly referred to as “bots”⁵¹, but even a small number of fake accounts can be harmful to an online community. Most recently, Twitter’s acquisition by Elon Musk and the deployment of a new strategy to charge \$8/month for the “blue checkmark” for verified accounts has made almost daily headlines, as the company moves through a tumultuous period.⁵² This is the first time we are seeing such a clear “identity verification for a fee” model on social media, and the months ahead will be key to observe user willingness to pay for identity and along with other premium services.

⁴⁸ <https://www.digitaljournal.com/pr/sharing-economy-market-size-with-emerging-growth-top-key-players-production-capacity-estimates-revenue-competitive-environment-and-swot-analysis#:~:text=The%20global%20Sharing%20Economy%20market,USD%20600000.0%20million%20by%202027>

⁴⁹ <https://timeattackmanila.com/news/generalnews/ubers-new-safety-feature-now-require-drivers-take-selfies/>

⁵⁰ <https://petition.parliament.uk/petitions/575833>

⁵¹ <https://theconversation.com/how-many-bots-are-on-twitter-the-question-is-difficult-to-answer-and-misses-the-point-183425>

⁵² <https://variety.com/2022/digital/news/twitter-blue-relaunch-blue-check-mark-imposters-1235456618/>



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 these platforms increasingly employ AI algorithms to determine the age of its users, given the lack of other authoritative digital identities for youth. TikTok is also planning to test ways to age-restrict some types of content in its app, a process that is not possible without identifying the users and/or their guardians.⁵³

Content providers like YouTube (Google) are also obliged to comply with regulation on age and other content restrictions YouTube. Two examples of emerging legislation influencing the social media and content landscape are from the EU:

- **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.

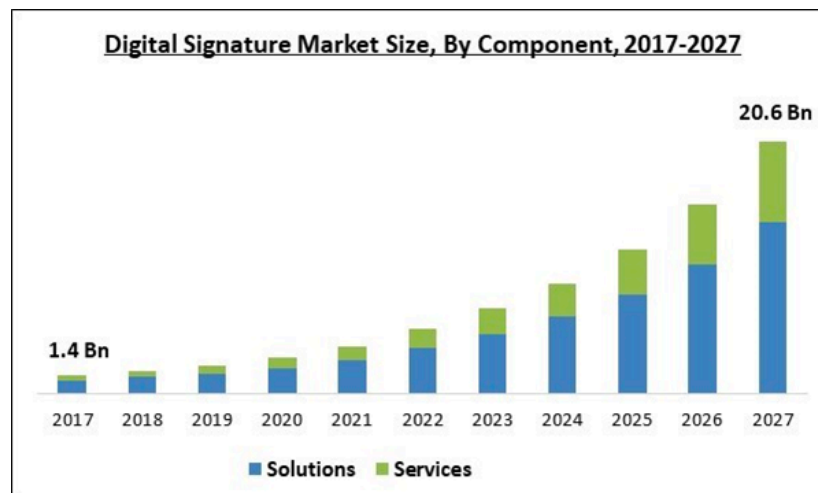
Similarly, in Japan online dating services have to rely on mobile network operators' (MNO) verification services in the absence of other widely accepted options. MNOs themselves are required to perform KYC checks for all subscriptions. Gambling is another regulated sector where online age verification is important to business operations.

Many social media businesses rely on consumer payments and or advertising, so they have a need to be able to accept and route payments across borders to fund their business. If mechanisms like Open Banking could lower their costs and improve the speed of payments they are likely to find favor with these global service providers. The challenge for these businesses is how to access global, consistent and interoperable identity and payment services that meet their requirements.

⁵³ <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, the 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 signing and its authentication requirements in Europe, but, unfortunately, it only works in Europe⁵⁴.

Digital signing is one of the first use cases pursued by the GAIN community.⁵⁵ The 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 first, but all the other identity use cases described within the paper can be served by GAIN.

Government Strategy

The Government objectives that seeded the Open Banking and Open Data regulations and global movement started with a desire to stimulate competition and innovation while ensuring user privacy (user-consent based data sharing), security and interoperability. The same motivations driving 20+ markets to expand or initiate Open Banking and Open Data implementations, sometimes with government-led approaches and sometimes with private sector-led approaches.

As the first phase of deployments reach fruition, and Governments refresh their strategies, we see more and more markets expanding their scope from Open Banking use cases to embrace a wide set of financial services, utilities, telecommunications, health, identity and

⁵⁴ <https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+-+Get+started>

⁵⁵ <https://gainforum.org/GAINWhitePaper.pdf>

other use cases. Below are a handful examples of the intergovernmental conversations underway now.

OECD / G20

The OECD has also been active in analyzing Data Portability such as their 2021 discussions on data portability encompassing, movement of user information, removing barriers to login, and facilitating competition, “Data Portability, Interoperability, and Digital Platform Competition.”⁵⁶ This work continues to be a key area of focus for the OECD with formal discussions and evaluations of current Open Banking and Open Data deployments during 2022.

In parallel, in October 2021, the G20 made cross-border payments a key priority, and developed a framework program to realize the potential.⁵⁷ The Financial Stability Board (FSB), which reports to the G20, together with the Committee on Payments and Market Infrastructures (which reports to the Bank of International Settlements, overseen by Central Bank Governors) jointly developed a roadmap to address cost, speed, transparency and access to cross-border payments by consumers and businesses. Open Banking and Open Data can help deliver on 6 of the 19 building blocks defined in the G20 Roadmap for Cross-Border Payments, as per the analysis in Annex D.

World Economic Forum

In 2019, World Economic Forum and Japan’s Prime Minister Shinzo Abe invited leaders to build an international order for “Data Free Flow with Trust (DFFT),” as noted in the Introduction to this paper. In 2020, Osaka Track was created to design global governance processes needed to realize the DFFT vision and unleash the benefits from cross-border data flows.⁵⁸ The subsequent report also produced several recommendations, and this whitepaper is one response to how to realize some of the objectives outlined in the DFFT.

Digital Government Exchange

In 2021, Digital 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 Interoperability Principles to enable mutual recognition and interoperability between domestic digital identity schemes.⁵⁹ These principles are in turn derived from the European Digital Identity Interoperability Framework.⁶⁰ Similar principles could serve to inform the governance of globally interoperable Open banking and Open Data ecosystems, and even help the global community determine what existing (or new?) entity is best placed to provide the governance capabilities required.

⁵⁶ <https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm>




⁵⁷ <https://www.fsb.org/2021/10/g20-roadmap-for-enhancing-cross-border-payments-first-consolidated-progress-report/>

⁵⁸ https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf

⁵⁹ https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

⁶⁰ European Union, 2017, ‘*New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*’, Publications Office of the European Union, Belgium.

Interoperability principles

- 1  Openness
- 2  Transparency
- 3  Reusability
- 4  User-centricity
- 5  Inclusion and accessibility
- 6  Multilingualism
- 7  Security and privacy
- 8  Technology neutrality and data portability
- 9  Administrative simplicity
- 10  Preservation of information
- 11  Effectiveness and efficiency

Open Health

Covid-19 laid bare the identity infrastructure gaps in most jurisdictions, gaps which complicated public health efforts such as testing operations, vaccine distribution, and privacy preserving data sharing. The multi-country paper above on Digital Identity in Response to Covid-19 is a striking summary of the potential for interoperable solutions to make a substantial contribution to public health in times of crisis. Beyond crises, people also need better health data interoperability, and governments are advocating for policies to realize user-consent based data sharing, or “Open Health.” People want more control over the ability to provide consent to move health records between providers, designate caregivers and authorize third parties to have access to medical information in tightly controlled use cases (e.g. de-anonymized use of brain scans for academic purposes and much more). In the EU, the government plans to leverage the European Digital Wallet infrastructure to support purchase of medicines and interoperability of health data and services, while in the US, Trusted Exchange Framework and Common Agreement (TEFCA) from the US Department of Health and Human Services seeks to offer a “universal floor for interoperability across the country,” with the Sequoia Project selected to operate the project.⁶¹ Other key standards bodies and intergovernmental organizations involved in enabling Open Health include HL7, IHE, and the WHO. A recent whitepaper by the OpenID Foundation published “The Global Open Health Movement: Empowering People and Savings Lives by Unlocking Data”⁶², reviews the current identity and health standards landscape, including current policies and regulations and market participants, and then outline key recommendations to realize the potential of Open Health.

⁶¹ <https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca>

⁶² https://openid.net/wordpress-content/uploads/2022/07/OIDF-Whitepaper_The-Global-Open-Health-Movement_1st-Editors-Draft_2022-07-21.pdf

US Mobile Driving Licenses

The US is actively pursuing mobile driving licenses, primarily by enabling apps and Wallets with digital versions of residents' physical driving license or state/jurisdiction identification card. Arizona, Maryland, Colorado, Florida, Utah, Louisiana and Oklahoma are some of the first states to offer such digital IDs, and some of them have been approved for acceptance at Transportation Service Authority (TSA) checkpoints (to date, Arizona, Colorado, Utah, and Maryland) with many other US states in the pipeline. Most of these implementations use the ISO 18013-5 standard although some states in the US, Canada, Australia and the EU are exploring the fit of verifiable credentials, and the relative benefits, risks and mechanisms to enable interoperability between them. Although these credentials can primarily only be used in the physical world, work on standards to enable online acceptance (ISO 23220-4 and ISO 18013-7) are also underway, along with discussions at the W3C and in other forums on how government issued credentials can be asserted in online transactions. Such capabilities could be of value for a range of regulated transactions like Open Banking and Open Data to ensure the user providing consent or payment is who they say they are. Since these standards are designed to be global interoperable standards, they could also help with technical efforts to enable Open Banking and Open Data across borders (although governance and policy considerations are out of scope for ISO standards).

In summary, there is a strong push from governments across the globe to expand Open Banking to Open Data specifically, and there are adjacent policy efforts in health, identity and cross-border payments that Open Banking and Open Data infrastructure can help serve as well. The OpenID Foundation is working on a whitepaper on the Identity and Government landscape, and a deep dive whitepaper into the privacy implications of government issued digital identity credentials. Interested people can contact director@oidf.org to learn more about these whitepapers, targeted for publication in Q1-Q2 2023.

Solutions

Currently Available Solutions

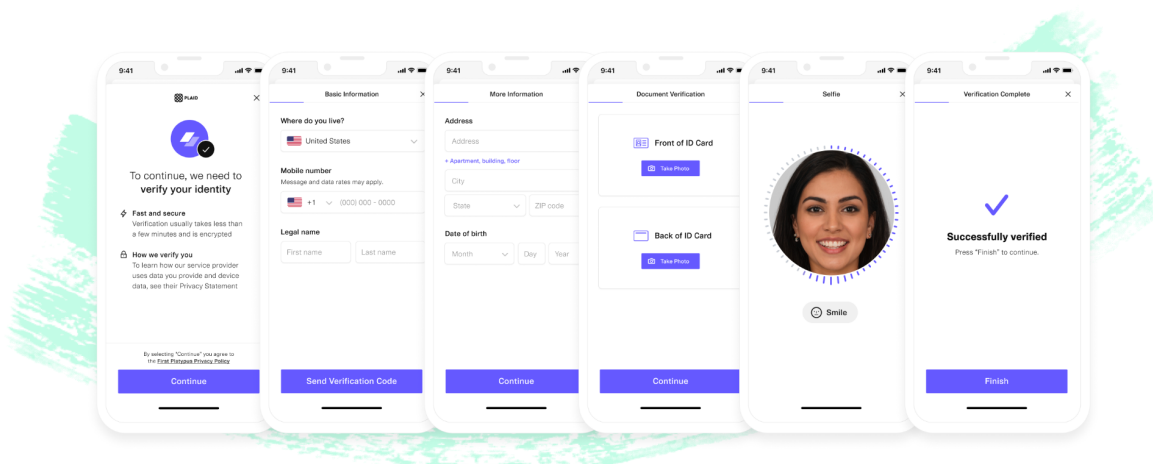
As mentioned in the Introduction, some of the first movers in the market for API-led open banking integrations were banks and Fintechs offering proprietary solutions, leveraging Open Banking implementations where they were available. All of these intermediary providers (and others) specialize in providing developer friendly, global APIs for:

- Identity verification
- Account information
- Payments

They usually seek to use open banking APIs where available, with fallback to screen scraping and direct integrations where required. Some of these providers are pure-play, connectivity providers, while some seek to offer “value-added” services as well.

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 the KYC space⁶³. By doing identity verification in-house, adding income verification and payments, Plaid can now provide end-to-end flow for their B2B customers. Plaid now operates in the US, Canada, the UK, France, Spain, Ireland, and the Netherlands.



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,⁶⁴ which sought to make it easy for developers to identify consumers. Recently, in May 2022, Stripe has announced further

⁶³ <https://plaid.com/blog/introducing-identity-verification/>

⁶⁴ <https://techcrunch.com/2021/06/14/stripe-goes-beyond-payments-with-stripe-identity-to-provide-ai-based-id-verification-for-transactions-and-more>

expansion into bank connectivity with Stripe Financial Connections.⁶⁵ Now their customers have fewer systems to connect to and manage, they can utilize the same platform for payments, subscriptions, payouts, identity and income verification.

As Open Banking and Open Data regulations and ecosystems mature, these intermediaries may face market risks such as the following:

- Disintermediation by new Open Banking and Open Data ecosystems
 - Proprietary APIs may become less relevant as markets roll out open standards; if the APIs are easy to implement to, more relying parties may “self-serve” and build to market APIs directly.
 - Commercial model disruption as relying parties may switch from high cost services from the intermediaries to free or low-cost services from the Open Banking or Open Data network.
 - If a global open standard and governance model emerges, this would add pressure to proprietary, multi-market approaches.
- Data Privacy
 - Models that assume the intermediary itself is processing and storing end-user data may contravene end user and regulator desire to limit data use by intermediaries.
- Other
 - Custom (non-standard) API and security profile specifications lead to switching costs as clients need to retool to switch between proprietary service providers.
 - Most providers rely on a network of subcontractors to add jurisdictions and new features, this can complicate data transparency and privacy issues.

If intermediaries cannot offer convenience or value-added services beyond what relying parties can access directly, their market position may be impacted. However, given the slow global rollout of Open Banking and Open Data, many of these providers probably have the ability to innovate their product and commercial models as may be needed.

⁶⁵ <https://stripe.com/newsroom/news/financial-connections>

Proposed Open Standards Based Cross-Border Solution

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 from different markets benefit end consumers. Technologists working on domestic implementations of open banking have led the thinking over the last year that has informed this analysis. In this chapter we will explore what good looks like and how a global model can be achieved.

Interoperability Principles

As noted above, the Digital Government Exchange defined a generic set of principles for cross-border identity ecosystems. We recommend applying the same principles for cross-border Open Banking & Open Data, as per the chart below⁶⁶:



Global Open Banking Standards

To deliver on the principles above, selecting standards is a fundamental activity to enable the interoperability at the key layers of the ecosystem architecture. One of the key recommendations is to re-use existing standards and not to invent new standards where possible. Technical standards applicable to Open Banking and Open Data can be grouped in two categories:

- **Trust management** (or the “control plane”) standards, focusing on how one participant of the interaction can trust another participant.
- **Data Exchange & Security standards** (or the “data plane”) or standards targeting how data is established once the trust has been established.

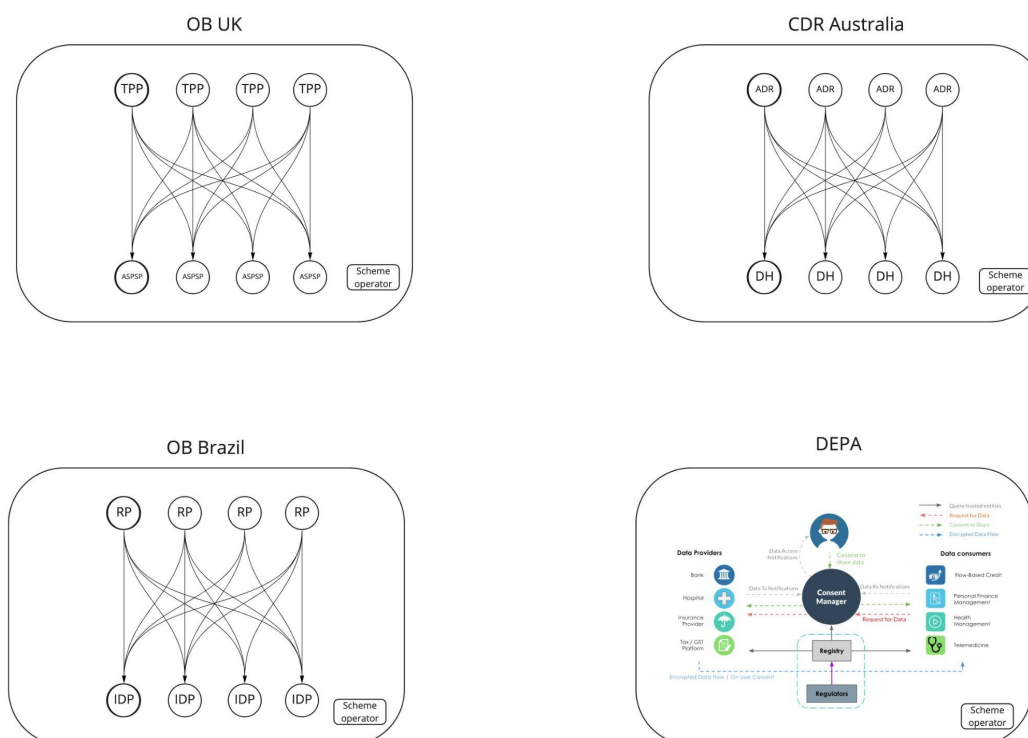
⁶⁶ https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

Trust Management (or Control Plane)

The GAIN Proof of Concept WG (hosted by the OpenID Foundation) and the Interoperability Working Group (hosted by the Open Identity Exchange) developed a model on how trust can be established between different participants.

Recommendation #1. “Networks of Networks”

Use a “networks of networks” approach and establish participant trust on a scheme to scheme level and perform data exchange directly between the participants. This is an illustration of how four networks like Open Banking UK, Consumer Data Right in Australia, Open Banking in Brazil and DEPA can remain intact operating their network as they do today, but each of those 4 entities then interoperate with the others.



This scheme-to-scheme approach (“networks of networks”) allows participants to:

- Preserve the autonomy of local networks, be it government led or private sector led, a form of “domestic sovereignty” over local network operating rules⁶⁷.
- Local market participant on-boarding, vetting and integration to a local scheme (scheme operator).
- Local market participant compliance with local regulation to a local scheme.
- Local network determination of the rules and mechanisms to enable interoperability between networks (a form of “interdependence sovereignty”⁶⁸).

Recommendation #2. Register Once

⁶⁷ Domestic sovereignty defined as “actual control over a state exercised by an authority organized within this state” <https://en.wikipedia.org/wiki/Sovereignty>

⁶⁸ Interdependence sovereignty defined as “actual control of movement across state’s borders” <https://en.wikipedia.org/wiki/Sovereignty>

Ideal outcome for relying parties would be if they can “register once and use it everywhere.” This minimizes complications, and it is a model we see in domain name registration, bank identifiers conducting cross-border payments (e.g. Legal Entity Identifier), and merchant identifiers participating in global payment networks (e.g. Visa, MasterCard).

Recommendation #3. Encapsulate "Local" in the Local Scheme

For example, delegate translation between networks to the local schemes and not the relying party. If the transaction between networks is done by a shared or entity service and it is masked in an SDK or another technical or proprietary solution then local participants lose transparency on the processes.

Recommendation #4. Minimize Central Infrastructure and Governance

Ideally there should be no central point of failure or control, no central decision making on what's allowed and what's not, and no scheme can make decisions on behalf of the other scheme. This premise ensures local governments and local scheme operators have the control they expect, consistent and uncompromised “domestic sovereignty” and “interdependence sovereignty.”

In contrast, if there is a central point of control and failure, we could see distortions in the marketplace that impede the ecosystem's ability to deliver on its desired objectives. For instance, if a single private entity controlled the global Open Banking or Open Data marketplace their monopoly control could lead to excessive rent seeking, limited accountability, and poor innovation. If a single government controlled the ecosystem, it could impede the full global coverage and utility of the ecosystem to the global community, as well as excessive rent seeking, limited accountability and poor innovation. If a single nonprofit or intergovernmental institution controlled the ecosystem, similar results could ensue. Open standards and APIs can allow for some key rules to be integrated into the standards themselves, limiting the need for complex governance regimes, so technical innovation can help minimize the obligations on any operating and governance entity. However, continued discussion is required by ecosystem stakeholders to evaluate the bare minimum of operating capabilities required, and establish common rules all network participants can sign up to under an “even playing field.”

Recommendation #5. Build on the Existing Foundations of GAIN and others

Work on the Global Assured Identity Network to enable identity interoperability at a standards and trust framework level, work underway since September 2021 in the OpenID Foundation's GAIN Proof of Concept Community Group and the Open Identity Exchange's GAIN Interoperability Working Group, can be leveraged to enable Open Banking and Open Data across borders as well. The work is very similar and extensible, the primary variation is a shift from person-based data in GAIN to “account based” information for Open Banking and Open Data.

Concepts and recommendations similar to #1 to #5 are explored in a context of cross border payments in a report written by the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) in collaboration with BIS Innovation Hub, the International Monetary Fund (IMF) and the World Bank⁶⁹. The report introduces a concept of multilateral platform that is multi-jurisdictional by design, discusses operational considerations, risk, barriers and challenges, provides analysis of existing platforms and recommendations. It is recommended to watch how this work develops further and utilize its relevant building blocks where possible.

Data Exchange and Security Standards

⁶⁹ <https://www.imf.org/en/Publications/analytical-notes/Issues/2023/01/18/Exploring-Multilateral-Platforms-for-Cross-Border-Payments-528297>

In order to achieve global interoperability, it is important to select a set of standards for inter-scheme communication. This does not mean that each participating scheme is obliged to change the standards they use internally, it just means there needs to be a mechanism to “translate” between the schemes.

The Open Banking Global Interoperability Working Group (OB GI WG at the Open Identity Exchange) has done extensive analysis of different ecosystems and standards being used globally. These are the agreed recommendations:

Identity Protocol

Recommendation #6. Use OpenID Connect to carry identity information between the participants.

OpenID Connect (OIDC) is a common language already understood by many private and open API ecosystems.⁷⁰ This allows for minimal effort for participants to implement, essentially it is a minimally invasive structure that lowers the barriers to participation and time to deploy.

OpenID Connect for Identity Assurance is an extension of the OIDC base protocol that can be used for the transfer of additional identity and trust framework data and metadata. Work is also underway to allow for data minimization (e.g. sharing information like age over 18) without the need to share the birth date.

Security Profile

Recommendation #7. Protect APIs with the FAPI 2.0 Security Profile

This OAuth 2 based profile is used by the growing majority of the schemes; for example, the UK, Australia, New Zealand, US, Canada, Brazil and Saudi Arabia all use FAPI 1.0, and Norway already uses FAPI 2.0 with Australia and Saudi Arabia including FAPI 2.0 in their 2023 Roadmaps. FAPI 2.0 is recommended because it delivers a simplified security profile and additional building blocks for interoperability. Like FAPI 1.0, FAPI 2.0 Security Profile has just completed formal security analysis by the University of Stuttgart.⁷¹

Functional API Specifications & Data Model

Use a practical approach to achieve interoperability at the API level between different markets that could deliver simplified APIs (e.g. the equivalent of an “Esperanto” API specification, or common simple language). Anecdotal evidence suggests that, in any mandated (not optimized) Open Data ecosystem, the majority of Relying Parties (Data Recipients) use only a small percentage of available APIs available, and a small percentage of data available via these APIs.

The OB GI WG has reviewed the following Open Banking specifications, and the potential to deliver simplified APIs that can work across markets seems achievable. If these target, simple APIs are also open standards, then it could also accelerate the adoption of Open Banking and Open Data by new countries:

⁷⁰ https://openid.net/specs/openid-connect-core-1_0.html

⁷¹ <https://openid.net/2022/12/19/fapi-2-0-announcement/>

#	Open Banking / Open Data ecosystem	URL
1	OB UK	https://github.com/OpenBankingUK/read-write-api-specs
2	US	FDX specifications are available after the registration https://financialdataexchange.org/FDX/Membership/Participation-Options.aspx
3	Berlin group	https://www.berlin-group.org/nextgenpsd2-downloads OpenAPI / YAML file: psd2-api v1.3.11-2021-10-01v
4	Australia	https://consumerdatastandardsaustralia.github.io/standards/#get-accounts
5	Mojaloop	https://mojaloop.io/
6	OB Brazil	https://openfinancebrasil.atlassian.net/wiki/spaces/OF/pages/17372032/Informa+es+T+cnicas+-+Contas+-+v2.0.1
7	India / UPI	https://indiastack.org/data.html
8	Plaid	https://plaid.com/products/
9	Tink	https://tink.com/products/

Recommendation #8. Start with a “Minimum Viable Product” of APIs and Payments

Picking a small set of APIs to start with “read” functionality MVP plus payment initiation will streamline the time to market. The OB GI WG suggested the following initial list:

- Account list
- Account detail
- Transaction list
- Transaction detail
- Payment initiation
- Payee confirmation

Furthermore, it is suggested to use one of the existing protocols as a base for simplification and global adaptation. For example, for payment initiation, UK's Open Banking payment initiation, Brazil's Pix's⁷² or SWIFT API specification can be used as a starting point.

Recommendation #9. Start with an Individual Customer MVP

The recommendation is to start with the customer's basic identity information delivered via OpenID Connect, basic information which serves as the foundation of regulated and unregulated use cases, and information generally of value for users to assert and relying parties to be able to offer services over the internet.

Recommendation #10. Payment initiation should be payment scheme agnostic.

There is no objective in Open Banking and Open Data to re-invent existing payment rails.

Recommendation #11. APIs should be simplified and optimized for Relying Party use.

The objective is to enable key global use cases in developer friendly ways, not to expose all the data available.

Summary

Customer-consent based data sharing has moved through multiple phases from Private APIs, to Open Banking, to Open Finance, Open Data and Open Health. We have seen 20+ markets move into implementing these programs, building scale in domestic markets. There is a level of inevitability now that these domestic implementations will continue their steady march, bringing more user control over data, competition, and innovation along with it.

The next "mountain to climb" is bringing Open Banking and Open Data across borders. The first key question is what use cases and which stakeholders will drive the effort? There are a large range of global relying parties and use cases that can benefit from Open Banking and Open Data including large digital platforms (e.g. Buy Now Pay Later), Fintechs offering identity and payment services, Sharing Economy businesses that need identity and payment to deliver trust, Digital Signatures and Dating apps who seek confidence in an individual real identity, and Age restricted content providers who need to be able to distinguish minors from adults, and much more. Cross-border Open Banking can deliver on these use cases in three formative ways:

- Access to user-consent based Open Data can unlock compelling new features and value-added services and simplify compliance with the law (where applicable).
- Improved security posture and lower maintenance and switching costs when the architecture is underpinned by mature, global standards.
- Leverages existing infrastructure where appropriate (e.g. leverage existing OpenID connect, SWIFT messaging, network payment rails, Legal Entity Identifiers, etc.).

As usual, proprietary solutions are in the forefront already offering some global capabilities, seeking to serve the global demand for identity and payment services with simple APIs. Where viable, these services already consume Open Banking data, and some of these intermediaries have been at the forefront advocating with policymakers and regulators for an "even playing field."

⁷² <https://www.infomoney.com.br/minhas-financas/banco-central-abrira-protocolos-do-pix-para-paises-que-queiram-copiar-tecnologia-de-graca/>

However, enabling interoperability between domestic Open Banking and Open Data networks, offers a paradigm shift to unlock benefits at far greater scale. The benefits of Open Banking and Open Data to a domestic market can be amplified when multiplied across markets. Users can have more data control, lower costs, more innovation in cross-border transactions, businesses can expand across borders more easily, and policymakers can deliver on macro and global objectives. For example, our government analysis indicated progressive appetite from policymakers for faster and lower cost cross-border payments, better data privacy protections, digital identity, and secure and resilient global infrastructure. These policy ambitions can be met, at least in part, by globally interoperable Open Banking and Open Data infrastructure.

The good news is that leading technologists already see a viable path to enable Open Banking and Open Data across borders. Our thanks to the contributing organizations and individuals noted in Annex A for their efforts over the past year to visualize and distill these recommendations. If “past performance is indicative of future returns,” we can expect their recommendations will become reality in the months and years ahead. The principles and recommendations highlighted in this paper serve as a robust starting point for public and private stakeholder conversations in the months ahead.

Next Steps

There are four key ways to get involved in this effort to bring Open Banking and Open Data across borders:

1. **Help form the Open Data Community Group.** This group intends to take the principles, recommendations and diligence from this paper and form a Community Group to brief public and private sector thought leaders, respond to government and intergovernmental requests for comment, and evaluate the optimal governance entities and approach. As the governance model requires wider stakeholder participation, the OpenID Foundation is offering this group a “safe space” to initiate the analysis, although the group may complete their evaluation and migrate work to a permanent home. To join this interest group in crafting the Community Group goals, participation agreement, and roadmap please contact director@oidf.org.
2. **Contribute to the OpenID Foundation FAPI Working Group.** FAPI is a key standard recommended to underpin Open Banking and Open Data crossing borders. Any individual or entity can contribute to Working Groups without paying a membership fee, provided the contribution agreement is signed. More information at <https://openid.net/wg/fapi/>.
3. **Contribute to the Global Assured Identity Network Proof of Concept Community Group.** This Group is working on trust management and global identity scheme interoperability, global account scheme interoperability, and providing a safe space for interoperable testing of solutions between networks. Participants include public and private sector stakeholders. More information on the GAIN Proof of Concept Community Group at <https://openid.net/gainpoc>.
4. **Join the Open Identity Exchange.** OIX established an Interoperability Working Group working on scheme governance, and business level interoperability and liability. This Work is also underpinning the GAIN efforts, and is well placed to help inform the Open Banking and Open Data crossing borders efforts as well. Find out more: <https://openidentityexchange.org>.

Annex A: Acknowledgement

Project Leader: Dima Postnikov.

Contributors: Gail Hodges, Nat Sakimura, Daniel Goldscheider, Lukasz Jaromin, Kosuke Koiwai, Ralph Bragg, Craig Borysowich, Max Geerling, Torsten Lodderstedt, Takahiko Kawasaki, Dave Tonge, Rupesh Kumar, Sanjay Jain, Chris Michael and Mike Leszcz.

Open Banking Global Interoperability Working Group (OB GI WG): This is an informal group of technologists unaffiliated with any specific organization. Members of this group agreed to contribute the findings of their weekly working group discussions from January-December 2022 to this paper. Participants of the group included: Anil Mahalaha, Daniel Goldscheider, Don Thibeu, Max Geerling, Chris Michael, Steve Pannifer, Mark Haine, Daniel Campos, Fiona Hamilton, Leif Johansson, Stephen Wilson, Gail Hodges, Ralph Bragg, Miguel Diaz, Michael Richards, Paul Makin, Nat Sakimura, Carl Hössner, Sanjay Jain, Dima Postnikov.

GAIN Proof of Concept Community Group, hosted by the OpenID Foundation (<https://openid.net/gainpoc>).

OpenID Foundation FAPI Working Group (<https://openid.net/wg/fapi/>).

Open ID Foundation eKYC & IDA Working Group (<https://openid.net/wg/ekyc-ida/>).

Open Identity Exchange GAIN Interoperability Working Group (<https://openidentityexchange.org>).

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 FAPI security profile and the Open ID Connect for Identity Assurance were selected by leading technologists to form the backbone of an interoperable global "networks of networks."

The OpenID Foundation does not think any single 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. The Foundation also offers itself as a "safe space" for the community to convene, to test and to develop tests that enable interoperability.

Membership in the foundation is not required to contribute to working groups or community groups. Contributors only need to sign up to the Contribution Agreement or Participation 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 $\frac{1}{3}$ by membership, $\frac{1}{3}$ by certification fees, and $\frac{1}{3}$ 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 <https://openid.net> or contact director@oidf.org.

Annex C: Standards Bodies and Non-Profits

Many domestic, regional and global standards bodies are making meaningful contributions to Open Banking, Open Data and cross-border payments.

Below are a few of the standards bodies active in the global discourse on Open Banking and Open Data across borders, outside of the OpenID Foundation and Open Identity Exchange referenced in Annex A & B:

Berlin Group (Germany, Europe)

The Berlin Group pursued standards to support regional 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 Open Banking)

The Brazilian central bank has taken a government-led, regulatory approach and went live in 2021, with a mandate for most Data Providers (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 Providers and relying parties. Open Insurance (OPIN) is in the process of being launched in the first quarter of 2023, led by the Brazilian Private Insurance Authority (SUSEP), it is designed using the same standards as the Brazilian Open Banking, so that it can add more data and services to the Brazilian Open Finance ecosystem.

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 (utilities), telecommunications and financial services such as insurance and investment providers. Australia has been active in the global arena, contributing to global standards development and co-funding the formal security analysis of the FAPI 2.0 security profile. The Australian approach has inspired a similar approach in New Zealand, which is currently working through their own Consumer Data Right legislation development and implementation.

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.”*⁷³ There are currently over 200 participants, both data providers and data consumers. As noted in the paper, the US Regulator Consumer Finance Protection Board has indicated its intent to set rules in late 2023 with feedback requested in Q4 2022 to Q1 2023, implementation in 2024 that will impact Open Banking.

Financial Stability Board (G20)

This G20 entity is working on common building blocks for cross-border payment initiation, and is active in Open Banking conversations.

⁷³ <https://financialdataexchange.org/FDX/About/FDX/About/About-FDX.aspx>

Open Banking Implementation Entity (UK)

In 2016 the Competition & Monetary Authority (CMA) published a report on the UK's retail banking market that 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 can share their current account information with third party entities who use that data to tailor apps and services.⁷⁴ 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 and it is governed by the Joint Regulatory Oversight Committee.^{75 76}

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 2022,⁷⁷ 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 and Open Data domain are:

- Emerging Payments Asia
- FDATA
- iSPIRT
- International Institute of Finance

⁷⁴ <https://www.openbanking.org.uk/about-us/>

⁷⁵ <https://www.openbanking.org.uk/news/open-banking-and-obie-highlights-may-2022>

⁷⁶ <https://www.openbanking.org.uk/news/what-the-future-holds-for-open-banking/>

⁷⁷ <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: Analysis of the G20 Roadmap for Enhancing Cross-Border Payments

Open Banking and Open Data moving across borders will address 6 of the 19 building blocks in this joint report from 13 October, 2021. A summary of the building blocks is found in the diagram below:



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

Our analysis of this report indicates there are 6 Blocks where Open Banking and Open Data can make meaningful contributions to improved cross-border payment “rails”:

- **Block 5: Applying Anti Money Laundering/CFT rules consistently and comprehensively.**
 - This can be facilitated with protocols like OpenID Connect for IDA that include reference to the policy that was followed in the originating jurisdiction so the relying party can simplify their own policy assessment.
- **Block 8: Fostering Know Your Customer and identity sharing.** Consistently identifying customer 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
 - 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 (like the working group members that contributed to this paper) 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-standardized data formats create additional complexity, unnecessary transformation, delays and potentially manual processing. This also adds risk of misinterpretation and data loss, and 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*⁷⁸.
 - The BIS Innovation Hub, SWIFT ran ISO 20022 hackathon in March 2021 to highlight the potential of cross-border payments standardization. At this event, 60 teams from payments and technology market participants demonstrated high interest and high potential of using common message standards and standardized API specifications⁷⁹. Mojaloop built one of the winning entries with ISO20022 format payments via SWIFT routing to Mojaloop for last mile delivery (via an adapter).
- **Block 16: Establishing unique identifiers with proxy registries.**
 - The Financial Stability Board 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 was founded by the G20 after the Financial Crisis of 2007-8 to define a common approach to financial service legal entities, to help with transparency of linkages between entities, beneficial owners of those entities, and the people making and receiving payments.
 - 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.

⁷⁸ <https://www.fsb.org/wp-content/uploads/P131021-1.pdf>

⁷⁹ <https://www.bis.org/press/p210325.htm>

Annex E: 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>>
11. Accenture: Power plays for monetizing Open Banking APIs (2020),
<<https://www.accenture.com/au-en/insights/banking/monetizing-open-banking-apis>>