The Smart Path to Open Finance.

How a Smart Data Right can deliver Open Finance and change our economy.

September 2021

COADEC

Authors

Charlie Mercer
Head of Economic Policy
The Coalition for a Digital Economy (Coadec)

Dom Hallas
Executive Director
The Coalition for a Digital Economy (Coadec)

About Coadec

The Coalition for a Digital Economy (Coadec) is an independent advocacy group that serves as the policy voice for Britain's technology-led startups and scaleups.

Coadec was founded in 2010 by Mike Butcher, Editor-at-Large of technology news publisher TechCrunch, and Jeff Lynn, Executive Chairman and Co-Founder of online investment platform Seedrs.

Coadec works across a broad range of policy areas that matter the most to startups and scaleups: Access to Talent, Access to Finance & Technology Regulation. We represent the startup community on the Government's Digital Economy Council, and the UK on the international organisation Allied for Startups Board.

Coadec has been at the forefront of the UK's Fintech policy conversations. We published our 'Blueprint for Open Finance' in November 2020 with the Chairs of the APPG for Fintech and APPG for Open Banking and, following this, the FCA has taken onboard a number of our key recommendations in their consultation on Secure Customer Authentication.

WHY WE'RE HERE...

Open banking is taking the financial world by storm. Since going live in the UK in 2018, it has taken off as a global phenomenon poised to disrupt financial services providers that have failed customers for years. The stage should be set for a post-Brexit UK to continue as the flagship in the open banking armada.

Alas, our pole position is in jeopardy, with ecosystems in Europe, Australia and Mexico, to name a few, set to overtake the UK in 2021. These threats to the UK's leadership in open banking are captured in the first section of this report.

In the Autumn of last year, Coadec published a report titled "Breaking Banks: A blueprint for open finance that puts customers first". In this report we outlined five recommendations to iron out some of the issues with the open banking ecosystem in the UK. These were:

1. Put customers first by creating a **new data sharing right** and removing the **90-day reauthentication rule**.
2. Complete the payments landscape by **publishing the findings of the VRP test** and by putting in place a clear set of **Service Level Agreements** around ASPSP **API performance**.
3. Maximise opportunity through **technologically-neutral, principles based smart regulation** to govern the move towards open finance.
4. Create a **better governance architecture** that incorporates better collaboration between the FCA, Digital Identity Unit and ICO.
5. Construct a **coherent governance structure**, that includes the proposed Smart Data Council to look towards opening up other industries and begin work on Premium APIs.

Consultations over the last year have set in motion *some* of these recommendations, but overall the picture is less promising and ecosystem innovation remains stunted. In the second section of this report we will discuss what remains to be mopped up for open banking in the UK.

Much of the discussion among the open banking cognoscenti today revolves around the future of the Open Banking Implementation Entity (OBIE). This is important because the Entity has been a central part of the UK's open banking ecosystem having been explicitly charged with enforcing the CMA's 2017 Retail Banking Market Investigation Order (hereafter, "the CMA Order"). Having consulted extensively with our ecosystem, however, we conclude that this discussion is distracting attention away from the more strategic issue of what comes next after open banking. The composition and powers of the future OBIE are to some degree moot in the event that open banking does not proceed on its journey towards open finance and beyond.

The FCA's Call for Input on Open Finance Feedback Statement published in March 2021 ***was not ambitious enough***. Consequently, this report seeks to inject the debate with a shot of strategic perspective and section three will articulate the three potential paths available to proceed towards open finance: organic expansion, regulator intervention and a Smart Data Right.

These pathways present three ways forward, with different degrees of complexity and varied challenges. Importantly, this complexity should not permit inaction: against the backdrop of an increasingly competitive international landscape, stunted data portability and market opportunity, it is time to choose a path.

Open finance is not the destination, it is merely another stop on the open data journey, and with this in mind only one option offers a path to this goal: a Smart Data Right.

With growing momentum behind realising the potential of Data Portability, the UK should follow through on the intent outlined in the whitepaper published in September 2020 by the Department for Business, Energy and Industrial Strategy (BEIS) to mandate industry involvement in Smart Data initiatives across the economy.

Coadec believes that a Smart Data Right is the preferable pathway to open finance and advocates that parliamentary time be allocated to legislate for this as soon as possible. At minimum, this should be in the next Queen's Speech.

In the final section of this report we outline some of the critical challenges and opportunities that a Consumer Data Right presents, including by recommending tactical steps that BEIS can take to set this legislation up for success.

KEY RECOMMENDATIONS

1. **Mop Up Open Banking**
   Remove 90 day re-authentication, redefine AIS, take meaningful steps to encourage the uptake of payment initiation, and enforce ASPSP API quality.

2. **Avenues to Open Finance**
   There are multiple pathways to open finance and this report analyses three options: organic expansion, regulator intervention and a Smart Data Right. Coadec recommends the latter: it should be in the next Queen's Speech.

3. **Legislating for a Smart Data Right**
   Setting the regulatory wheels in motion for a Smart Data Right is a necessary step but will present complex issues. It is vital that the Government sets the legislation up for success by focusing on a few tactical areas: cross-sector third party authentication, reciprocity and digital identity. It is recommended that BEIS launch a consultation on a Smart Data Right in Autumn 2021.

SECTION 1:
The State of Play in Open Banking.

THE GLOBAL REGULATORY PICTURE

In contrast to the picture in January 2018 when the UK was the only regulated open banking ecosystem on the planet, the scene is a lot more crowded in Autumn 2021. There are now eight other jurisdictions with open banking regulations enacted, plus EU member states, a further five launching regimes in 2021 and four more set to table legislation.

Open banking legislation likely to be tabled in 2021	***Open banking to launch in 2021***	***Open banking live (date)***
Indonesia	Hong Kong	UK (2018)
Philippines	Mexico	Europe (2019)
Saudi Arabia	Nigeria	Bahrain (2019)
USA	Turkey	Australia (2019)
	Ukraine	South Korea (2019)
		Japan (2020)
		India (*voluntary* 2020)
		Brazil (2021)
		Israel (2021)
		Taiwan (*pilot* 2021)

Table 1: Open Banking Regulations in 2021

Importantly, of the chasing pack, at least three regimes have already built in or publicised ambitious plans to expand the scope of the regulations beyond that which is currently live in the UK.

CASE STUDY: MEXICO

In 2018, Mexico published a far-reaching Fintech Law setting out an ambitious legislative agenda for regulating Fintech activities such as cryptocurrency, crowdfunding platforms and electronic payments. It also included the introduction of open banking across all financial products, to be implemented incrementally. So far the CNBV has not published details of operationalisation beyond product data APIs but all signs point to the rubber hitting road this year.

CASE STUDY: SOUTH KOREA

South Korea initially started investigating Open Platform initiatives as far back as 2015 and launched an open banking pilot in October 2019. The Korea Finance Telecommunications & Clearings Institute (KFTC) is responsible for overseeing the regulatory implementation and, in contrast to every other open banking ecosystem globally, runs a centralised data access network known as the Open Banking Platform Centre (OBPC). The OBPC facilitates TPP access to bank APIs to enable both account information and payment transfer.

As of September 2020, 22 million Koreans, representing 82% of the economically active population, were using OBPC enabled services, with 42 financial entities engaged with providing services. The Financial Service Commission in Korea unveiled plans in February 2021 to expand the scope of accessible accounts to savings and credit cards in the first half of 2021, with investments following later in the year.

CASE STUDY: AUSTRALIA

The Consumer Data Right (CDR) was announced in November 2017 as a far reaching piece of legislation that will equip citizens in Australia with a right to access and consent to transfer their data between entities. Initially starting in the financial sector with the Big Four banks in Australia, the initiative laid out the phased implementation across the majority of financial products and providers between 2019 and 2021 and was enforced by the Australian Competition and Consumer Commission (ACCC). Customer data started to be shared from July 2020 and as of July 2021 all authorised deposit-taking institutions are required to enable customers to grant access to their data under the CDR.

The Australian Consumer Data Right was unique in its conceptual ambition, with the expansive scope not just covering much of the financial sector, but aspiring to incorporate Energy and Telecommunications within a few years. In June 2020 the ACCC formally expanded the regulation to cover the Energy sector and launched a consultation into the rules a month later, which remains ongoing.

OPEN BANKING IN THE UK TODAY

It is now three years since open banking launched in January 2018. The number of third party providers (TPPs) has an annual compound growth rate of 47%, and in June 2021 there were 230 TPPs registered with the OBIE, which is more than in the rest of Europe combined. Covid-19 has accelerated adoption and there are now nearly four million active users, with over 50% of SMEs using open banking enabled tools. In May 2021, total successful API calls reached a record 834.1 million.

While these are not insignificant numbers, the ambition of open banking was to break the hold of the biggest banks in the UK; against this objective, open banking has not yet succeeded.

Data from the UK's current account switching service demonstrated that in Q1 2021 the CMA9 banks saw a net loss in account holds of 6,707, while non-CMA9 banks saw a net gain in account holders of 6,765. Three years into open banking, this is not a resounding success, especially when overall current account additions for the CMA9 banks were 274% that of the non-CMA9. The stranglehold persists.

Banking is not yet open, it is at best ajar.

So, how could the ecosystem be improved to further ease this grip?

Thankfully, we already pointed out a selection of opportunities in our last report. With the UK's departure from the EU now finalised, there is a great opportunity to return to these recommendations:

1. **Update the SCA-RTS to remove 90 day reauthentication limit and redefine AIS**

2. **Make tactical changes to encourage the uptake of PIS**

3. **Enforce API quality and performance.**

SECTION 2: Mopping Up Open Banking.

THE NINETY DAY HEADACHE

With the advent of Brexit, the FCA now has the freedom to change the regulatory technical standards that operationalise open banking in the UK. The first action that the FCA can take to tie up one of the most pressing loose ends is to remove the 90 day re-authentication obligation in the RTS.

In February 2021, the FCA published a consultation on changes to the SCA-RTS that included a shifting from the language of re-authentication to the language of re-consent. In truth, other than rightfully giving TPPs ownership of the consent journey, the proposed changes accomplish very little. This is because the 90 day re-authentication requirement is anathema to the intent of open banking.

Strong Customer Authentication (SCA) is designed to minimise customer harm by presenting necessary friction to decisions that could negatively impact them. Regardless of whether it has been designed correctly or not to achieve this objective, it is here to stay. For the initial account information service connection, many of our members recognise that SCA is justified as reflecting the identical requirement for accessing information through a proprietary online banking journey.

The 90 day reauthentication stipulation, however, presents unnecessary and obstructive friction to the provision of open banking services.

The evidence for this is clear. Data from a broad sample of mature TPPs, shows that under the 90 day re-authentication requirement, customer attrition rates have varied between 13-65%, depending on the business model. These rates are simply not economically sustainable at either end of the spectrum.

Importantly, the reason behind the 90 day re-authentication is not clear. Is 90 days the time it takes for a product to be deemed valuable by a customer? Is there a consumer goldfish phenomenon where customers only remember the last 89 days of their lives that the European Commission has evidence of? Interestingly it seems that Australian consumers have evolved further than us, as they appear to be able to handle 364 days before having to be reminded.

This is of course facetious. It is vitally important that consumers are able to change their minds about data sharing. However, placing an arbitrary limit of the timeline open to service providers to justify their wears, whilst they are innovating and evolving rapidly seems at best condescending to both consumers and TPPs, and at worst anticompetitive. Open banking use cases are varied and no one limit works best in all cases.

This is additionally frustrating when compared to the other customer services like direct debit. In the case of direct debit, a customer consents to a recurring payment, sometimes indefinitely, which is processed automatically, without customer consent. In contrast to the provision of AIS, which is read-only and minimal customer risk, direct debit is a process that involves the transfer of funds. The former is arbitrarily hindered by a cut-off after 90 days, the other can go on indefinitely. This report is not seeking to reform direct debit, but instead highlight the inconsistent and unproportionate regulation today.

The 90 day limit should not be reviewed. It should not be reformed. It should be removed.

Instead, the FCA should encourage the creation of access dashboards by all ASPSPs. Currently, only ASPSPs under the CMA Order are compelled to do so. It is currently already a requirement for Account Information Service Providers (AISPs) in the UK to host consent dashboards, and TPPs are often best placed to offer intuitive interfaces for consent management (see below case study). It is through these interfaces that users have control over their data sharing. Instead of enforcing the termination of a data exchange *that they have already authorised and have a legal right to*, the FCA should encourage ASPSPs not mandated to create a consent dashboard. Returning to the direct debit example, I expect to be able to view, modify or revoke direct debits through my bank: I should be able to do the same for data access.

In parallel, the FCA should consider ways to encourage ASPSPs to send reminders periodically (potentially every 90 days) of the live data connections. Data transfer should be opt-out, however, rather than opt-in as they are today through the 90 day re-authentication mechanism.

CASE STUDY: PLAID PORTAL

Keeping track of where they have consented to share financial information is a critical customer need. It is also fundamental to open banking: the initial sharing must be directed by consumers with their informed and explicit consent, and they should be able to track and revoke consent on demand. To support this need, Plaid has developed a product called “Plaid Portal” that will enable users to see their permissions in one easy to use interface. It’s kinda like an access dashboard but hosted by Plaid for end consumers to use.

Currently only available in the US, it is being used by consumers to monitor and control permissioned data access for their US Bank accounts and Fintech applications. Through a simple swipe, consumers can turn off data sharing, meaning their data will no longer be shared between the bank and Plaid’s Fintech partners. For non-US consumers Plaid Portal is available in beta in the UK and the Netherlands.

REDEFINING ACCOUNT INFORMATION SERVICES

The definition of AIS in the UK Payment Services Regulation is unique and unhelpful. HMT defined AISP as 'an online service **which provides consolidated information to the account holder...**'. For example, a Personal Financial Management app that displays a customer's banking data all in one place. This is in distinct contrast to other European markets, where the provision of AIS is not so prescriptively defined.

According to the European Commission, PSD2 does not require an AISP to share the consolidated information to the customer in order for the service to be an 'account information service' within the meaning of PSD2. The AISP may transfer the consolidated information to a third party with the express consent of the payment service user. However, other provisions of EU law, such as the General Data Protection Regulation (GDPR) may apply to the third party.

The Dutch financial regulator (the DNB), for instance, based its definition on the retrieval of data and not the display. In their view consolidated account information already exists if the original information from one or more payment accounts is retrieved by the AISP from a financial institution for a certain period of time. It is then up to the AISP to decide whether it wants to share that consolidated information back to the customer or not.

The customer is then able to give the AISP a GDPR permission to send the data onto another third party. After all, the definition of the term account information service does not specify to whom the consolidated account information is provided. According to the DNB, the actual processing of the collected payment data can then be done by the third party.

This is a more forward thinking approach that has prompted greater innovation whereby another third-party can use that information to provide a service for the end consumer, for example, in the case of credit scoring, mortgage applications or loan applications. But it also lays the groundwork for the necessary data-sharing infrastructure required to unlock an open data ecosystem. If we think about open finance, and open data beyond that, it will be necessary for AISPs to send data that exists in different product verticals (or different sectors in the case of smart data) onto third parties for them to aggregate/consolidate and provide their services to consumers.

This difference in definition alone is actually threatening to deter foreign direct investment into the UK. US and global brands like Venmo, Chime and Acorn are now looking to expand their business to Europe, favouring the continent versus the UK. Even Microsoft is considering this as well for its open banking services, just because of the huge additional utility that this slight definitional difference brings.

Changing the definition of AIS would make the UK more attractive for foreign firms that see open banking and open finance as an opportunity, and it would greatly encourage inward flows of investment.

PAYMENT INITIATION PROLIFERATION

Payment Initiation Services Providers (PISPs) represent an overdue and high-upside innovation in the payments space. The underlying technology offers significant opportunities for reducing merchant fees and increasing speed and security of payment, alongside an intuitive user experience, *if implemented correctly.*

PIS has failed to take off in the same way as AIS has in the last three years of open banking. While the relative proportion of overall AIS/PIS API calls is often cited as evidence for this (>99% AIS), this is a misleading figure due to the fundamentally different use cases delivered by both.

Instead, it's more helpful to recognise the volume of PIS calls relative to the volume of other payment types. In April 2021 there were 7,692,939 successful PISP API calls compared to 1.6 billion card payments. This is a stark reminder of the early stage of this payment method.

What can be done to accelerate adoption? API success rates are improving, providers are increasing volumes and the recent HMRC tender will all help with ubiquity, but challenges remain.

In many of the discussions with our startup community, the issue of 'first use failure' came up time and again, largely linked to the growing and pressing issue of authorised push payments (APP) fraud.

APP scams occur when fraudsters trick account users into transferring money to them by posing as a legitimate payee or constructing fraudulent reasons for a payment. It is the second largest type of payment fraud, with losses of £207.8 million in the first half of 2020. APP scams are rightfully the focus of concerted industry efforts to minimise consumer harm through education and processes to mitigate the chance of a user authorising a fraudulent transaction.

Unfortunately, APP fraud concerns may be hindering the uptake of PIS, particularly for high value, first use transactions. Under the original wording of PSD2, ASPSPs must not present additional obstacles to the provision of AIS or PIS by legitimate TPPs. The only circumstances whereby blocking may be legitimate is in the event of 'unauthorised or fraudulent' activity. Anecdotally, providers in our community spoke of incidents of legitimate PIS being rejected on APP fraud grounds. This is perhaps inevitable given the Payment Systems Regulator's (PSR) focus on ASPSP liability, which necessarily puts banks on the defensive.

Approaching this important but thorny issue creatively and with urgency should be a priority for the FCA.

One potential weapon in the arsenal against APP fraud is the Confirmation of Payee (CoP) initiative. Through CoP, customers can verify that the name of the account holder they are paying matches the intended recipient. In theory, while this alone will not eliminate APP fraud, it would give customers confidence in making informed transactions. There are challenges with operationalising CoP, including issues around data accuracy if account holders have failed to maintain up to date information, but if thoughtfully integrated into user journeys and framed appropriately could present a way to encourage uptake of PIS.

We eagerly anticipate the findings of the PSR consultation on APP scams that closed in April 2021: measures such as standardised shared fraud scoring would be welcomed in the event that more legitimate first time PIS transactions are permitted. Importantly, the voices of PIS providers must be heard as part of this review. It is challenging to imagine how PISPs will thrive whilst regulators incentivise ASPSP caution.

Finally, delivering on the VRP and sweeping elements of the OBIE roadmap, as the CMA has stated it will do, will undoubtedly enrich use cases.

CASE STUDY: CREZCO

Crezco, a registered PISP, uses its AIS license to build proprietary payment fraud prevention tools, demonstrating the power of combining the two regulated services to prevent customer harm. Crezco founder Ralph Rogge says a challenge with preventing APP fraud is that the payer's bank knows nothing about the payee. Victims have been sent erroneous details by email, text or post to process manually. Open banking PISPs like Crezco can sit between the two and can provide assurance to payers about the legitimacy of their intended payees due to being an AIS too.

To be paid via Crezco as payee, you need to create an account with them first. Crezco analyses the payee's bank account before agreeing to process payment initiation requests to that bank account. Rogge says, "a fraudster's bank is distinctly different to a legitimate payee's bank account. In identifying and either restricting or blacklisting fraudulent bank accounts Crezco allows the legitimate customers to operate more freely while mitigating APP. Crezco's analytical approach is more accurate than arbitrarily setting transaction limits which affect all payees and payers alike."

Fraudsters are quick to learn: if transaction limits are set to £20,000, they will soon start requesting £19,000. This risks a race to the bottom creating more friction than fraud prevention. Beyond simple transaction limits, ASPSPs run their own fraud identification systems, but the number of false positives is often high. ASPSPs may block legitimate and regular payments to suppliers or employees. While perhaps well-meaning, this not only inconveniences customers but prevents familiarity and trust building in PISPs. This is additionally frustrating given the AIS tools available to mitigate the risk.

APIs: STICKS AND CARROTS

APIs are currently best practice for data exchange. They are far superior to the previous means of data exchange, screen-scraping enabled by credential sharing, which exposes user credentials to potential risk, operationally strains both third party provider and payment service provider technical infrastructures, and risks instability and process breakdown.

For the necessary transition away from credential sharing to occur, payment service provider APIs must be better than the screen scraping connection.

Open banking in the UK had an 18 month head start on its counterpart in Europe and this, alongside the coordinating presence of the OBIE, has meant that ASPSP API quality is one of the best around. The continental bar, however, is not high.

As we look towards a post-OBIE open banking regime, the FCA should be proactive in policing the quality of the APIs available from the banks. In parallel, the FCA should also seek to define in more detail what constitutes a premium API to equip banks with more certainty around how they can monetise data exposure. Importantly, customer data that they are entitled to share under the Right to Data Portability under Article 20 of the GDPR should never be available through premium APIs.

For this reason we are not impressed by the OBIE's Extended Customer Attributes (ECA) API specification. It is against the very premise of open banking for the Heritage Banks to monetise identity attributes of their customers. This is particularly prescient considering research from Tink has found that 2 of the 3 most offered open banking use cases in the UK are identity based (KYC and digital identity services).

If the ECA specification is operationalised, it sets the precedent that Heritage Banks *own* customer identity data. We are greatly concerned about this.

It is pragmatic to recognise that ASPSPs will be seeking ways to recoup some of the expenditure exerted over the last few years but this should not be at the expense of data portability. Instead, premium API standards that could be attractive to ASPSPs, *and* compatible with the principle of data portability.

Critically, therein lies the distinction between the raw data points/attributes, which belong to the customer, and the abstract interpretation of a bundle of data points that could constitute a proprietary "digital identity", which could then be monetised. Implementing a premium "ECA API" must never replace provision of the raw attributes for free under a Smart Data Right.

An alternative premium API could be for product information, data that is not yet required to be shared outside of the CMA9. Further premium APIs could be offered *in addition to* the regulatory required API: an ASPSP could offer a non-standard API to meet regulatory requirements and then offer an API built to a defined standard at a premium.

THE OBIE QUANDRY

The OBIE has accelerated the adoption of open banking in the UK: the contrasting experiences here compared to the European continent illustrate this. It is, however, an entity that existed to fulfil a distinct purpose and it is appropriate to recognise that this original roadmap is nearing its end.

Earlier this year the CMA consulted on the future of the OBIE as it nears the end of its remit. In March 2021, UK Finance, a trade body representing the Heritage Banks in the UK, published a proposal for the future model of the OBIE once its roadmap under the 2017 CMA Order expires. The fact that the CMA's proposal asked for stakeholder critique *on UK Finance's proposal* demonstrates there is a risk that the Heritage Banks are already seeking to define a future open finance ecosystem that works in their favour. Regardless of the content of this proposal, it is concerning that the CMA did not consult in a more open-ended and transparent way.

There is too much at stake for the Heritage Banks, who have most to lose from the emancipation of customer data, to dictate the rules of open finance.

Looking forward, the future entity must become financially self-sufficient, and the advent of open finance is an excellent opportunity for the OBIE to move towards an independent, but voluntary, standards setting body. The expertise it has accumulated over the last few years sets it up well to be a useful actor in the ecosystem, but now is not the time to prescribe the entity's role in future open data initiatives. As we look towards open finance and beyond, this evolution of the governance paradigm should be built flexibly and ambitiously.

More fundamentally, debates around the future of the entity are occupying the attention of the ecosystem while it is not clear that as much time is being spent articulating a vision for getting to open finance.

SECTION 3: Avenues to Open Finance.

In March 2021, the FCA published its long awaited response to the Call for Input on Open Finance it ran in December 2019. It's safe to say the UK Fintech sector wasn't inspired. It contained no concrete next steps or commitments that will support the expansion of the open banking ecosystem to cover more financial products. It did, however, validate the appetite from stakeholders across industry to pursue open finance.

From the FCA consultation we can outline the benefits of open finance as to:

- Increase competition
- Improve advice
- Promote product innovation
- Improve access
- Accelerate "modernisation" and digitization
- Enable downstream operational expenditure savings

According to a June 2021 report from McKinsey, if open finance was realised in the UK there could be a potential increase of 1-1.5% in GDP by 2030, with $133 in increased deposit yields per account per year through easier account switching.

The availability of more data sets will enrich existing use cases and lead to unforeseen innovation. A recent report from Platformable highlighted how open finance could also precipitate broader societal benefits, from job creation and financial inclusion, to environmental and ethical practices.

Two areas that feature heavily as the next sectors to look to open up are savings and pensions. In both cases, there are providers ready to utilise data portability in these industries to create services and products for customers.

Against the backdrop of near consensus that expanding the ecosystem to cover more financial products is aspirational, there is far less agreement on how to get there. There are multiple pathways, of which three merit serious consideration.

Pathway One: **Organic Expansion**

Pathway Two: **Regulator Intervention**

Pathway Three: **a Smart Data Right in Primary Legislation**

CASE STUDY: PENSIONBEE & OPEN PENSIONS

PensionBee exists to reunite its customers with their pensions and discover how to take steps towards financial freedom. They do this through enabling customers to combine pensions from multiple providers into one new diversified online plan. Over 500,000 UK customers have an account with PensionBee, attracted by an intuitive interface, transparent fees and great service.

Open Pensions would enable customers to port customer data from one provider to another, like PensionBee's, to enable easy aggregation of information, but more importantly, the ability to take informed decisions based on what they see.

PensionBee has previously carried out research into customer awareness of their pensions schemes, finding that despite 70% of savers knowing who their pension provider is, they face multiple hurdles to accessing, let alone transferring, their data under the existing conditions. Paper forms, wet signatures and multiple ID verification steps are often required, meaning highly sensitive information needs to be sent via the post.

This is not the 90s. It's impossible for consumers to take responsibility for their retirement if they cannot access their information quickly, securely, and on demand. Open Pensions is a way to fix this broken process and bring greater consistency to consumer experience. The transparency of information will also inject much needed accountability into an ecosystem where incumbent providers often rely on customer inertia.

CASE STUDY: PLUM & OPEN SAVINGS

UK and Greece based Fintech Plum enables intelligent, automated saving for its 1.5m customers across Europe powered by open banking, and is forecasted to have more than $1.5bn saved globally by the end of 2021. Plum leverages an AISP partner to aggregate users' bank accounts into one consolidated view and then offers tailored savings support based on the users profile and goals. Today, Plum enables saving in interest-bearing accounts, investments and, as of June 2021, a self-invested personal pension (SIPP).

The advent of Open Savings and Open Pensions would enrich Plum's offering even further: while to date only payment accounts are guaranteed to be available to aggregate through open banking APIs, the possibility of adding ISAs and pensions to the equation could enable even further personalization and convenience for Plum's users. It would also increase opportunities for Plum to help maximise the saving potential of its users.

PATHWAY ONE: ORGANIC EXPANSION

There is a school of thought that this expansion to open finance could be possible through organic industry-driven innovation. To some extent this organic expansion is already happening, with providers entering into bilateral agreements to expose data points not covered by regulation.

Organic expansion could be accelerated by coordination from industry consortia. An international example is the Financial Data Exchange (FDX) in the US, and, closer to home, the Investments and Savings Alliance (TISA) is already laying the groundwork for Open Savings. Over the last two years, TISA has developed the Open Savings, Investments and Pensions (OSIP) initiative seeking to define the standards for API enabled data sharing in the savings industry. Since the start of 2019, OSIP has completed phases 1 and 2 of its roadmap, so far successfully defining the scope and vision, and also completing a proof of concept in 2019. Phase 3, the implementation roadmap, commenced in December 2020.

There is no direct equivalent in the Pensions sector, though there is legislative backing for the Pensions Dashboard, a long standing initiative aimed to go live in 2023 with the objective of reuniting users with "lost pensions" through an industry wide identity. The Pensions dashboard does not introduce Open Pensions, however, which instead refers to customer directed sharing of pensions data with consent. While it is intuitive that the Pensions Dashboard and Open Pensions overlap, it is not inevitable that the first leads to the second. Indeed, given the opaque and complex nature of the pensions sector, it is very unlikely that providers will be open to exposing data to enable data portability, particularly as some providers remain paper based.

An alternative source of organic growth could be through the guidance and coordination of the OBIE. So far the OBIE has proven effective in progressing discussions on premium APIs, refining API specifications (through the introduction of refunds for PISPs, for example), and facilitating certification, particularly post-Brexit with the revocation of eIDAS certificates. It is not clear, however, that the OBIE will ever be able to facilitate open finance.

As highlighted above, the attempt by the CMA9 to assert control of the future direction of the OBIE demonstrates their desire to limit the extent to which they are compelled to act any further through organic growth of the ecosystem under the OBIE's direction. And who can blame them when the OBIE was created by the CMA Order in 2017 as a remedy to a very specific competition intervention? Any future roadmap must link back to their original order, and it is not clear how much more can be tangentially linked.

Unfortunately, despite these shoots of progress in savings and pensions, evidence from markets without compulsion for data providers to open up APIs to TPPs demonstrates that progress is slow, if it occurs at all.

In the US, data access agreements (DAAs) are time and resource intensive, meaning they are few and far between, while screen-scraping enabled by credential sharing continues to persist. As a result of the slow progress, President Biden signed an Executive Order in July 2021 encouraging the CFPB to commence a rulemaking order to facilitate financial data portability. In Japan, where in theory the Amended Banking Act introduced open banking in 2020, there is no compulsion for non-discriminatory access. In reality, Heritage Banks and data providers in Japan can hide behind a paywall and the onus is on third parties to still negotiate DAAs if they want to access information through APIs. This has led to painstaking delays in the transition to API enabled data sharing.

In sum, unless financial institutions *have* to enable customer data portability, they won't, or they will, but on their terms. A recent report from Platformable found that 9/10 of the most advanced enabled open banking ecosystems in the world were governed by regulation, all in Europe. It is clear that the road to open finance requires a source of compulsion.

The experience of open banking in the UK combined with the now extensive list of similar initiatives captured in section one of this report give a helpful choice of routes to expanding the open banking regime to include savings and pensions data. One option is for open finance to be pursued as correcting a competition issue in a sector, as it was as part of the remedy outlined in the CMA Order.

PATHWAY TWO: REGULATOR INTERVENTION

One of the primary benefits of open banking is that the increased portability of information removes friction for customer comparison between products, while also enabling new use cases that add value and increase competitive innovation in sectors. More explicitly in the UK, fixing a market failure that precipitated at least one adverse effect on competition (AEC) was an explicit driver behind the creation of open banking under the CMA Order. Through this, the nine biggest banks and their subsidiaries were compelled to open up APIs and the OBIE was created.

As a consequence, there is a precedent for enabling data portability in an industry through regulator intervention, and this is one possible avenue for expanding open banking to open finance.

What would this tangibly entail? Firstly, for open finance to be imposed by the CMA, it would need to conduct a full investigation into a market under sections 131 and 133 of the Enterprise Act 2002 and conclude that an AEC is present. Secondly, it would need to conclude that data portability is part of the remedy.

There are multiple uncertainties here. Initially, the CMA would need to have justification to investigate, triggered by a substantive case that there is a market failure in a financial industry. Further, it is not necessarily the case that AECs would be uncovered. Are there financial markets that exhibit the hallmarks of AECs? Utilising the examples of savings and pensions, highlighted above as two open finance market candidates, presents useful insights.

Regulator Intervention in the Savings Market

Savings are notorious for consumer inertia, as many consumers do not think about their savings everyday they are more likely to leave it with a provider and risk missing out on better rates.

According to the FCA's 2020 Financial Lives Survey (FLS), the percentage of UK citizens with bank accounts has increased to 77%, while the percentage with an investment product has increased to 33%. In fact the FLS found that 90% of savers hadn't switched savings accounts within 3 years of opening, despite average interest rates dropping after 12 months. The survey also found that 27% of customers remain with their savings provider for over 10 years.

The Covid-19 pandemic is likely to make this consumer inertia even more pronounced: as a result of reduced spending, the households' saving ratio, which represents the proportion of household savings to disposable income, reached historic levels in 2020 of over 25%. By giving customers the opportunity to compare products and switch providers more easily, "Open Savings" could erode consumer inertia encouraging more consumers to save and get the best rates possible.

The savings market bears similarities to the current account market in market share of providers, many of whom were compelled to act by the original CMA Order and thus have the existing operational and technical infrastructure to build APIs.

Regulator Intervention in the Pensions Market

Evidence suggests that 60% of people don't know how much money they have in their pension savings, while 25% had never even checked their savings. In 2018 the Pensions Policy Institute estimated that there may be as much as £19.4 billion in "lost pension pots". This isn't surprising as research from PensionBee states that 80% of consumers leave their pension behind when they switch jobs.

In 2013, the Office of Fair Trading (OFT) launched the 'Defined contribution workplace pension market study', an investigation into consumer harm in the pension market. It's conclusions described the buyer side of the defined contribution workplace pensions market as one of the 'weakest that the OFT has analysed in recent years'. They found that pensions are too complex, members don't understand the array of charges, are unable to pick their provider, and yet bear all the risk. None of the issues identified back in 2013 have been addressed. In contrast to other financial markets, there is a multitude of providers in the pensions space though many occupy the long tail, with relatively low absolute market share. Handily, our friends at Pensionbee have already calculated that 12 providers hold around 80% of defined contribution pension data, and thus the prospect of an intervention compelling the major players to open up the customer information they hold could be practical.

In both the savings and pensions verticals there *may* be a case for the CMA to investigate the presence of AECs. However, intervention in this way as a route to open finance is *not desirable* because of complexity, time and the chance of creating a fragmented, multi-track open data economy.

Firstly, for the CMA to intervene there must be concerns from the industry that anti-competitive practice is afoot. It is not clear that this is the case: if it were, the CMA would be investigating already, and it's not clear from the discussion above that there is an undiscovered definitive case for CMA investigation.

Secondly, CMA investigations necessarily take a long time. It took two years for the CMA to go from initiating the retail banking investigation to defining a remedy, and a further two years for this remedy to be enforced. Indeed, the continuing existence of the OBIE three years subsequent means that the CMA Order has currently taken seven years (2014-2021) to implement, *so far*. Against the backdrop of increasing international competition, nascent consumer demand to share data, and the market opportunity of open finance, this is too long to wait for one more vertical to open up.

Thirdly, and finally, even if the CMA were to intervene, it's not certain that the remedy to the potentially identified AEC(s) would be open finance. Even if it were, it would likely lead to a distinct open data regime from the other sectors that wouldn't necessarily interact with the existing OBIE and PSD2 regimes. It is likely that multiple open data ecosystems would emerge, with distinct actors, infrastructure, and therefore a fragmented and inconsistent experience for consumers.

For the above reasons, regulator intervention is not aspirational. Instead, all roads lead to the third option, a Smart Data Right. This is the best way to achieve open finance, and would also set the fundamental foundation for an open data economy.

PATHWAY THREE: LEGISLATING FOR A SMART DATA RIGHT

In February 2021, Ron Kalifa OBE published the findings of his review of UK Fintech. As part of the review, he identified that a cross-sectoral approach to Smart Data was vital, recognising that open finance was the first step on a long journey towards open data. To ensure this initiative is set up for success, Kalifa referenced the need to ensure that "firms that hold very significant amounts of data (such as large technology companies)" are brought into the fold.

We agree. Open finance is not the destination, it is merely another stop on the open data journey. Our ticket to ride is the Smart Data Right.

Since 2016, citizens of the EU have the Right to Data Portability under the GDPR. In the UK, this was transposed as the UK GDPR and the Data Protection Act in 2018. This right entitles an individual to request a data holder transfer, or "port", information the data holder has about the individual to another entity in a structured, commonly used and machine readable format... so far so good... within a month. A whole month.

This gereatric "portability" is useless in an information age where value must be delivered quickly and efficiently: one of the most powerful successes of open banking is the live-time-ification of this right to data portability. To realise the true potential of data portability, and indeed to properly equip consumers with agency over their data, the UK must seek to develop an open data ecosystem, or what the Government refers to as "Smart Data". This is already the ambition of Australia through its own Consumer Data Right and was explicitly outlined in the UK Government's Smart Data Strategy published in September 2020.

Legislation should be technologically-neutral and principles and outcomes based, with clearly defined scope, timelines and enforcement mechanisms. This is a fundamental first step towards an Smart Data economy.

Ideally, the Government should deliver on this ambition and legislate for a Consumer Data Right within this Parliament. Coadec agrees with the Taskforce on Innovation, Growth and Regulatory Reform (TIGRR) aspiration that "BEIS brings forward it's Smart Data legislation as soon as possible this year" however, as it did not feature in the 2020 Queen's speech, this timetable is unlikely.

Consequently, it is imperative that the Smart Data Right features in the next Queen's Speech.

SECTION 4:
A Smart Data Right.

With growing momentum behind realising the potential of Data Portability, the UK should follow through on the intent outlined in the whitepaper published in September 2020 by the Department for Business, Energy and Industrial Strategy (BEIS) to mandate industry involvement in Smart Data initiatives across the economy.

This should be achieved through primary legislation for a Smart Data Right, with subsequent secondary legislation compelling the opening up of specific sectors.

Practically, to achieve open finance, this would require the primary Smart Data Right, followed by secondary legislation mandating the opening up of customer information in savings and pensions.

The lodestar should be a world where consumers can consent to securely share their data in live time across industries in exchange for delightful experiences, efficient servicing, and exciting products delivered by our world-leading tech startups.

There is an emerging assortment of governmental and regulatory bodies directly or indirectly related to the open data ecosystem: the Smart Data Working Group, the Digital Markets Unit (DMU), the Centre for Data Ethics and Innovation (CDEI), the CMA, sector specific regulators and industry collectives. It is important that these bodies coordinate effectively, with roles and responsibilities clearly defined and segmented.

The overall strategic direction must be directed by the Government. We agree with the broad recommendations of the Smart Data Working Group's June 2021 proposal to establish a Smart Data Council, led by a Steering Committee. This Committee must reflect a diverse range of stakeholder opinion, including the startup ecosystem and consumers. Enforcement of regulatory obligations must sit with the sector specific regulators, such as the FCA.

Ahead of the transition to open finance, the UK should look to the approach of the Mexican Fintech Law, where each product vertical regulator has explicit responsibility for enforcement. Meanwhile inspiration for compliance monitoring could be sourced from Brazil, where each data provider's API must pass a validation test to gain conformance accreditation.

Outside of this strategic direction and enforcement responsibility, there is scope for numerous actors to support the development of open data, including an opt-in service provider OBIE, the DMU and the CMA. All parties must partner cohesively, particularly as there are significant political, conceptual and operational challenges ahead.

There is also a vitally important role for regulatory sandboxes at an early stage in the expansion of open data ecosystems in new industries. For effective standards to materialise it is important for use cases to develop organically: one of the limitations with the FDX in the US is the imposition of use cases on to the ecosystem. In contrast, the FCA's sandbox has proven a catalyst in testing use cases, and we agree with the TIGRR recommendation that this example be used as a role model for future regulation. Regulatory sandboxes should be accessible, effective and publicised for every iteration of data portability across the economy. As open data expands beyond the FCA, it will also be important to consider setting up cross-sector sandboxes to truly enable innovation, and also the introduction of what TIGRR called "scaleboxes" to provide agile regulatory support to scale-ups. The FCA's Fintech regulatory nursery launching this autumn will be an interesting next step in this direction.

Alongside introducing a Smart Data Right, the Smart Data Council within BEIS should be empowered to form working groups on some of the most important challenges facing the realisation of a Smart Data economy.

To get the ball rolling, BEIS should consult on the design of a Smart Data Right in the Autumn of 2021. This will focus minds, stimulate discussion and bring the complexities to the surface. Coadec is willing and waiting to support this.

Three fundamental issues that should be included in this consultation and should be addressed as a matter of priority are: cross-sector third party accreditation, reciprocity and digital identity.

THIRD PARTY ACCREDITATION

For cross-sector Smart Data use cases to flourish, it is vital that there is an effective and functioning way for third parties to identify themselves to data holders as competent and secure recipients of a consumers' data.

In June 2021, BEIS published the results of a research study into cross-sector third party accreditation. This extensive review provides a useful precedent for subsequent research into the critical challenges posed by Smart Data. We were encouraged not just by the process but by the content of the review. We particularly agree with the specific recommendation that:

> *"Once TPPs have met accreditation requirements in one sector, they could be granted a 'passport'. This passport would 'fast-track' a TPP's application to access data from another sector and if successful provide them with a 'visa stamp' for the additional sector."*

The role of intermediaries like account aggregators will be vital in the open data economy, both in providing the technical capabilities for the exchange of information, and in providing consumers with consistent, trustworthy and secure user experiences. It makes sense that if third parties have gained certification to transfer financial information, they will be secure enough to transmit less sensitive information too.

Building on this report, we would like to highlight the Non-Financial Banking Company Account Aggregation (NBFC-AA) ecosystem in India. The NBFC-AA construct takes the intermediary role to a new level of significance in an open data regime. Instead of the three party regime articulated in the BEIS research, NBFC-AAs are a fourth party that orchestrates the entire data sharing. They perform a direct to consumer role, not just facilitating data exchange but also owning a consent dashboard that enables consumers to approve or decline data exchange.

Conceptually, this four-party construct may work well in an open data economy where cross-sector use cases proliferate, particularly if supported by a directory of regulated firms, as outlined in the BEIS research. We welcome the opportunity to work with BEIS on consulting with the ecosystem on how cross sector authentication could work, including the different entity relationships and structures that could facilitate this.

In its July 2021 report exploring the role of data intermediaries, the CDEI outlined six issues that may "prevent optimal data sharing": a lack of incentives, lack of knowledge, commercial, ethical and reputational risks, legal and regulatory risks, costs, and missed opportunities to use data in the public interest. Through this lens, the Smart Data Working Group should investigate how cross-sector data intermediaries could be defined, and regulated, in such a way that most if not all of these issues can be mitigated.

RECIPROCITY

Under the CDR in Australia, the reciprocity mechanism means those who wish to become accredited and consume CDR data at a consumer's request are compelled to share equivalent data in response to a consumer request. To consume, a firm must expose. The principle of reciprocity also applies to the NBFC-AA ecosystem in India.

Through the reciprocity mechanism, which could be set out in primary legislation, there is a clear ambition to enable maximum data portability across multiple sectors. Though there is clearly work to do to define "equivalent" data, this could be clarified through clear data scope set out in primary legislation where the default data scope is that which is available to the user through the proprietary online interface. This also clearly sets participant expectations that they will have to act in the future, including the Big Tech firms.

The Smart Data Council should start to grapple with this concept and consider whether it should be part of the UK Smart Data Right.

It is imperative that industry stakeholders are consulted on this, particularly those firms in our community. Implemented incorrectly, this could present an additional barrier to entry for firms. Alternatively, as the Smart Data Ecosystem matures, and APIs become commonplace, this could become a cost of doing business, with significant innovation opportunities as a result. Indeed, in response to the CDEI's first potential obstacle to optimal data sharing, 'a lack of incentives', introducing reciprocity would lay out clear costs and benefits of entry that could lead to organic growth of the ecosystem.

DIGITAL IDENTITY

In a world where users are able to truly exercise their right to Data Portability, products and services will combine data from across sectors to power completely new and innovative propositions. To support this cross-sector innovation, the ability to digitally identify users accurately will become imperative.

In August 2021, the Department for Culture, Media and Sport (DCMS) published its updated UK Digital Identity and Attributes Trust Framework, which included an 'Alpha' version of a proposed trust framework for Digital Identity providers. It is helpful that the DCMS is looking into this seriously, particularly as McKinsey have previously estimated that Digital Identity has the potential to increase UK GDP by 3% in 2030.

Importantly, this work cannot happen in isolation from the activities of the Smart Data Council. For Digital Identities to be useful, they must be linked to data portability. With a collaborative and joined-up approach to both initiatives, there is scope to unlock significant value across the economy.